Argonne NATIONAL LABORATORY

The Journal of Physical Security

Volume 7(3), 2014

JPS

THIS ISSUE...

Table of Contents

Journal of Physical Security, Volume 7(3), 2014

Editor's Comments

Welcome to volume 7, issue 3 of the Journal of Physical Security. This is the first time we have had 3 issues in the same year. This issue has papers about diplomatic security versus security expenditures, subjective approaches to security, physical security as a field, a performance-based approach to the security of sealed radioactive sources, crime reporting and victim support in Nigeria, and unconventional security devices.

As usual, the views expressed by the editor and authors are their own and should not necessarily be ascribed to their home institutions, Argonne National Laboratory, or the United States Department of Energy.

*****

Serialization & Product Counterfeiting

The last paper in this issue briefly discusses virtual random numeric tokens as a counter-measure to product counterfeiting (page 108). This kind of approach often gets confused with serialization, and sometimes with Track & Trace. Even when there isn't confusion, it often gets implemented in ways that involve one or more of 3-dozen common blunders. Contact me for more information.

*****

Objective Arguments for Subjectivity

The second paper in this issue is a viewpoint paper that discusses the importance, neglect, and even fear of subjective methods for security risk management. The September 6, 2014 issue of the *Financial Times* has an interesting article by Tim Harford about rigorous studies on the effectiveness of forecasting future events. (Security risk management, threat assessments, and vulnerability assessments are all, at least partially, exercises in predicting the future.)

The studies that the article summarizes conclude that the best forecasters are people who are "actively open-minded" thinkers. They welcome controversy and conflicting viewpoints, and aren't afraid to change their mind. To a lesser extent, forecasters did the best when they could think broadly rather than deeply, intuitively rather than logically, self-critically rather than in assured manner, and in *an ad hoc* way rather than systematically. In other words, subjective thinking beats objective thinking for prediction.

The *Financial Times* article offers practical suggestions for seeing ahead. The two most relevant for security are: (1) Don't let your hopes influence your forecasts, and (2) Keep in mind the famous remark attributed to John Maynard Keynes: "When my information changes, I alter my conclusions. What do you do, sir?"

*****

Corruption Eruption

A new study conducted by the University of Hong Kong and Indiana University identifies the most and least corrupt states. The researchers analyzed over 25,000 convictions of state officials for violating federal corruption laws between 1976 and 2008 relative to each state's number of public employees. Their findings indicate that the 10 most corrupt states are:

1. Mississippi
2. Louisiana
3. Tennessee
4. Illinois
5. Pennsylvania
6. Alabama
7. Alaska
8. South Dakota
9. Kentucky
10. Florida

The researchers estimate that 5.2% of state expenditures in the 10 most corrupt states are lost to corruption, representing $1,308 per resident on average.

The least corrupt states were Oregon, Washington, Minnesota, Nebraska, Iowa, Vermont, Utah, New Hampshire, Colorado, and Kansas. For more information on the study, see http://onlinelibrary.wiley.com/doi/10.1111/puar.12212/abstract.

*****

Why Biometrics Aren't a Silver Bullet

Dave Atel wrote a short article that nicely summarizes the problems with biometrics: (1) your biometric signature can't be kept secret, (2) it can't be revoked, (3) it's not hard to counterfeit, and (4) biometric readers can be spoofed. See http://www.usatoday.com/story/cybertruth/2013/09/12/why-biometrics-dont-work/2802095/

*****

Supply Chain Security

Dana Martin and Dean Ocampo have an interesting article in the May 1, 2014 issue of *Supply & Demand Chain Executive* entitled, "Crossing the Chasm in Supply Chain Security". They equate the current state of supply chain security and resilience to where IT security was 10 years ago. They bemoan the poor risk management, and the lack of clear security

strategy and process. They point out some of the lessons that IT security can teach supply chain security.

*****

Shoplifting

Rachel Shteir has written an interesting book I recommend that you buy (but don't steal). It is entitled, *The Steal: a Cultural History of Shoplifting.* Shoplifting is a relatively old crime; the term has been around for hundreds of years. She cites the statistic that about 11% of Americans have engaged in it.

*****

Some Things to Keep in Mind That Have Implications for Security

1. "High Security" is not a product attribute. It's a context-dependent value judgment.

2. In contemplating the use of any new security measure, strategy, or product, you need to determine the correct answers to 3 questions:
   (1) To what extend does this really improve security?
   (2) What are all the costs, tradeoffs, and side effects (because there always are some)?
   (3) Is 1 commensurate with 2?

3. Putting Security under the Operations Department is usually a bad idea because the culture is wrong and the focus/priorities are wrong for good Security.

4. If you automatically think "cyber" when somebody says "security", you probably have neither good cyber security nor good physical security.

5. Historically, the most frequently shoplifted book is the Bible.

6. Of the 30 million know species of bacteria, only about 70 cause disease.

7. About 1 million Americans are arrested each year for drunkenness.

8. Kernighan's Law: Debugging is twice as hard as writing the code in the first place. Therefore, if you write the code as cleverly as possible, you are, by definition, not smart enough to debug it.

9. According to Gary Kasparov: The number of different possible chess games is 10^{120}. A player looking 8 moves ahead is already presented with as many possible games as there are stars in the galaxy. There are more possible chess games than the number of atoms in the universe. [Given this, is it surprising that security and forecasting is hard?]

10. English television talk show with guests Paul Merton and Member of Parliament Glenda Jackson
Host: Do you remember your school motto?
Jackson: [Unsure of whether the host is asking her or Paul Merton] Who are you looking at?
Merton: That must have been one tough school!

*****

Field Research

A Washington DC news crew visited a particular DC neighborhood to investigate whether it did indeed have a high crime rate. While they were interviewing neighborhood residents, their van was broken into and most of their gear was stolen. Guess so! See http://www.newser.com/story/192419/tv-news-crew-robbed-on-story-about-sketchy-neighborhoods.html

*****

Expensive Criminal

Albuquerque KOAT-TV reported that an Albuquerque man charged with stealing cookies won't be released from jail because he cannot raise the $5 bond. A bail bond agent says that $5 is simply too high a risk to take. Meanwhile, the suspect sits in jail costing the taxpayers $80 a day.

*****

Keeping Threats in Perspective

A quote that made the newspapers:

> *She took an honorable icon that is seen in sporting venues everywhere and degraded it. Fortunately, the foam finger has been around long enough that it will survive this incident.*

This is a quote from Steve Chmelar, inventor of the foam finger, after Miley Cyrus performed a lewd song and dance routine with one at the 2013 MTV Video Music Awards

*****

--Roger Johnston
Vulnerability Assessment Team, Argonne National Laboratory, September 2014

LinkedIn: http://www.linkedin.com/in/rogergjohnston
VAT: http://www.ne.anl.gov/capabilities/vat
Journal of Physical Security: http://jps.anl.gov

Is Security Funding for U.S. Diplomatic Posts Correlated with the Death Rate from Significant Attacks?

Anthony Negrut
Michigan State University

Introduction

The terrorist attack on the U.S. Consulate in Benghazi on September 11, 2012 is still fresh in our minds, and the arguments on who is to blame, and what is to be done is still raging on Capitol Hill. The fact that U.S. Ambassador to Libya, Chris Stevens, and three other security personnel were killed is a tragedy, but this is not the first time the U.S. Department of State (DOS) or Diplomatic Security (DS) have dealt with (arguably) terrorist-related attacks at diplomatic missions. According to Al Jazeera (2013), there have been 709 significant attacks on U.S. missions between 1987 and 2012.

This paper examines how the amount of funds appropriated by the DOS for the security of its U.S. diplomatic posts for a fiscal year compares to U.S. deaths at diplomatic posts from terrorist attacks on a yearly basis for the associated calendar year. Additionally, the data for the amount of funds that were requested for each fiscal year were also collected and analyzed in order to see whether a larger discrepancy between enacted and requested funds led to additional deaths for that year. Years were also offset in the data to take into account possible lag times between deaths and funding.

Background

The 1983 bombings of military barracks and a U.S. embassy in Beirut which killed dozens U.S. personnel prompted the passage of the Omnibus Diplomatic Security and Antiterrorism act of 1986, which led to the creation of the Bureau of Diplomatic Security (Tiersky, 2013). Other measures included in this bill were:

> Improvements in State's protective intelligence, threat analysis, and alerting procedures; improvements in training for Foreign Service personnel and dependents; improvements in contingency planning at posts; assigning Marine Security Guard detachments to all highly sensitive posts; revising the Diplomatic Security Service physical security standards; pursuing a substantial building program to correct security deficiencies, in particular regarding perimeter security; and initiating a capital budgeting procedure to avoid security improvement delays due to budgetary reasons. (Tiersky, A. & Epstein S.B. 2013, pg. 13).

The adoption of this bill and its provisions were the result of the Inman Commission created in response to the Beirut bombings. The commission was tasked with providing recommendations to the DOS in order to prevent future terrorist attacks. The 1998 bombings of the U.S. embassies in Kenya and Tanzania led to the establishment of an Accountability Review Board that showed that the DOS had failed to give the appropriations necessary to meet the standards of the Inman Commission, as these embassies were only considered moderate and low-risk posts (Tiersky, A. & Epstein S.B., 2013). Furthermore, the board estimated that about 80% of the U.S. diplomatic facilities around the world were still short of meeting the Inman Commission standards.

Since the DOS's new security standards where implemented after the 1998 bombings, 200 facilities required upgrading in order to meet those standards. There have been 78 contracts awarded for the building of new compounds, with 50 already built and 80 more contracts to be awarded by the end of FY 2014 (Johnson, C.M., 2008). The attack on the U.S. temporary consulate in Benghazi has spurred the DOS to ramp up their production of more secure facilities, and they have requested $1.614 billion from Congress for Embassy Security, Construction and Maintenance (ESCM) for fiscal year 2014, which is more than double of what was requested the previous year at $689 million (Tiersky, A. & Epstein S.B., 2013).

Hypotheses

This paper concerns a comparison of the number of deaths from significant attacks on U.S diplomatic posts to the money requested and appropriated by the DOS for ESCM. I hypothesize that (1) the amount of funding appropriated to ESCM for a given fiscal year will be directly correlated with a decrease of deaths (which does not include the attackers) resulting from attacks on U.S. diplomatic posts for that associated calendar year.

However, when the amount of requested funds is significantly greater than what was appropriated to ESCM for that fiscal year, I predict (2) that casualties will increase drastically as Congress simply did not give enough money to the DOS to shore up any security deficiencies it uncovered. In other words, the greater the "funding shortfall" (requested funding – enacted funding) for a given fiscal year, the greater the amount of deaths (on average) for that calendar year, therefore displaying a positive correlation.

Furthermore, I hypothesize (3) that earlier years should generally have more deaths than later years as more embassies are brought up to the standard of the Inman Commission.

It should be noted that this is an introductory study that compares the correlation between variables. While I may speculate about causation, more data and analysis would be required to reliably determine causation.

Research Methodology

The funding for ESCM by fiscal year will be taken from two sources: The DOS website for the years 2002-2007, and the CRS report for the remaining years by Tiersky and Epstein. The number of casualties from significant attacks on U.S. diplomatic posts comes from a single source: the DOS and DS report on "Significant Attacks against U.S. Diplomatic Facilities and Personnel". The data for this variable was obtained by adding the deaths that occurred as the cause of attacks on U.S. diplomatic missions by calendar year, including deaths caused by attacks on U.S. diplomatic motorcades abroad. Significant attacks, as defined by the report, include any attacks that caused deaths or injury to any U.S. citizens, contractors, or other personnel residing at the facility during the attack, excluding the attackers. Some attacks where the motive could not be determined where excluded from this report, thus deflating the numbers.

The span of years for which there are data includes 2000 through 2014. No data were reported for deaths in the years 2000, 2001, 2013, and 2014, and no data were reported for enacted funding for 2014. There were also no data reported for requested funds for the years of 2000 and 2001. Therefore, the data used in this analysis covers the years 2002-2012, with data from other years used for discussion purposes.

In order to measure any correlation between ESCM funding and deaths, Pearson's linear correlation coefficient, r, was utilized.

Results

Table 1 lists the data used in this study, taken directly from certified U.S. government reports. It is important to note, as stated earlier, that some of the casualty numbers may be under-represented, as the report did not use data for any attack where the motive was unclear.

Figure 1 shows a graph of the data in table 1. Note the spikes in the number of deaths in 2002, 2008/2009, and 2012. Note also that there is no general trend of decreasing deaths with time, so my hypothesis #3 above is not supported.

Table 2 shows the Pearson's Correlation Coefficient (r) for the requested or enacted funding versus deaths between 2 years later and 3 years earlier (columns 4-9 in table 1). These offsets are of interest because there well may be a delayed effect between when more deaths drive increased funding, or when increased funding can implement security improvements that could help lower death rates. A correlation coefficient of $r = +1$ means perfect correlation between the two properties, $r = 0$ means no correlation, and $r = -1$ means perfect anti-correlation.

Table 1 - Funds enacted and requested for ESCM compared to diplomatic casualties. Adapted from Tiersky, A. & Epstein S.B., 2013, Table 1 and U.S. Department of State, 2013.

Year	Enacted Funding (millions of dollars)	Requested Funding (millions of dollars)	Deaths	Deaths Moved Up 1 Year	Deaths Moved Up 2 Years	Deaths Moved Up 3 Years	Deaths Moved Down 1 Year	Deaths Moved Down 2 Years
2000	736	---	---	---	32	5	---	---
2001	747	---	---	32	5	7	---	---
2002	747	747	32	5	7	9	---	---
2003	800	787	5	7	9	7	32	---
2004	840	797	7	9	7	5	5	32
2005	879	818	9	7	5	39	7	5
2006	898	872	7	5	39	17	9	7
2007	903	898	5	39	17	3	7	9
2008	671	809	39	17	3	3	5	7
2009	905	948	17	3	3	20	39	5
2010	847	938	3	3	20	---	17	39
2011	793	824	3	20	---	---	3	17
2012	775	938	20	---	---	---	3	3
2013	688	689	---	---	---	---	20	3
2014	---	1614	---	---	---	---	---	20

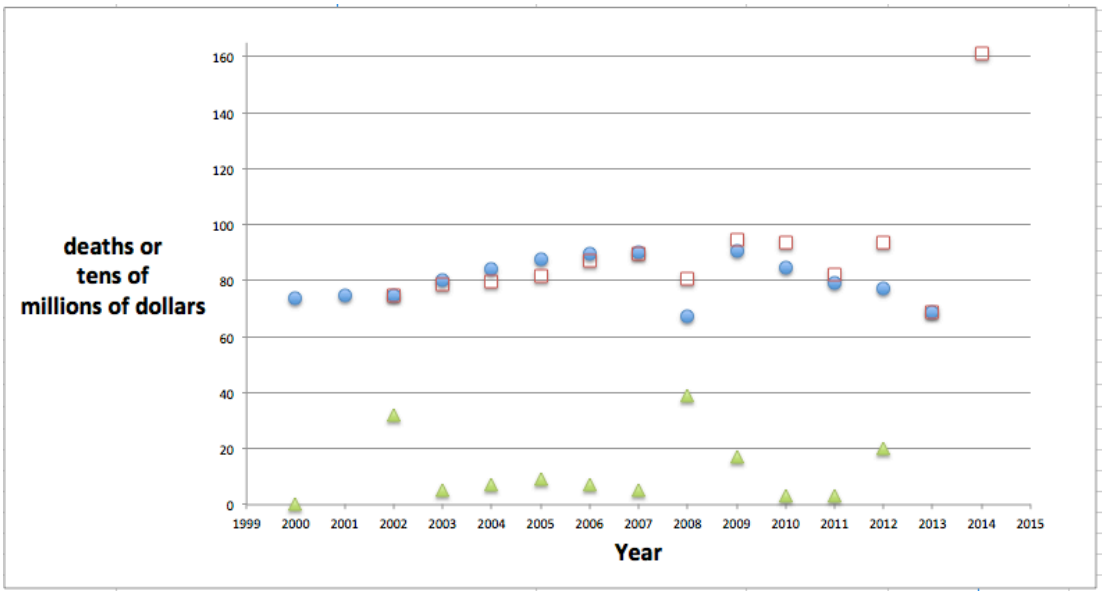

Figure 1 - Requested funding (red squares), enacted funding (filled blue circles), and deaths (triangles) in a given year. The two kinds of funding are plotted in tens of millions of dollars.

Table 2 - Correlation coefficients (r) for enacted or requested funding versus deaths offset by various numbers of year. (The correlation coefficient for x vs. y is the same as for y vs. x.)

	Deaths With Zero Offset	**Deaths Moved Up 1 Year**	**Deaths Moved Up 2 Years**	**Deaths Moved Up 3 Years**	**Deaths Moved Down 1 Year**	**Deaths Moved Down 2 Years**
Enacted Funds	**-0.72**	-0.16	0.21	**0.51**	0.17	0.17
Requested Funds	-0.26	0.06	0.34	0.19	0.14	0.21

The only relatively strong correlations or anti-correlations in table 2 are between enacted funds versus deaths the same year (anti-correlated), shown in figure 2, and deaths versus enacted funding 3 years earlier (correlated), shown in figure 3.

In the case of zero offset shown in figure 2, the value of r for deaths versus enacted funding (or enacted funding versus deaths) for the same year is fairly strongly anti-correlated: r = -0.72. Thus, deaths go down as spending goes up in a given year. This supports hypothesis #1 that security funding for U.S. diplomatic facilities is connected with a reduction in deaths for the same year. Such correlation, however, does not establish causation.

It is interesting to note that the value of r squared, which gives the fraction of the variation in deaths that is due to the variations in enacted funding, is fairly large: $r^2 = 0.52$.

For a 3-year offset, shown in figure 2, the value of r for deaths vs. enacted funding 3 years earlier is surprisingly positive: r = 0.51. This means that deaths increase with increased funding from 3 years earlier.

Referring again to figure 1, it is clear that the difference ("funding shortfall") between requested and enacted funds is greatest in 2008 and 2012 where two of the major spikes in deaths occurred. In fact, the correlation coefficient (r) for funding shortfall vs. deaths in the same year is r = 0.48, showing some degree of the positive correlation that was predicted in hypothesis #2 above . Thus, the funding shortfall tends to increase in the same year when deaths increase.

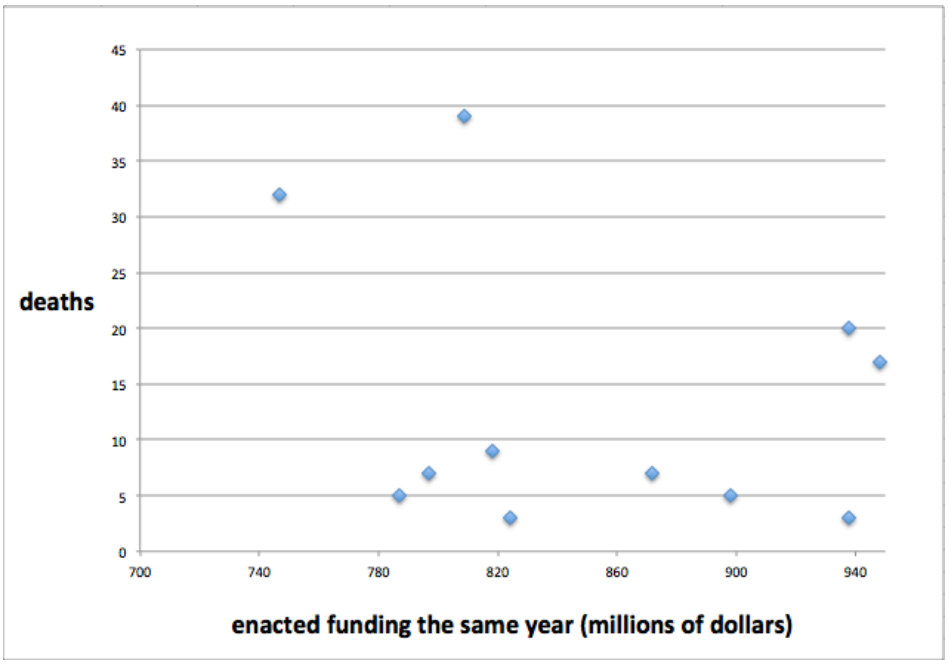

Figure 2 - Deaths in a given year versus the enacted funding for that same year. The correlation coefficient is r = -0.72, indicating substantial correlation between higher levels of funding and lower death rates.

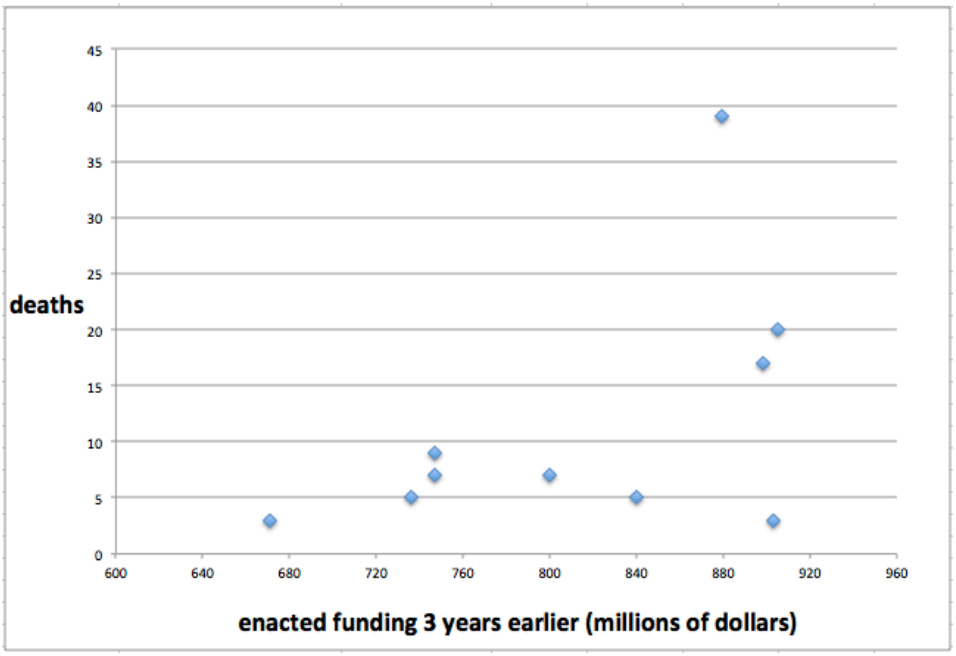

Figure 3 - Deaths in a given year versus the enacted funding 3 years earlier. The correlation coefficient is r = 0.51, rather than the expected negative correlation.

Discussion

Based on the findings collected in the tables and displayed on the graphs, it is clear that there there is indeed a negative correlation between the ESCM funding and death rates in the same year. Spend more money and deaths seem on average to go down.

What is harder to explain is the weak correlation for other time offsets, and the moderately strong positive correlation between deaths and enacted funding 3 years earlier.

It is also interesting that there is a moderately strong positive correlation between annual deaths and funding shortfalls (requested funding – enacted funding). Indeed, if we compare the 5 years with the lowest enacted funding, compared to the 5 years with the highest enacted funding, the number of deaths in years where the requested funds were less than the enacted funds totaled 33. In contrast, the number of deaths in years where the requested funds were greater than the enacted funds was 82. This is well more than the twice the amount of casualties, and also indicates that deaths tend to increase with a funding shortfall. (The year 2002 was omitted in this calculation because enacted funds equaled requested funds.)

To summarize, hypothesis #1—that increased funding is correlated with fewer deaths in the same year—is supported ($r = -0.72$). Hypothesis #2—that a funding shortfall (requested compared to enacted funding) will correlate with more deaths—is somewhat supported ($r=0.48$). And hypothesis #3—that earlier years will have more deaths—is clearly not supported.

Conclusion

This study has identified two important correlations: a correlation between the amount of funds that are appropriated to ESCM and deaths resulting from attacks on U.S. diplomatic targets, and a correlation between funding shortfalls and death rates. It will be interesting to look at the numbers for 2013 as the DOS requested $1.614 billion in ESCM funding, a substantial increase.

While this study has explored some interesting issues and correlations, it would be difficult to say that the funds enacted (or not enacted) are a *cause* of the death rates, or *vice versa*. There are simply too many variables to isolate to make such a statement. Moreover, the sample size of this experiment, eleven years, is probably too small to predict long-term trends reliably. The political climate in foreign countries, world events, the economy, embassy closures, heightened security alerts, sporadic terrorist attacks how the funds for ESCM are specifically used, and which type of security features are the most effective for each region, and are all additional parameters that could and probably do impact these questions.

Acknowledgements

The editor suggested the use of the Pearson's linear coefficient, calculated the values, generated the graphs and table 2, and suggested that offsets of ±0-3 years be considered in the analysis.

References

Aaronson, T. (2013, September 3). Benghazi report details security flaws at US diplomatic posts.

Aljazeera America. Retrieved from http://america.aljazeera.com/articles/2013/9/3/-Exclusive benghazireportdetailssecurityflawsatusdiplomaticposts.html

Johnson, C.M. (2008, January). EMBASSY SECURITY Upgrades Have Enhanced Security, but Site Conditions Prevent Full Adherence to Standards. (GAO Report No. 08-162). Retrieved from Government Accountability Office website: http://www.gao.gov/new.items/d08162.pdf

Tiersky, A. (2013, September). *Securing U.S. Diplomatic Facilities and Personnel Abroad: Legislative and Executive Branch Initiatives.* (CRS Report No. R43195). Retrieved from Congressional Research Service website: http://www.fas.org/sgp/crs/row/R43195.pdf

Tiersky, A. & Epstein S.B. (2013, September). *Securing U.S. Diplomatic Facilities and Personnel Abroad: Background and Policy Issues*. (CRS Report No. R42834). Retrieved from Congressional Research Service website: http://www.fas.org/sgp/crs/row/R42834.pdf

United States. Department of State. *Department of State Budget in Brief*. Retrieved on October 8, 2013 from Department of State website: http://www.state.gov/s/d/rm/rls/bib/index.htm

United States. Department of State. Bureau of Diplomatic Security. (2013). *Significant Attacks against U.S. Facilities and Personnel*. Retrieved on October 11, 2013, from http://www.state.gov/documents/organization/211361.pdf

Viewpoint Paper

Why Fearing NORQ is Bad for Security*

Roger G. Johnston, Ph.D., CPP, Christopher N. Folk**, and Jon S. Warner, Ph.D.
Vulnerability Assessment Team
Argonne National Laboratory

Introduction

Security managers, security practitioners, and organizations involved in critical security applications often seem to have an irrational fear of Non-Objective, Non-Reproducible, and Non-Quantitative (NORQ) approaches to analyzing security. These NORQ approaches are subjective; don't always produce consistent, predictable, or identical results; and can be difficult to measure with metrics. While we would never argue that ORQ approaches (Objective, Reproducible, Quantitative) should be abandoned, they simply aren't sufficient alone for providing good security. Creative, imaginative, proactive analysis is also needed.

ORQ approaches include such techniques as security surveys, security audits, threat assessments, the CARVER Method, the Delphi Method, and Event/Fault Trees. While these primarily ORQ techniques have merit, they are simply inadequate. They do not usually uncover new security vulnerabilities or suggest countermeasures; get inside the heads of the adversaries or predict their behavior; or deal effectively with insider threats, security culture, organizational behavior, and other human factors that are the key to effective security. In practice, some of these techniques often confuse safety with security, threat assessments with vulnerability assessments, compliance with security, and control with security. They often lead to ignoring or under-protecting certain assets and organizational attributes. Certainly the supposed rigor, precision, and completeness often claimed or implied for these ORQ techniques are illusionary. All this leads to defective security.

The common idea among security managers, engineers, and bureaucrats that risk management for security can rely entirely on ORQ analysis is wrong. Effective risk management in any context has always required some degree of experience, subjective judgment, synthesis, prediction, and imagination.

Left vs. Right Brain

Scientific research has indicated that there is a *tendency* for certain cognitive brain functions to be supported more strongly on one hemisphere of the brain than the other. This is called brain lateralization. Typically (though there is much variability), the left

* This paper was not peer reviewed. A version of this paper first appeared in *Homeland Security Today* **11(4),** 39-41 (June/July 2014).

** Current address: Department of Psychology, University of Texas at Arlington.

hemisphere is thought to be the major player in language processing, mathematics, objective analysis, rule-following, and logical reasoning. The right hemisphere is often stronger in attention, sound processing, spatial manipulation, facial perception, artistic ability, creativity, intuition, processing of emotions, and synthesis of ideas. In practice, both hemispheres are heavily involved in all major mental activity.

While popular psychology has greatly exaggerated brain lateralization to the point of discrediting it, the concept still has some scientific validity if not overstated. More importantly, it is useful metaphor for differentiating between (so-called "left-brain dominated") thinking that is linear, logical, objective, quantitative, and reductionist, and ("right brain dominated") thinking that is imaginative, intuitive, and holistic, and also good at exploiting metaphors/analogies, identifying connections between ideas, and seeing "the big picture".

In this article, we roughly equate NORQ analysis with "right brain dominated" thinking, and ORQ with "left brain dominated" thinking.

In his 2005 book, "A Whole New Mind: Why Right-Brainers Will Rule the Future", Daniel H. Pink notes the reluctance that many organizations and "left brain dominated" thinkers (for example, engineers) have in accepting right-brain type thinking. (In our experience with many organizations and security professionals, "irrational fear" might be a more accurate term than "reluctance".) We certainly see a great deal of resistance to creative NORQ analysis in physical security and nuclear safeguards, especially for critical applications.

We believe one of the reasons that vulnerability assessments (VAs), particularly for physical security and nuclear safeguards, are often ignored or glossed over by security professionals, organizations, and security textbooks is that true VAs are basically creative NORQ exercises in thinking like the bad guys. Whereas assessing threats (who might attack with what resources), choosing what assets to protect, and deciding the security resources that will be fielded can be handled—at least with some effectiveness—using ORQ methods, this is not true for VAs

The common flawed objections raised about NORQ security approaches typically fall into these 5 categories:

Myth 1: Critical security applications are too important to be left to "flaky" creative analysis. Reality: Critical security applications are too important *not* to utilize all the tools available to us, especially powerful (though admittedly unpredictable) tools like NORQ analysis.

Myth 2: Right brain thinking won't yield the "right" answer. Reality: There usually is no one "right" answer. Security is a very difficult optimization problem involving many complex trade-offs and value judgments, and it usually has problematic metrics. Even if there were one "right" answer for security, there is usually no way to prove it is the "right"

answer. We need instead to focus on getting a good answer. NORQ analysis can help us with that.

Myth 3: Right brain thinking will lead to disagreements and controversies. Reality: That is one of the strengths of NORQ security analysis, not a weakness! Anything as important and difficult as security, with all its complex trade-offs, human factors, and value judgments, ought to be controversial. Disagreements help to clarify thinking. As General George S. Patton said, "If everybody is thinking alike, then nobody is thinking."

Myth 4: If I can't reproduce the results of our security analysis, they are of no use. Reality: Perhaps someday we will understand security and creative analysis well enough to be able to provide both effective *and* reproducible results. In the meantime, it is irresponsible not to take advantage of NORQ analysis (in conjunction with ORQ analysis) to help us improve security, even if NORQ analysis is somewhat uneven and unpredictable.

Myth 5: All the vulnerabilities won't be found with NORQ analysis. Reality: ORQ techniques won't find all the vulnerabilities, either, and are usually worse at it than NORQ methods. More to the point, it is not even possible to find all the vulnerabilities for a non-trivial security device, system, or program, no matter what techniques we use. Even if we could somehow find them all, it isn't generally possible to prove that we have done so.

Current NORQ Problems

These myths often prevent NORQ approaches from being tried in the first place. When NORQ security measures *are* deployed, they are often misleadingly dressed up to look like ORQ techniques. They are done under the cover of semi-quantitative, pseudo-scientific nonsense—lacking a solid scientific basis, meaningful independent review, rigorous analysis, and effective metrics. The polygraph is a classic example: a pseudo-scientific, semi-quantitative, sham-rigor technique that a 2002 National Academy of Sciences study called a threat to national security. (See http://www.nap.edu/books/0309084369/html/.) Numerous spies, insider attackers, and murderers have successfully passed polygraphs, often multiple times. Belief in the polygraph as a measure of *future* behavior is particularly dubious.

Another example of a questionable or badly executed NORQ technique based at least partially on sham-rigor is behavioral screening done by Transportation Security Administration (TSA) officials. After spending over $1 billion to implement such techniques at airports, both the DHS Inspector General and the General Accounting Office (GAO)—in 3 separate reports—slammed behavioral screening for having no significant scientific basis, failing to detect a single terrorist, and lacking adequate training, critical analysis, and meaningful metrics. Despite these criticisms, the TSA has expanded the program.

One of us (Johnston) has attended multiple presentations on behavioral observation "case studies" at national and international security conferences. The presentations

typically turn out to be anecdotes and "war stories", not discussions about rigorous case studies, analyses, or metrics. The argument that such results would be too sensitive to discuss publicly, even if they existed, is disingenuous. The argument that cops on the beat, Israeli security officials, and others have long used behavioral analysis (while true) is not a justification for implementing it in a haphazard, wasteful, amateurish, pseudo-scientific manner.

A third example of a NORQ technique with serious problems is background/integrity screening of personnel. While security clearances and background checks have arguably offered important security benefits, they have consistently failed to detect spies and insider attackers, including Snowden, Manning, and Ames. In a 2010 paper in *Information Forensics and Security*, Pfleeger, et al. concluded that "studies of espionage and white collar crime have failed to exhibit a correlation between personal attributes and malicious intent to do harm". Background checks are often discussed as if they were a thorough, formalistic, rigorous process, but in reality they are highly subjective—and could hardly be otherwise.

The common obsession with mental health in background checks seems especially questionable, given that the vast majority of spies and (non-violent) insider attackers are not mentally ill. Mental health is more appropriately a concern when preventing workplace violence is the primary concern.

Conclusion

Bottom line: We need to make more use of NORQ techniques for planning and analyzing security. We need to stop fearing them. But when we do deploy NORQ security measures, they should be carefully studied before relying on them, or spending massive sums of money in deploying them to the field. We also don't need to pretend that security measures and techniques that are fundamentally NORQ in nature are ORQ.

Despite their right-brain nature, NORQ security measures must still be implemented in a thoughtful, logical, rigorous, research-based manner with plenty of independent, critical reviews and meaningful evaluative metrics. "NORQ" should not mean the same thing as "non-rigorous" or "Security Theater".

Acknowledgments

This work was supported by the U.S. Department of Energy, Office of Basic Sciences, under contract #DE-AC02-06CH11357. The views expressed in this article are those of the authors and should not necessarily be ascribed to Argonne National Laboratory or the United States Department of Energy.

Viewpoint Paper

Is Physical Security a Real Field?*

Roger G. Johnston, Ph.D., CPP and Jon S. Warner, Ph.D.
Vulnerability Assessment Team
Argonne National Laboratory
http://www.ne.anl.gov/capabilities/vat

With a 10,000+ year history and many tens of thousands of practitioners, it may seem odd to maintain—in a journal devoted to physical security no less!—that physical security isn't a real field. But in many ways, it's not.

We define physical security as measures taken to protect *tangible* physical assets (people, buildings, money, drugs, museum artifacts, etc.) from harm. But physical security also involves deploying corporeal means (access control devices, guards, fences, etc.) to protect *intangible* assets (intellectual property, PII, sensitive information, digital data, etc.).

In a real field—think physics, anthropology, or business for example—there are usually a plethora of fundamental principles, experimental and case studies, and models/theories that make specific predictions that can be tested. There are a wide range of available metrics, meaningful standards, licenses and certifications, rigor, ongoing debates and controversies, critical thinking, and creativity. Snake oil, product hype, misleading claims, and charlatanism, while unavoidably present, tend to get weeded out fairly reliably. Committees, groupthink, and linear/concrete thinkers don't dominate the field.

It would not be fair or accurate to say that physical security totally lacks these attributes, but it clearly has far less than the much newer field of cyber security, for example (not to even mention a field like medicine).

Continuing our comparison with cyber security, where are the degrees in physical security from major 4-year research universities? Try calling up your closest flagship university and ask for the people who work on cyber security. You may be connected with any number of departments doing cyber security research: computer science, mathematics, the IT department, electrical engineering, the business school, etc. Ask instead for the people dealing with physical security and you are likely to put in touch with the folks who arrest drunken frat boys.

Certainly some undergraduate and graduate degrees touch on physical security: degrees in homeland security, criminology, or forensics, for example. But the first is often more about public administration or management than physical security, the second may utilize

* This paper was not peer reviewed. A version of it first appeared in *Security* **51**(5), 28-30 (2014).

physical security but isn't primarily devoted to studying it, and the third is fairly far afield.

And where is the research and development (R&D)? There are many national and international conferences where *cyber security* researchers go to discuss their theories, mathematical models, controlled experiments, double blind tests, and rigorous case studies. Most conferences devoted to physical security, on the other hand, primarily entail seasoned security practitioners sharing the "war stories" and vague generalizations about what they have learned over the years.

Table 1 hints at the lack of physical security R&D. It shows the number of peer-reviewed journals devoted to various fields. Physical security falls far short of other "fields", including the totally bogus "field" of astrology! (Note that there are a number of excellent trade journals that include coverage of physical security, but these are not peer reviewed and usually not devoted to just physical security.)

Table 1 - The approximate number of peer-reviewed journals dedicated to various "fields". Caveats: There may be more peer-reviewed journals than we were able to find (especially in languages other than English), but the table shows at least the minimum number. Note that some peer-reviewed journals count in multiple fields, e.g., the *Journal of Hospitality, Leisure, Sport & Tourism Education*. A larger number of peer-reviewed journals than shown here may occasionally *accept* papers in a given field, but aren't primarily *dedicated* to that field. Trade journals (typically not peer reviewed) are not included in the table.

"Field"	peer-reviewed journals
Tourism	29
Cyber/IT Security	19
Hospitality Industry	18
Recreation & Leisure	15
Criminality & Law Enforcement[1]	10
Astrology[2]	7
Transportation Security	4
Cryptography	2
Physical Security[3]	1

[1]Excludes journals devoted to medical forensics.
[2]Not a legitimate field!
[3]Excludes journals devoted to nuclear safeguards. The one peer reviewed journal devoted to physical security was started by the authors (http://jps.anl.gov).

Some people might maintain that physical security is a trade, not something that can be studied in a rigorous or scholarly manner. We disagree. Medicine and Hotel/Motel Management are also trades, but both fields have large amounts of very active and quite rigorous research efforts. In comparison with cyber security (which is a real field and has

loads of rigorous R&D), physical security is more multidisciplinary, multidimensional, and complex. Physical security is also more important. When physical security fails, people may die. When cyber security fails, we lose some ones and zeros.

So, what is to be done? We believe we need more emphasis on rigor, R&D, and physical security education. We need more physical security R&D conferences, and more scholarly peer-reviewed journals devoted to physical security. Importantly, we also need more authors/speakers willing to write/talk about their models, theories, analyzes, controlled experiments, speculations, and case studies. We need this from both technical and social science specialists.

Ultimately, we need to start thinking about physical security as something that can be a highly scholarly research subject, interesting not just for its practical applications, but because it is a fundamentally fascinating field for study. Perhaps with more rigor, scholarship, and R&D, we can have more effective physical security; as vulnerability assessors, we find remarkably poor practices and hardware on a regular basis, including for very critical security applications.

Acknowledgments

This work was supported by the U.S. Department of Energy, Office of Basic Sciences, under contract #DE-AC02-06CH11357. The views expressed in this article are those of the authors and should not necessarily be ascribed to Argonne National Laboratory or the United States Department of Energy.

About the Authors

Roger Johnston, Ph.D., CPP and Jon Warner, Ph.D. are with the Vulnerability Assessment Team (VAT) at Argonne National Laboratory (http://www.ne.anl.gov/capabilities/vat). The VAT has provided consulting, training, vulnerability assessments, R&D, and security solutions for over 50 government agencies and private companies.

Performance-Based Approach to the Security of Radioactive Sealed Sources*:* A Canadian Perspective

Raphaël Duguay, M.Sc., PSP
Nuclear Security Division
Canadian Nuclear Safety Commission, Canada
raphael.duguay@cnsc-ccsn.gc.ca

Abstract

In 2013, the Canadian Nuclear Safety Commission (CNSC) published a regulatory document *REGDOC 2.12.3* to enhance the security of radioactive sealed sources in Canada. This regulatory document is based on the security recommendations of the International Atomic Energy Agency's *Code of Conduct on the Safety and Security of Radioactive Sources* and related documents in the *Nuclear Security* series, and follows a risk-based approach using a performance-based regulatory framework. This paper provides the reader with a Canadian perspective on the security of radioactive sealed sources, and a reflection on those security measures and practices that have proven to work effectively, as well as those that look promising from a security management and physical protection standpoint.

Note on Terminology: In this paper, the term "performance-based" means focusing on setting a goal (or an objective) without proposing any specific means to achieve it. Also, the term "radioactive source security" is used in relation to a physical protection program that includes technical and administrative security measures and practices to prevent the theft, loss, or sabotage of radioactive sources that could be used for malicious purposes. It does not include import and export controls, or safety measures used for radiation protection, detection instruments, or emergency response.

Background

After the terrorist attacks of September 11, 2001, the CNSC adopted a strategy to enhance physical protection of nuclear facilities throughout Canada and in particular high-security sites. The CNSC Nuclear Security Division was expanded to include a group of security specialists mandated to conduct field inspections at those licensee facilities authorized to possess high-risk radioactive sealed sources. Due to the absence of specific security regulations for radioactive sealed sources, the CNSC used a performance-based approach, and worked closely with industry and licensees, to identify potential vulnerabilities in their physical protection systems and explore solutions to reduce risks. (One example: device hardening to increase the adversary's efforts, increasing the adversary's risk of being apprehended by enhancing security detection and assessment systems, and/or extending patrols and surveillance).

Performance-based regulatory approach

In 2006, the CNSC began developing a regulatory document[1] for the security of radioactive sealed sources, based on the International Atomic Energy Agency's (IAEA) *Code of Conduct on the Safety and Security of Radioactive Sources.* The purpose of this regulatory document is to prevent the loss, sabotage, illegal use, illegal possession, or illegal removal of radioactive sealed sources while stored at an authorized location or during transport. The adopted regulatory approach includes both prescriptive and performance-based language. In addition, this document identifies a clear objective and the criteria to achieve compliance, and provides guidance to licensees to assist them in finding appropriate security solutions, commensurate with the category of their radioactive sealed source (based on the IAEA *Categorization of Radioactive Sources* and the associated security level). For example, a performance-based requirement states that "the licensee must implement a means to detect unauthorized access", but does not specify the means (which can rely on either human activity or electronic measures).

It is my opinion that the performance-based approach permits implementation of security measures providing the licensee and the regulator with flexibility in the manner in which they seek to meet international standards for source security/protection. In the initial phase, the approach consisted of setting applicable security objectives and focusing on the end-result—or the effectiveness—of the process. Many Canadian licensees did not possess the necessary technical security expertise and there was limited guidance, so security specialists from the CNSC were utilized to help identify effective and acceptable solutions. After the initial inspections and the implementation of additional security measures, the licensees gained sufficient experience to implement solutions (specific to their operations and locations) to meet the regulatory requirements. In the initial phase, the focus was primarily on high-risk radioactive sealed sources. This approach was developed to allow flexibility for the licensees and the industry as a whole, recognizing that "one size does not fit all" when implementing security measures. The strategy allows the licensees to: gain knowledge and experience by developing their security program; and take different initiatives to achieve compliance without compromising safety or security.

Canadian approach: A mix of performance-based and prescriptive regulatory requirements

The Canadian model for the regulatory documentation concerning the security of radioactive sources is based on the security recommendations of the IAEA *Code of Conduct on the Safety and Security of Radioactive Sources* and IAEA Nuclear Security Series. During the development of this document, CNSC staff consulted other government agencies responsible for regulating dangerous goods (such as explosives, biohazards and chemicals agents). CNSC also consulted other countries, to ensure the alignment of security requirements and avoid regulatory conflicts (which may impede the trade and transportation of radioactive sealed sources across borders).

[1] REGDOC 2.12.3, *Security of Nuclear Substances: Sealed Sources* (2013).

As a result, a performance-based approach was implemented for security measures during the entire lifecycle from their manufacture until their safe disposal including while they are in storage and/or transport. In some areas, the CNSC used more prescriptive language to identify minimum requirements to prevent inadequate measures (e.g., retention of training records, testing frequency of alarm systems, site security plans, arrangements with offsite responders, and conducting trustworthiness and reliability verifications).

Operational experience: What works?

Performance-based inspections and associated compliance activities

It is my opinion that security inspections focused on performance, allowing both the regulator and the licensee to assess the effectiveness of a physical protection system and its vulnerabilities, have considerable merit. For example, during an inspection, the inspector may ask the licensee to test the intrusion detection system at the site where the radioactive sealed source is stored, in order to collect information on the time taken for detection, assessment, delay and response. At this stage, the devices or process vulnerabilities will be reviewed and tested to see if they compromise the overall objective of the security system.

Facility security plans are another example where feedback and comments from the regulator proved beneficial to the licensee. Although it may appear to be prescriptive in nature (because it is usually included as part of a license condition or a regulatory requirement), the responsibility in the development and implementation of this document belongs to the licensees. The consultation process is another instance where the regulator may help the licensee identify areas of improvement, and avoid non-compliance during inspections. This is particularly beneficial for licensees who submit security system designs and plans for specialists from the regulator on whether the proposed design meets the security requirements. During the site security plans reviews, it is possible to identify gaps related to mandatory requirements and missing information that support the security program. For example, missing information on the frequency of security devices maintenance and security awareness training should be documented to provide records that they are being implemented and maintained in accordance with requirements.

Working with the industry associations and licensees

It is my experience that some licensees lack security experts or have limited knowledge of physical security systems. Security specialists from the regulatory body are available to provide additional assistance and support in identifying vulnerabilities, as well as options to mitigate risks and meet requirements.

Security specialists are also involved at the construction phase of a new license facility (i.e., new build) or when a licensee is relocating or opening a temporary job site to a new location. In these instances, security advisors assist the licensees (or contractor) to identify the appropriate security measures that must be implemented before the site is ready to possess the radioactive sealed source. This approach often results in licensees saving on

expenses related to physical security enhancements that were not included in the initial budget.

During the development of this regulatory document, industry was consulted extensively, and encouraged to take proactive steps to address the updated security objectives. CNSC security advisors also met with licensees, to assist them in finding solutions that met the regulatory expectations. This experience has proven to be very effective in establishing strong communications and good relations with the licensees.

New licensees can also contact CNSC's security advisors to get an understanding of the requirements and to obtain clarification on the *Nuclear Security Regulations* and the CNSC expectations. In some cases, the CNSC provided assistance to the licensees in establishing contact with the appropriate local law enforcement authorities to facilitate the exchange of information and development of response arrangements to security incidents.

Case Studies: Communicating with the industry

Oil well logging and radiography companies occasionally work in remote locations, with a reduced presence of law-enforcement agencies and security contractors. In such situations, security systems can be expensive, and certain technologies may be unavailable. Following consultations with the regulator, some companies implemented equivalent security procedures (such as the "two-person rule", constant human surveillance, improved communication practices) to maintain control of the source during operations. The intent is to avoid unreasonable costs and implement a balanced solution, which still meets security requirements.

The consultation process was transparent and open for public comment. During the process, the industry asked for additional guidance on criminal record name checks (CRNC). The regulator provided more detail and suggested reliable CRNC alternatives. This flexibility allows the licensees to save on costs and avoid duplication on rules and requirements coming from different regulatory agencies. For example, a Canadian firearm acquisition license requires a thorough background verification, which is completed by a law-enforcement agency and can be used as a CRNC equivalent.

What's promising?

Threat and risk assessment, adversary pathway analysis and security self-assessment

In collaboration with the CNSC, some members of industry conducted security self-assessments, adversary pathway analyses, and/or threat and risk assessments specific to their site or activity. These assessments are recognized as good practices[2] as they helped the licensees identify potential threats and vulnerabilities specific to their sites. It is my

[2] The World Institute of Nuclear Security (WINS) has developed a series of Best Practices documents that also encourage the use of self-assessment methodologies to identify gaps and weakness in a security program.

opinion that this approach allows the licensees to implement reasonable security measures, commensurate with the level of risk associated with their licensed facility.

Unannounced performance testing of security systems, procedures and personnel

It is my experience that some licensees have taken a proactive stance, by implementing more thorough unannounced verification to ensure the readiness of systems, processes and personnel. This practice is a very effective tool in identifying vulnerabilities in physical security systems, access control, and other internal processes and procedures. In other cases, the licensees conducted performance testing of their security equipment and response personnel, to ensure timely detection, assessment and response, without having any operational impact on the site.

Involving management and other stakeholders in security

In some cases, licensees have created special security committees for the protection and management of radioactive materials at their site. These committees were also responsible for addressing security issues related to information technology, transport, trustworthiness and verification, training, workplace violence, personnel, etc.

One medical facility licensee created a multi-disciplinary team (including personnel designated for radiation safety, security, fire safety, a medical treatment team and a building manager) to ensure that all necessary considerations are taken into account when implementing security upgrades. It is my opinion that this integrated approach to security, which also involved management, was an adequate means to manage risks and to promote workplace safety and security culture.

Security awareness training and promoting security culture

To ensure effective and regular training, most public facilities have included security awareness in the mandatory annual safety and radiation protection training. To ensure compliance and good practices, security awareness is now integrated into a mandatory refresher training courses and safety manuals, and is provided to onsite security personnel. In some cases, members of the local law enforcement agencies were invited to a familiarization tour of the site and to get basic security and safety training.

Some licensees are quite innovative in using social media and communication tools. One licensee, for example, published a monthly security bulletin and was very proactive by doing fund raising for non-profit organizations in parallel with security awareness activities. To motivate its employees and increase worker participation, the licensee distributed security quizzes and rewarded the best participants with prizes. The employee participation in these events was strong, and provided an excellent opportunity to improve the security culture and raise funds for a good cause.

International efforts

Several international initiatives are being implemented by the IAEA to increase security awareness and training of individuals involved in the security of radioactive sealed sources. Canada has taken part in these efforts, for example, by providing early support and assistance both domestically and to international partners. These global initiatives provide

excellent opportunities for exchanging information on best practices, as well as for conducting professional networking.

Learning from best safety practices

The Canadian nuclear industry has training programs on safety and radiation protection as part of mandatory requirements. When new security requirements were implemented, they were also integrated into the licensee training program. Some licensees already followed stringent inventory control measures and security verifications that were easy to implement. For transportation security, the containers' safety design (such as shielding, weight, size) already included robust security features, which are difficult to defeat and provide additional level of security.

Challenges

- Identifying roles and responsibilities: because of the multiple licensees' representatives, it is at times difficult to define specific roles and responsibilities and to identify who is responsible for the security of radioactive sealed sources.

- Potential for duplication: because of multiple requirements from various regulators, it is important to avoid duplication with other government agencies, resulting in unnecessary financial burdens and costs to the industry.

- Finance/Cost: Some licensees have difficulty finding the financial means to enhance physical security. It was important to address "operational needs" and to implement reasonable measures to assist the operator in meeting requirements without imposing a financial burden and without impeding their core operations (i.e. hospital environment). However, the licensee must implement compensatory measures if they are not meeting the requirements.

- Public and semi-private facilities: Facilities that are open to the public pose particular security challenges. For instance, universities and hospitals have more difficulties in implementing surveillance, access control measures and in identifying and assigning responsibility for security and response. As such, it is important to work with the licensee, to establish good security practices and promote an effective security culture. These facilities are considered to be "soft targets", and controlling access and conducting trustworthiness and reliability verifications for students, foreign researchers or third-party service providers may be a challenge. In addition, medical facilities need to balance security with patient safety, patient privacy and movement of sources within the facility.

- Remote locations: Response times of law-enforcement agencies are longer when high-risk sealed sources are transported and/or stored in remote locations. The effectiveness of security technologies for detection and assessment may also be challenged by the location's geographical features and/or inclement weather conditions.

- Safety/Security: One of the biggest challenges was to ensure that security controls did not adversely affect safety measures and practices and vice-versa. Through experience and case studies, the CNSC identified several potential conflicts between safety and security, and worked toward finding balanced solutions, to ensure both of these were properly addressed.

- Sustainability/Security Culture: Continuous security awareness and promoting a sustainable security culture continues to be a challenge, particularly when it comes to protecting radioactive sealed sources against malicious use. Some licensees see security as an unwarranted expense against non existent threats, or assume that their remote location provides sufficient protection. Promoting continuous security awareness and a proper sustainable security culture continues to be a challenge.

It is the my opinion that despite the challenges of implementing security enhancements and developing a robust security program, working in collaboration within industry allows everyone to achieve the same goal and enhance the security of all radioactive sealed sources.

Lessons learned and recommendations

It is my opinion that:

- It is important to work closely with the industry and licensees to design and implement effective security measures. It is also important to address their concerns and questions, and share best practices in the field. For example, CNSC-sponsored workshops on industrial radiography are held annually, to discuss licensing and compliance expectations and current issues related to this field of activity. The regulator also publishes information bulletins, to promote awareness and exchange of information. It was also noted during field inspections and desktop reviews that the compliance rates were higher when the licensees were engaged in an outreach activity or another form of communication with the CNSC.

- Regulatory compliance verifications and performance-based inspections related to radioactive source security are now routinely conducted by safety inspectors. Safety inspectors receive basic training on security measures and regulatory requirements. In general, the first initial security assessment is conducted by a security expert for every new location or new operating licence. Safety inspectors conduct follow-up field inspections and unannounced verifications to ensure that the licensee has an effective safety and security program which meets all the regulatory requirements. This approach may prove to be more sustainable in the long-term, but requires cooperation, planning, structure, and routine security-awareness training for safety inspectors.

- Although Category 1, 2 and 3 radioactive sealed sources[3] are considered to be the most dangerous, it is important to ensure good security and prudent management practices for low or very low-risk radioactive sources (category 4 and 5). This is the approach taken during the security awareness training provided to inspectors from the CNSC, as well as in the regulatory documents that provide requirements and/or guidance to licensees.

- Guidance documents should be more specific for different source use types, and provide more details to licensees. For example, a licensee in the medical sector should have access to guidance documents and technical references that can help them implement, design and maintain a security program to protect their radioactive sealed sources. These can have multiple applications and some may pose unique challenges including; radiation protection, patient safety, or mobile sources.

[3] International Atomic Energy Agency (IAEA) Categorization of radioactive sources, IAEA TECDOC-1344, July 2003.

Support for Victims of Crime in Lagos, Nigeria

Ayodele, Johnson Oluwole

Department of Sociology, Lagos State University, Lagos, Nigeria
johnson.ayodele@lasu.edu.ng

Abstract

Following criminal attacks, victims require support to regain the control of their destinies. Yet, support for distressed community members is often inadequate. This study examines the level of support that victims of crime enjoy in Lagos, Nigeria. Both qualitative and quantitative methods were used. The study covers the three senatorial districts in Lagos using data obtained from 948 respondents selected through a multistage sampling procedure. A total of 6 in-depth interviews, 12 key informant interviews, and 10 case studies provided complementary qualitative data. Data analysis involved the use of simple percentages, chi square, regression, and content analysis.

The findings indicate that 75% of the respondents judged the level of support available to crime victims in their community as very poor. While chi square analysis showed that the amount of support a crime victim receives is significantly correlated with place of residence and gender, there is little correlation between the support a crime victim receives and his/her age or education.

This study concludes that the influence of imported values has eclipsed traditional care for victims, estranged youths from their extended family networks, and exposed victims to undue neglect. The study suggests the need for community-based support networks to resuscitate African values, and strengthen them to reconnect community members with crime victims through empowerment. This is a promising way to provide accessible humanitarian assistance for victims of crime, reduce their trauma in the aftermath of crime, and accelerate their recovery from crime-induced tragedies.

Keywords: Crime Victims, Family Values, Support, Lagos, Nigeria

Introduction

In Africa, the moment security measures fail to protect victims from attack and the offender is apprehended, he/she is made to atone for his/her crime through punishment. The integrity of the punitive process has positive therapeutic implications for the victim as well as his/her recovery from the pain of crime. It is for this reason that punishment is tied to justice. Thus, tradition favors victim support on the grounds that the offender injured the victim, not the nebulous modern state which, nevertheless, often takes all the economic benefits of prosecution in the course of criminal justice. It is against this background that punishment is intricately linked with victim support so as to reinforce the high value placed on human life in African traditional communities.

In some peculiar instances, it has been historically permissible to kill an enemy, just as is the case today. In all other situations, taking another person's life is unacceptable. In fact, no distinction has been made historically in Africa between murder and manslaughter; both were considered murder. Murder was punished according to the principle of compensation.[1] The essence of this principle was that if one man injures another, he should compensate for the injury rather than being merely punished for doing it. This meant that although nothing could be done for a murdered man, his associated group could be compensated.[2]

Among the southern Agikuyu, Leakey [3] observed that the criminal fine was the same for any death, regardless of whether the death was caused accidentally or intentionally. Thus, if a male was killed by a member of another family, whatever the age, the standard fine was 100 goats and sheep.[3] This fine was paid to the family of the deceased by the family of the killer. Among the Akamba, the murder of a man was compensated for by the payment of 12 cattle (11 cows and one bull) or 14 cattle (13 cows and one bull), depending on location. The murder of a woman was compensated by payment of 4-5 cows and one bull or by the payment of 8 cattle (7 cows and one bull), depending on location.[4] Among the southern Agikuyu, the family of the deceased was paid 30 goats and sheep. If the deceased happened to be a married woman, 25 of these animals were paid to the family into which she was married and the remaining five were paid to her brother.[3]

Among the Akamba, adultery was a crime punishable by a fine of a bull and a goat. The goat was killed and used in cleansing the husband of the offending wife before he got back to his house.[4] The fine was much higher if an adulterous wife died in childbirth. In this case, the paramour had to pay 5 cows and one bull. The community insisted on this deterrent fine because the responsibility of the woman's death was considered to lie with the offending man.[4] Among the southern Agikuyu, in contrast, the adulterer was fined 3 stall-fed rams, which he paid to the council of elders. The offender was also made to produce a small ram or he-goat, and he took a *muuma* (oath) that he would never again visit that woman, and that he would never again commit adultery with any other woman.[5] Among the Pokot of Baringo, an adulterous man was punished physically and materially. The man was first tied to a tree in which stinging ants resided. The ants were then disturbed and as they stung him, he was beaten as his 'lover' watched. After this, he

was fined 6 cows, 6 goats, a pregnant sheep, and six ostrich feathers. In addition, he prepared a tin of honey with which to appease the offended husband.[6]

Support for crime victims is far from universal. Statistics indicate, for example, that of an estimated one million victims of crime in Scotland each year, only about 175,000 receive any kind of support.[12] Even when support is provided, the research literature on social ties has long recognized that the community and social contacts can be unsupportive as well as supportive.[8] Individuals close to victims may feel threatened by the victim's affliction, people may be uncertain about how they ought to react to victims because they have little experience to guide them, or people may not understand what is and is not appropriate to say and do.[9-10] The idea that social ties can have negative effects has been emphasised by researchers looking at people's reactions to victims of serious physical, emotional, and financial pains.[11-12] Unsupportive behavior can include withdrawal, criticism, ineffective help, or inappropriate help.[13-14]

To avoid behavior that is unsupportive of victims of crime in Africa, children are traditionally socialized to establish empathy with crime victims. Through appreciation and condemnation, children grow up distinguishing between legitimately appropriate support, and support withheld or offered unenthusiastically. The idea is to inculcate in the minds of young Africans the virtue of support for neighborly coexistence. It is therefore not surprising that in adulthood, individuals found not showing desirable empathy with victims are looked at as nonconformists. Any society that aspires to meet the needs of its citizens, deal with serious social problems, and avoid violent conflict must address these issues.[15] It is against this background that this study examines victim support in Lagos, Nigeria by addressing the following questions: (1) What *level* of support is available for victims of crime in the community? (2) What *kind* of support is available to victims in the study site? (3) What is the *quality* of the support available for victims of crime in the study site?

Data and Methods

This study focuses on Lagos State in the Southwest geopolitical zone of Nigeria. Crime is a serious problem there.[16] Fully 67% of Lagos residents report fear of becoming victims of crime, and 23% claimed to have experienced crime. The official crime rate in Lagos has increased from 12% of citizens in 2011 to 21% in 2012. The most prevalent crimes are robbery (28% of all crime) and theft (17% of all crime).

This study was based on both quantitative and qualitative data. The main source of primary quantitative data was a questionnaire administered to 948 respondents who were selected through a multi-stage sampling procedure. Qualitative data were obtained via in-depth interviews with 3 traditional rulers and 3 religious leaders selected equally from each of the three Senatorial Districts, as well as interviews with 3 Divisional Crime Police Officers, 3 Chairmen of Landlord Associations, and 6 Members of Victims' Family. There were also 10 case studies conducted with victims of serious crimes that provided complementary qualitative data for the study.

A multistage sampling technique was used to select respondents, purposefully for the study site (Lagos), and randomly for the local government areas in urban, semi-urban, and rural communities of Lagos. In the first stage, a simple random sampling technique was used to select 1 local government area (LGA) from each of the 3 senatorial districts, giving a total of 3 LGAs. In the second stage, based on prior research findings, areas recognized as the "black spots" of crime in Lagos in each of the 3 selected LGAs were randomly selected. In stage three, all 13 wards in Mushin LGA were included, 10 of the wards from Lagos Island LGA were randomly selected, and 5 wards were randomly selected from Ibeju Lekki LGA to reflect population differences in the randomly selected LGAs.

In the final stage, from each of the 13 and 8 political wards that were randomly selected from Mushin and Lagos Island LGAs, 2 streets were selected randomly. From the 5 political wards that were randomly selected from Ibeju Lekki LGA, 2 communities were randomly selected. Overall, 42 streets and 10 communities were randomly selected. One household was randomly selected from each of the selected 20 houses, making 520 houses from Mushin LGA, 320 houses from Lagos Island LGA, and 200 houses from Ibeju Lekki LGA. The sum of these equals 1040 houses. However, in a case where more than one family occupied a house, a lottery method (yes/no) was used to select the respondent interviewed. Copies of a questionnaire were given to the heads of each of the each of the 1040 households.

The data analysis involved both quantitative and qualitative approaches, which complemented each other. A univariate analysis used frequency counts and simple percentages to characterize data. Bivariate analysis involved cross tabulation and the use of inferential statistics such as the chi square test to establish association between variables. All these were processed through the Statistical Package for Social Sciences (SPSS 20.0 Version). For qualitative data, raw data from in-depth interviews, key informant interviews and case studies were transcribed, sorted, and labeled. However, verbatim quotations, ethnographic summaries, and content analysis were used to enrich quantitative data.

The study area was chosen based on its level of urbanisation and diversity. Lagos derives its demographic significance from being a premier city with considerable social, political and economic functions. It has a population of 17.5 million. This figure, however, is disputed by the Nigerian government and judged to be unreliable by the National Population Commission of Nigeria.[17] The UN estimated Lagos's population as 11.2 million in 2011. The New York Times estimates that the population of Lagos is now 21 million, surpassing Cairo as Africa's largest city.[18]

It is clear that whatever the size, and however the city is defined, Lagos is the center of one of the largest urban areas in the world. With a population of perhaps 1.4 million as recently as 1970, its growth has been stupendous. Rice estimates that Lagos generates about a quarter of Nigeria's total gross domestic product. It is the center of Nigeria's modern economy, is the most industrialized city in the country, and is home to many millionaires. Despite all of this, approximately two thirds of the population of Lagos are slum dwellers.[19]

Results

Demographics

Table 1 summarizes the selected socio-demographic characteristics of the respondents. Subjects included 66.1% male and 33.9% female respondents. The proportion of male to female has implications for the kind of support required by, and appropriate for, the victims of crime in the study site. Female victims appear to be more culturally assumed to need support as victims than their male counterparts. In some important ways, age also affects the access of victims to support in Lagos communities. In this study, a 10-year age grouping was used. The age patterns of respondents indicated that only 1.9% of respondents were less than 20 years old; about 61.0% of the respondents were between 21 and 40 years old. Individuals within these age brackets were assumed to be more actively involved in regular and gainful employment, which may make them less in need of support after a crime than those younger or older.

The data indicate that only 8.1% of the respondents did not have the advantage of formal education at all, while 61.2% had tertiary education. Data on marital status of respondents revealed that 46.5% of respondents are single, 44.6% are married, and 8.9% are separated, divorced, or widowed. A total of 68.7% of the respondents were Yoruba, 20.6% were Ibo, and 10.8% were other ethnic groups. Religious affiliation of the respondents showed that Christians constituted 56.3%, Muslims 42,7%, and indigenous religions 0.9%. In terms of the respondents' residence, 54.4% lived in semi-urban areas, 38.6% in urban areas, and 7.0% in rural communities of Lagos. The income distribution of the respondents showed that the majority (53.0%) earned an annual income of N10, 000,001 ($61,728.4), while 23.1% earned less than N2,000,000 ($12,346). The distribution of occupations showed that respondents engaged in various occupational activities such as business (61.7%), students (19.6%), civil servants (11.1%), and others (7.6%).

A female interview respondent looked at victim support essentially from the perspective of ethnicity and concluded:

> *One could merit a better support as a victim if one is victimised in one's locality. Without the necessary cultural network, there can be no accessible support in a multicultural society such as Nigeria. In Nigeria, as yet, policy makers have not come up with any structured national plan to see crime victims as not just victims of circumstance but victims of state negligence. If a citizen defaults in tax payment, tax collectors go after him. Ultimately, he is compelled to pay the tax and other incidental additions as fines. Regrettably, however, when state negligence causes a citizen to be attacked, nobody gets blamed. If the truth about equity and social justice must be told, the time when the state is held vicariously liable for undue victimization of citizens has come.*

Table 1 - Socio-Demographic statistics for participants in this study.

Variable	Frequency	Percentage
Gender		
Male	627	66.1
Female	321	33.9
Total	948	100
Age		
Less than 20 years	18	1.9
21 – 30	423	33.2
31 – 40	264	27.8
41 – 50	135	14.2
51 and above	108	11.4
Total	948	100
Education		
No Formal Education	77	8.1
Primary Education	99	10.4
Secondary Education	192	20.3
Tertiary Education	580	61.2
Total	948	100
Marital Status		
Single	441	46.5
Married	423	44.6
Separated/Divorced/Widowed	84	8.9
Total	948	100
Ethnicity		
Ibo	195	20.6
Yoruba	651	68.7
Others	102	10.8
Total	948	100
Religion		
Christianity	534	56.3
Islam	405	42.7
Traditional/Others	9	0.9
Total	948	100
Residence		
Urban	366	38.6
Semi urban	516	54.4
Rural	66	7.0
Total	948	100
Occupation		
Civil Servant	105	11.1
Business Person	585	61.7
Student	186	19.6
Other	72	7.6
Total	948	100
Annual Income In Naira		
Less than N 2,000,000	219	23.1
N 2,000,001 – N 4,000,000	69	7.3
N 4,000,001 – N 6,000,000	30	3.2
N 6,000,001 – N 8,000,000	74	7.8
N 8,000,001 – N 10,000,000	54	5.7
N 10,000,001 and above	502	53.0
Total	948	100.0

Victims and Support

This section discusses the amount of support which crime victims in our study reported receiving. Both qualitative and quantitative data were gathered to characterize the interwoven experiences.

Table 2 shows the proportion of crime victims who got support in the communities of Lagos.

Male victims had slightly greater access (64.1%) to support in the aftermath of criminal victimization than their female counterparts (61.7%), but chi square analysis shows that gender is not significantly correlated to access [X^2 p value = (.462) > 0.05]. Respondents whose ages fell between 31 and 40 years had the greatest access to support, while those between 61 and 70 had the least access. Chi square used to analyse the relationship between age and access to support indicates there is no significant relationship between the two variables: [X^2 p value = (.885) > 0.05]. Chi square analysis indicated that there is no significant relationship between education and access to support in the community [X^2 p value = (.943) > 0.05].

On the support situation in the study site, a 65-year old male in-depth interview respondent was concerned about the display of inconsideration of man to man, contrary to normative compassion that Africans are known to show to their neighbors in times of tragedy:

> *Africans are famous for their culture of brotherliness. Everyone is his brother's keeper. At what point did self-centeredness creep into African ways of life that people no longer care about fundamental African values? It is high time policy makers used traditional African belief system in respect of welfare as foundation of support for victims of crime. Not until the philosophy of an injury to one is seen as an injury to all is adopted as the focus of our welfare agenda, a community driven concern for victims of crime will elude vulnerable members of the community.*

Chi square analysis shows that religion is not significantly related to access to support in the study site: [X^2 p value = (.995) > 0.05]. Semi-urban respondents had more access to support (63.7%) than rural respondents (63.6%) and urban counterparts (53.7%). Chi square analysis shows that there is no significant relationship between respondents' places of residence and their access to support: [X^2 p value = (.977) > 0.05]. Yoruba respondents (64.7%) had more access to support than Ibo respondents (61.0%) and others (58.8%). However, chi square analysis shows that ethnicity is not significantly correlated with access to support in the study site [X^2 p value = (.399) > 0.05].

Table 2 - Support received by victims.

Variables	Respondents' Reporting Support					
	Yes		No		Total	
	N	%	N	%	N	%
Gender						
Male	(402)	64.1	(225)	35.9	(627)	100
Female	(198)	61.7	(123)	38.3	(321)	100
Total	(600)	63.3	(348)	36.7	(948)	100
	X^2 p value = (.462) > 0.05					
Age						
less than 20 yrs	(11)	61.1	(7)	38.9	(18)	100
21-30	(266)	62.9	(157)	37.1	(423)	100
31-40	(171)	64.8	(93)	35.2	(264)	100
41-50	(86)	63.7	(49)	36.3	(135)	100
51-60	(34)	63.0	(20)	37.0	(54)	100
61-70	(23)	54.8	(19)	45.2	(42)	100
71 years and above	(9)	75.0	(3)	25.0	(12)	100
Total	(600)	63.3	(348)	36.7	(948)	100
	X^2 p value = (.885) > 0.05					
Education						
No education	(28)	62.2	(17)	37.8	(45)	100
Primary education	(65)	65.7	(34)	34.3	(99)	100
Secondary education	(123)	64.1	(69)	35.9	(192)	100
Poly & University education	(384)	62.7	(228)	37.3	(612)	100
Total	(600)	63.3	(348)	36.7	(948)	100
	X^2 p value = (.943) > 0.05					
Religion						
Christianity	(339)	63.5	(195)	36.5	(534)	100
Islam	(225)	63.0	(150)	37.0	(405)	100
Traditional	(4)	66.7	(2)	33.3	(6)	100
Others	(2)	66.7	(1)	33.3	(3)	100
Total	(600)	63.3	(348)	36.7	(948)	100
	X^2 p value = (.995) > 0.05					
Marital Status						
Single	(280)	63.5	(161)	36.5	(441)	100
Married	(265)	62.6	(158)	37.4	(423)	100
Separated	(55)	65.5	(29)	34.5	(84)	100
Total	(600)	63.3	(348)	36.7	(948)	100
	X^2 p value = (.880) > 0.05					
Respondents' Residence						
Urban	(233)	53.7	(133)	36.3	(366)	100
Semi Urban	(325)	63.7	(191)	37.0	(516)	100
Rural	(42)	63.6	(24)	36.4	(66)	100
Total	(600)	63.3	(348)	36.7	(948)	100
	X^2 p value = (.977) > 0.05					
Ethnicity						
Ibo	(109)	61.0	(76)	39.0	(195)	100
Yoruba	(421)	64.7	(230)	35.3	(651)	100
Others	(60)	58.8	(42)	41.2	(102)	100
Total	(600)	63.3	(348)	36.7	(948)	100
	X^2 p value = (.399) > 0.05					

The respondent of the case study reported in box 1 below believed that the police were an impediment to the administration of justice. He therefore advocated for a victim support system that would not involve the police in any manner.

Box 1

I am 32 years old, a Muslim, bachelor, West African school certificate holder, and driver from Yoruba part of Nigeria. It was on a Saturday afternoon when the police embarked on their undue arrest and torture. I cannot recall the exact amount on me which they collected but they inflicted serious injuries on me. The police arrested me for no just reason, detained and charged me to court. The criminals in this instance are the police. Who is empowered to arrest them? The crime was reported to a civil rights lawyer. The lawyer created for me a public awareness that I was being detained for a crime I did not commit. Subsequently, I was granted bail. The event affected my economic and psychological stability. Since the crime was committed by the police, it further deepened my lack of trust in them. My previous experience of dealing with the police was worst. How the type of crime influenced my decision to report initially threw me into confusion. The relationship of the police with me as their victim was really agonizing. My experience with the police was negative. The quantum of information made available was insignificant. The level of sympathy which the police demonstrated in my case was very poor. As it were, these combined to further dampen my enthusiasm to develop any confidence in the police. To me, the police do not have the nerve to solve crime in my neighborhood because the level of police operation is ridiculously low. The case got to court and I was present. The police were never punished. My court experiences were partially positive. My experience would have been fulfilling if the court had told the police its limitations and indicted its erring members. As a result of the performance of the formal criminal justice system in my case, I think public policy should consider the use of informal crime control alternatives to solve crime in future. I would have loved a system for getting support that did not involve the police in my community. I paid the lawyer myself. I learnt someone wanted to support me, but the divisional police officer declined.

An in-depth interview respondent attempted to rationalise why victimization seemed to be evenly distributed among the rich and the poor, while support is unevenly provided:

> *One might be under the illusion that criminals only strike the haves and leave the have-nots. From the atmosphere of criminal activities in Lagos communities, experience has shown that criminals don't strike based on the economic viability of their victims alone. Their operation is sometimes sustenance driven. If the 'rebellion of the stomach' can cause dogs to eat dogs, then there might be some justification in criminals attacking areas notably accepted as residences of the poor in Lagos. Residents of poor neighborhoods lack the financial means to embark on target tightening mechanisms that will make criminal attacks difficult. At the same time, they lack the means to engage with unfortunate victims by providing concrete support in the aftermath of victimisation.*

Table 3 shows the kinds of support available for crime victims in the communities of Lagos.

Female respondents enjoyed more monetary support (5.6%) than males (2.7%), and more information support (33.0%) than males (28.7%). Married participants enjoyed more emotional support as victims of crime in the study site, but separated respondents received greater monetary support (6.0%) than their single (3.6%) and married (3.3%)

counterparts. Furthermore, married respondents received more material support as victims of crime in the study sites (14.7%) than their single (13.8%) and separated (10.7%) counterparts. Separated participants, however, received more information support (34.5%) than their single (33.6%) and married (25.8%) counterparts.

Table 3 - Kinds of Available Support

Variables	**Respondents' Kinds of Support**					
	Emotional	**Money**	**Material**	**Information**	**Others**	**Total**
	N %	**N %**	**N %**	**N %**	**N %**	**N %**
Age less than 20 yrs	(11) 61.1	(0) 0.0	(1) 5.6	(6) 33.3	(0) 0.0	(18) 100
21-30	(203) 48.0	(16) 3.8	(54) 12.8	(137) 32.4	(13) 3.1	(423) 100
31-40	(144) 54.5	(10) 3.8	(41) 15.5	(68) 25.8	(1) 0.4	(264) 100
41-50	(67) 49.6	(4) 3.0	(22) 16.3	(42) 31.1	(0) 0.0	(135) 100
51-60	(34) 7.1	(1) 1.9	(5) 9.3	(14) 25.9	(0) 0.0	(54) 100
61-70	(15) 35.7	(4) 9.5	(8) 19.0	(14) 33.3	(1) 2.4	(42) 100
71 years and above	(6) 50.0	(0) 0.0	(1) 8.3	(5) 41.7	(0) 0.0	(12) 100
Total	(480) 50.6	(35) 3.7	(132)13.9	(286) 30.2	(15) 1.6	(948) 100
	X^2 p value = (.163) > 0.05					
Gender						
Male	(330) 52.6	(17) 2.7	(91) 14.5	(180) 28.7	(9) 1.4	(627) 100
Female	(150) 46.7	(18) 5.6	(41) 12.8	(106) 33.0	(6) 1.9	(321) 100
Total	(480) 50.6	(35) 3.7	(132)13.9	(286) 30.2	(15) 1.6	(948) 100
	X^2 p value = (.081) > 0.05					
Marital Status						
Single	(205) 46.5	(16) 3.6	(61) 13.8	(148) 33.6	(11) 2.5	(441) 100
Married	(236) 55.8	(14) 3.3	(62) 14.7	(109) 25.8	(2) 0.5	(423) 100
Separated	(39) 46.4	(5) 6.0	(9) 10.7	(29) 34.5	(2) 2.4	(84) 100
Total	(480) 50.6	(35) 3.7	(132)13.9	(286) 30.2	(15) 1.6	(948) 100
	X^2 p value = (.030)< 0.05					
Education						
No education	(17) 37.8	(4) 8.9	(6) 13.3	(18) 40.0	(0) 0.0	(45) 100
Primary education	(53) 53.5	(6) 6.1	(9) 9.1	(30) 30.3.9	(1) 1.0	(99) 100
Secondary education	(95) 49.5	(3) 1.6	(31) 16.1	(61) 31.8	(2) 1.0	(192) 100
Tertiary education	(315) 51.5	(22) 3.6	(86) 14.1	(177) 28.9	(12) 2.0	(612) 100
Total	(480) 50.6	(35) 3.7	(132)13.9	(286) 30.2	(15) 1.6	(948) 100
	X^2 p value = (.239) > 0.05					

Ethnicity						
Ibo	(170) 54.9	(11) 5.6	(22) 11.3	(51) 26.2	(4) 2.1	(195) 100
Yoruba	(322) 49.5	(20) 3.1	(96) 14.7	(204) 13.3	(9) 1.4	(651) 100
Others	(51) 50.0	(4) 3.9	(14) 13.7	(31) 30.4	(2) 2.0	(102) 100
Total	(480) 50.6	(35) 3.7	(132)13.9	(286) 30.2	(15) 1.6	(948) 100
	X^2 p value = (.565) > 0.05					
Residence						
Urban	(170) 46.4	(16) 4.4	(51) 13.9	(126) 34.4	(3) 0.8	(366) 100
Semi Urban	(273) 52.9	(15) 2.9	(74) 14.3	(143) 27.7	(11) 2.1	(516) 100
Rural	(37) 56.1	(4) 6.1	(7) 10.6	(17) 25.8	(1) 1.5	(66) 100
Total	(480) 50.6	(35) 3.7	(132)13.9	(286) 30.2	(15) 1.6	(948) 100
	X^2 p value = (.198) > 0.05					
Income						
Less than N 2,000,000	(106) 48.4	(9) 4.1	(32) 14.6	(67) 30.6	(5) 2.3	(219) 100
N 2,000,001 – N 4,000,000	(37) 53.6	(2) 2.9	(5) 7.2	(25) 36.2	(0) 0.0	(69) 100
N 4,000,001 – N 6,000,000	(17) 56.7	(2) 6.7	(4) 13.3	(7) 23.3	(0) 0.0	(30) 100
N 6,000,001 – N 8,000,000	(46) 62.2	(1) 1.4	(6) 8.1	(20) 27.0	(1) 1.4	(74) 100
N 8,000,001 – N 10,000,000	(29) 53.7	(2) 3.7	(8) 14.8	(15) 27.8	(0) 0.0	(54) 100
N 10,000,001 and above	(245) 48.8	(19) 3.8	(77) 15.3	(152) 30.3	(9) 1.8	(502)100
Total	(480) 50.6	(35) 3.7	(132)13.9	(286) 30.2	(15) 1.6	(948) 100
	X^2 p value = (.791) > 0.05					

Data in table 3 show that male respondents received more emotional support in the aftermath of victimization (52.6%) than their female counterparts (46.7%). Chi square analysis shows that gender is not significantly related to the kind of support that victims received in the study site [X^2 p value = (.081) > 0.05]. Also, respondents whose ages were 20 years and less enjoyed the most emotional support (61.1%), while respondents whose ages are within 61 and 70 years received the least emotional support (35.7%). However, respondents whose ages are 71 years and greater enjoyed more emotional support (50.0%) than those whose ages are within age bracket 61-70 years in the study site. In terms of access to monetary support, respondents whose ages fell within 61 and 70 years had the highest access while respondents whose ages were 20 years and below and 71 years and above did not have access to monetary support in the community. Respondents within the age bracket of 61 and 70 years enjoyed greater access to material support

(19.0%) while those who are 20 years and below had the least access (5.6%). While respondents whose ages are 71 years and above had the highest access to information in the community (41.7%), those whose ages fall within the bracket of 31 and 40 had the least (25.8%). Chi square analysis shows that there is no substantial correlation between age and the kind of support a victim of crime accesses in the study site [X^2 p value = (.163) > 0.05].

The kind of support a victim requires depends on the intensity of his/her victimization, age, socioeconomic background, and the cultural disposition of members of his/her immediate community to humanitarian concerns. In box 2, the case study respondent did not expect any financial or even emotional support from the community. All she simply wanted was the restoration of procedural decorum in the way the criminal justice system does its investigation. If this had been done, she would have felt adequately supported.

Box 2

I am a 51 year old woman, a Muslim, west African school certificate holder, and trader from Yoruba part of Nigeria. It was on a November afternoon last year that the case of three million naira fraud almost rocked my life. The challenge did not end with that huge financial loss, I was also seriously injured. I had received a call informing me that a new product in which I intend to deal in will arrive in a full container and that I should pay a deposit of one point two million to be a district supplier. The ages of the criminals ranged between 32 and 35 years. They were both male and female. Prior to the incident, the criminals were my online friends. The crime was reported to the police to find a way of retrieving the money. Regrettably, the criminals escaped. The crime has effect on my health and business up to the present time. The police were reluctant to intervene because it was an online transaction which cannot be retrieved. Since I did not seek their advice before the online interaction, I think they made efforts to unravel the crime. The crime was not charged to court because the criminals were faceless. There was no support. Shame did not even give me the courage to solicit help from neighbours and even members of my family. Irrespective of my state of mind, some close family members and friends still assisted me. The kind of support that I seriously needed that I think would have provided me with the fullest opportunity was a complete investigation of the case through Interpol.

Data in table 4 show that married respondents had more emotional support (55.8%) in the community than their other counterparts. Separated respondents had access to more monetary support (6.0%) in the community than people who were not separated. Married respondents had more access (14.7%) to material support in the community than their other counterparts, while separated respondents had more access (34.5%) to information than others in the community.

Chi square analysis confirmed that there is no correlation between marital status and the kind of support a victim of crime receives in the study site [X^2 p value = (.030) < 0.05]. Respondents with polytechnic and university education had the highest emotional support, respondents without education had the highest monetary (8.9%) and information (40.0%) support, while respondents with secondary education had the highest material support (16.1%) in the study site. Nevertheless, chi square analysis shows that education is not correlated with the kind of support an individual crime victim received in the study site [X^2 p value = (.239) > 0.05].

Ibo respondents accessed more emotional (54.9%), monetary (5.6%), and information support, while Yoruba respondents accessed more material support in the study site. Nevertheless, chi square analysis shows that ethnicity has no significant relationship with the kind of support a crime victim accesses in the study site [X^2 p value = (.565) > 0.05]. Rural respondents accessed more emotional support (56.1%) and monetary support (6.1%), semi-urban respondents accessed more material support (14.3%) and urban respondents accessed more information support (34.4%). Chi square analysis shows that there is no significant relationship between respondents' places of residence and the kind of support they accessed in the study site [X^2 p value = (.198) > 0.05].

The evidence from in-depth and key informant interviews indicates that communities put more support behind young and older victims. A female in-depth interview respondent at Ibeju Lekki regretted that the criminals strike anyone they find in possession of items that catch their fancy or attempts to block their easy escape. She further added:

> *It is worrisome that contemporary criminals are no respecters of age. When we were young, criminals hardly attacked children and the aged. Today, babies and very elderly members of the society are kidnapped and used as baits to extort money from those who consider these people valuable to them. Community members feel more concerned when babies and the elderly become victims of crime. It is their helplessness that causes more support to be concentrated on this at risk population in this community. In the aftermath of crime, community people shower clothing gifts on children more than they do on adults.*

Respondents whose income per annum is between N6,000,001 and N8,000,000 ($37037-$49383) had the highest emotional support (62.2%), those whose income per annum between N4,000,001 and N6,000,000 ($24691-$437037) had the highest monetary support (6.7%). Respondents with income N10,000,001 and above ($61728+) had the highest material support (15.3%), and respondents whose annual incomes are N2,000,001 to N4,000,000 ($12346-$24691) accessed the highest information support (36.2%).

In box 3 below, the case study respondent was very satisfied with the structure of support on ground for victims of crime in the study site.

Table 4 shows data on respondents' perception of the quality of the support they received in their various communities as victims of crimes. Male respondents and female respondents judged the support they received as crime victims to be very poor, by 77.5% and 69.8%, respectively. Chi square analysis shows that gender is significantly related to the quality of support a victim receives in the study sites (X^2 p value = (.009) < 0.05). While more respondents who were 71 years and above (91.7%) rated the support they received very poor, the smallest number of respondents who shared the same impression came from age bracket 61–70. Respondents without education (80.0%) said the support was very poor; the least came from respondents who had secondary (74.5%) and tertiary

education (74.5%). Chi square analysis shows that education is correlated with the quality of support a victim receives in the study sites (X^2 p value = (.866) > 0.05). All believers in traditional religions maintained that the support they received as victims of crime was very poor, while 73.4% of Christian respondents and 72.7% of Muslim respondents felt the same. Chi square analysis shows that religion is not significantly related to the quality of support a victim receives in the study sites (X^2 p value = (.343) > 0.05).

While the majority of single respondents (76.2%) said that the quality of support that was available for victims in the communities of Lagos was very poor, 75.4% of married respondents and 65.5% of separated respondents shared the conviction that the quality of the support given to victims of crime in Lagos was very poor. Chi square analysis shows that marital status is not significantly related to the quality of support a victim receives in the study sites (X^2 p value = (.110) > 0.05).

More urban respondents (79.2%), rural respondents (68.2%) and semi urban respondents (63.0%) concluded that the quality of support available for victims in the aftermath of crime in Lagos communities was very poor. However, chi square analysis confirmed that there is a significant relationship between respondents' place of residence and the quality of support that a victim enjoys in the communities of Lagos (X^2 p value value = (.037) < 0.05).

Box 3

I am 37 years old, an atheist, bachelor, BSc holder, and surveyor from Yoruba part of Nigeria. It was in May 21st last year between 6:40 and 6:00pm. There was no financial loss but I was seriously injured. The event took place in the street. I was attacked by a group of gang having issue with my younger brother. They stabbed me several times. The boys were colleagues with my younger brother. Some of the criminals were arrested along with their parents. Some of them escaped. The gang members were detained. They were later made to pay the bills for my hospital treatment. It was really a nasty experience. Having been stabbed several times, I lost lots of blood that caused me to be extremely weak. Therefore, I was not the one that reported the incident. Later, the police came to me to ask questions that will enable them apprehend the gang members. The police tried their best. The experience was a bit bearable because the police made the gang members pay dearly for their criminal conduct. My level of confidence in the police has been heightened by the way they handle the report of the case. The kind of help I got from neighbors was the one I expected. It was relieving that I got the support when I really needed it. The support was useful to the extent that it helped the feeling of retaliation to go off completely from my mind. I will still embrace the system for getting support that will involve the police. Were they not involved, those gang boys would completely have disappeared into the thin air. There would have been nobody to hold responsible for the crime. It is exciting that I got adequate emotional, financial and information support. The providers of the support were the police, my neighbors and my family members. I cannot remember any offer of support that I declined. I am not aware of any culture that forbids neighbors supporting victims of crime. However, if any such culture exists, it should be discarded because it is repugnant to gainful brotherhood. The police should try harder in the area of information provision and utilization to get to the root of all crimes. This will prevent innocent souls from suffering for the misconduct of the badly behaved members of the community. For crime to be reduced in the community, families, institutions, police and neighbors should partner to review traditions that inhibit crime reduction efforts in the community. However, the support that is available in the community for victims of crime is encouraging.

Table 4 - Quality of Support Accessed by Respondents

Variables	Respondents' Feeling About The Quality of the Support Available To Crime Victims In The Community					
	Very Poor		Very Good		Total	
	N	%	N	%	N	%
Age						
Less than 20 yrs	(13)	72.2	(5)	27.8	(18)	100.0
21-30	(319)	75.4	(104)	24.6	(423)	100.0
31-40	(202)	76.5	(62)	23.5	(264)	100.0
41-50	(96)	71.1	(39)	28.9	(135)	100.0
51-60	(42)	77.8	(12)	22.2	(54)	100.0
61-70	(27)	64.3	(15)	35.7	(42)	100.0
71 years and above	(11)	91.7	(1)	8.3	(12)	100.0
Total	(710)	74.9	(238)	25.1	(948)	100.0
	X^2 p value = (.415) > 0.05					
Gender						
Male	(486)	77.5	(141)	22.5	(627)	100.0
Female	(224)	69.8	(97)	30.2	(321)	100.0
Total	(710)	74.9	(238)	25.1	(948)	100.0
	X^2 p value = (.009) < 0.05					
Education						
No education	(36)	80.0	(9)	20.0	(45)	100.0
Primary education	(75)	75.8	(24)	24.2	(99)	100.0
Secondary education	(143)	74.5	(49)	25.5	(192)	100.0
Tertiary education	(456)	74.5	(156)	25.5	(612)	100.0
Total	(710)	74.9	(238)	25.1	(948)	100.0
	X^2 p value = (.866) > 0.05					
Religion						
Christianity	(392)	73.4	(142)	26.6	(534)	100.0
Islam	(375)	72.7	(95)	23.5	(405)	100.0
Traditional	(6)	100.0	(0)	0.0	(6)	100.0
Others	(2)	66.7	(1)	33.3	(3)	100.0
Total	(710)	74.9	(238)	25.1	(948)	100.0
	X^2 p value = (.343) > 0.05					
Marital Status						
Single	(336)	76.2	(105)	23.8	(441)	100.0
Married	(319)	75.4	(104)	24.6	(423)	100.0
Separated	(55)	65.5	(29)	34.5	(84)	100.0
Total	(710)	74.9	(238)	25.1	(948)	100.0
	X^2 p value = (.110) > 0.05					
Residence						
Urban	(290)	79.2	(76)	20.8	(366)	100.0
Semi Urban	(325)	63.0	(141)	27.3	(516)	100.0

Rural	(45)	68.2	(21)	31.8	(66)	100.0
Total	(710)	74.9	(238)	25.1	(948)	100.0
	X^2 p value = (.037) < 0.05					
Ethnicity						
Ibo	(146)	74.9	(49)	25.1	(195)	100.0
Yoruba	(481)	73.9	(170)	26.1	(651)	100.0
Others	(83)	81.4	(19)	18.6	(102)	100.0
Total	(710)	74.9	(238)	25.1	(948)	100.0
	X^2 p value = (.269) < 0.05					
Income						
Less than N 2,000,000:00	(166)	75.8	(53)	24.2	(219)	100
N 2,000,001 – N 4,000,000:00	(47)	68.1	(22)	31.9	(69)	100
N 4,000,001 – N 6,000,000:00	(21)	70.0	(9)	30.0	(30)	100
N 6,000,001 – N 8,000,000:00	(52)	70.3	(22)	29.7	(74)	100
N 8,000,001 – N 10,000,000:00	(43)	79.6	(11)	20.4	(54)	100
N 10,000,001 and above	(381)	75.9	(121)	24.1	(502)	100
Total	(710)	74.9	(238)	25.1	(948)	100
	X^2 p value = (.561) > 0.05					

A visibly traumatised middle-age male respondent in Mushin Local Government area was alarmed by the fruitlessness of government's investments on security. He said:

> *In-spite of the huge amount of money invested by government on security of Nigerians in contemporary times, criminals still maim innocent citizens as if effective crime control mechanisms are not in place to mitigate these reckless attacks on community residents. Since it is now established by practice that government's efforts are not stemming crime, public policy should simply focus its attention on redressing and rehabilitating victims of crime, so that the members of at risk population can have some respite.*

The case study respondent in box 4 below disagreed with the position of his counterpart in box 3 to assert that beyond the assistance that came from members of his nuclear family, no other forms of support came from anywhere to bail him out of the frustration which victimization unleashed on him in the study site.

Box 4

I am 47 years old, married, a Yoruba man, Christian and a graduate. I am a businessman. On my arrival from Abuja after a contract, some guys came visiting at 10:00 am. They met my housemaid downstairs doing some washing. The hoodlums asked if she lived in one of the apartments in the building. The girl told them she did cloth washing on contract basis. They left her. They then went to a door that was ajar in one of the boys' quarters. They met a nursing mother. Her baby was barely two weeks old. They collected her phone and ordered her to keep her mouth shut. They asked of other tenants that were at home, the woman said the lady washing outside resided upstairs. On their way out, the one who took her phone went back to return it not because of her baby. However, if they showed such consideration and she announced their presence to anyone, he would come back to kill her baby. When they got to where my housemaid was, they simply directed her to take them to her masters flat. She obliged but used the wrong keys for the door. In that process, the hoodlums were becoming impatient with my housemaid. Disturbed by the argument that ensued, one of the tenants downstairs intervened. On discovering that they were hoodlums and well armed, he simply too simply cooperated. First, they followed him to his flat and raided him before they now used him to cause me to open my gate. On opening, I saw three of them already in my bedroom and four with my neighbor's wife downstairs, putting finishing touches to their mopping of her husband's apartment. Prior to this time, my neighbor and his family were driven from Ibadan to Lagos by incessant victimization by criminals. They hoped that Lagos was a place of safety.

My wardrobe was open because I was preparing to go out and in the process of making a choice about which cloth to wear. All the seven hoodlums were holding locally made short guns. They collected my twenty two thousand, my gold necklace presented to me by my wife and my wife's jewelry. I quickly thought the boys might be neighborhood guys. If per chance I knew any of them, the knowledge might qualify me for more hostility. With that reasoning, I decided to lie down facing the floor. Only God knows what came upon one of them who suddenly approached me and hit my face against the floor. Immediately, I lost a tooth! Then, blood started flowing. The hoodlum yelled, 'hey! I don't like the sight of that ugly fluid. Clean it before it gets me angrier.' After cleaning the blood, he told me to look at his gun. He shouted that they did not come to my apartment to play. He then asked if I could feel the gun. By this time, blood from my mouth had soaked my dress. Again, he reminded me to clean the blood because he said it was irritating him. He said wipe it now or I waste you. After re-cleaning it, he ordered me to bring any other precious thing out of my wardrobe. I brought out my digital camera. He collected it, he reeled coded instruction to his other colleagues. They went down the stairs, with me by their side, on instruction. Outside, we met one of them to whom all of them gave account of their exploits. On seeing how badly they had injured me, he asked how much did you collect from him? The man that dealt with me said he did not get money on me that was why he dealt with me. The man ordered that if I had nothing to offer, he should go upstairs and waste my mother. At that point I told their commander that his man actually took twenty two thousand from me. They simply warned us to cooperate as they escaped in two waiting motorcycles. I did not report because it may not result in any helpful outcome. Nevertheless, my mother told the LCDA chairman. There was no help, in concrete terms, came from anybody outside my nuclear family. However, the chairman of the LCDA came visiting for a couple of times. Without financial means, crime reporting can be self-defeating. The police could be effective if they wanted to because they know the criminals, their hideouts and their godfathers.

A total of 74.9% of Ibo respondents, 73.9% of Yoruba respondents, and 81.4% of respondents from other ethnic backgrounds maintained that the quality of support which the community residents put behind crime victims was very poor. While the majority of respondents (79.6%) that judged community support for crime victims vto be ery poor came from those earning between N8,000,001 and N10,000,000 ($49383-$61728), the least (68.1%) came from participants earning between N2,000,001 and N4,000,000 ($12346-$24691). Chi square analysis shows that income is not strongly related to the quality of support a victim receives in the study sites (X^2 p value = (.561) < 0.05).

Discussion

Traditionally, various kinds of support appropriate to the nature of the crimes have been offered to crime victims. These were graduated in accordance with the intensity of the losses which the victim suffered. It is disconcerting that today the degree of support for victims of crime is low. While cultural justifications exist for young and elderly members of traditional African settlements to be considered as vulnerable and therefore requiring special attention and support in times of emergency, this kind of communal interest is available to children but not to elderly crime victims. This perhaps shows that the level of attachment between children and their aged parents in contemporary times is rapidly giving in to the pressures of urbanization. It is indeed a paradox in the context of normative provision of care among Africans that younger victims of crime have greater access to community support than the elderly.

There are two possible reasons for this disparity. It could be an expression of payback to what might be perceived as a non-caring older generation, or else an indication of hostility of the younger generation which might have been fuelled by the intense outcome of economic hardship foisted on them by the socio-economic negligence of the older generation. Traditionally, the degree of support provided to the elderly in Africa is usually non-negotiable.

It is significant that the very elderly respondents did receive at least some appropriate support from the community. This might be in compliance with the Yoruba belief that "*ti okete ba dagba tan, omu omo re nii mu,"* which means that on the attainment of old age, the young rabbit suckles its aged.

It is interesting that while the widespread assumption in Lagos is that female crime victims are more likely to receive more community support, data from this study confirm that male respondents actually received more support from the community. This appears to suggest that the patriarchy may still be in play.

The different religious denominations are relatively equal in terms of their adherents' access to support in the community. Separated participants enjoyed greater support than their married counterparts. This is probably not an accident; among the Yoruba people, it is customarily understood that the individual without identifiable support becomes the burden which the community must shoulder, if that individual is to remain integrated. It is this principle that is the basis of the saying, "*malu ti koni iru, oluwa nii ba lesinsin,"* meaning that the tailless cow relies absolutely on God to rid it of wanton flies. That urban respondents had the least access to support might be due to the blasé kind of life that characterises the urban communities of Lagos.

The fact that Yoruba respondents had more access to support than respondents from other ethnic backgrounds is expected because the study site is predominantly inhabited by resident Yoruba people. Moreover, among the Yoruba people, presenting gifts to the less fortunate is deep-rooted in their culture. This study also reflects the idea that Ibo crime

victims in Lagos receive very strong emotional support. This may be due or related to their very strong town meetings.

The logic behind the different kinds of support available to different segments of Lagos is understandable. Respondents in semi-urban and rural communities of Lagos enjoyed more support from the community in the aftermath of victimization than their counterparts in urban settings because the former are more integrated into their community than the latter. The increased access to information by urban respondents is no doubt also partly due to increased sophistication of their environment.

According to Durkheim's 1933 prediction [20], in less formal environments, mechanical solidarity holds sway and causes people to behave alike and share sentiments that provokes wholeness than is the case for urban settings. In urban settings, interactions are differentiated by a relatively complex division of labor; the dichotomy of lifestyles and occupations thrust people apart and further undermines the principles of organic solidarity. Yoruba respondents received the greatest support probably because the study site is subsumed in the Yoruba ethnic group, and their culture is apparently more integrative than others and strongly focused on relationships with victims of misfortune. Qualitative data, especially those emanating from the case studies, confirm that some respondents would feel supported if the restoration of public confidence in the criminal justice system was restored. As it is, respondents would prefer a victim support system that does not involve the police in any way.

Conclusion

In Nigeria, community residents traditionally support crime victims in their communities. This study, however, did not find formally structured support for the victims of crime, even when survey respondents acknowledged the existence and importance of traditional support systems.

Since there is evidence of pervasive victimization not matched by proportional support, it is high time that humanitarian assistance for crime victims be taken beyond mere emotional support so that community residents can find comfort living and doing their businesses in the communities of Lagos.

The overall quality of support for crime victims in the Lagos was judged by survey respondents as very poor. Consequently, an urgent intervention is required to redress the unjust injuries inflicted on innocent citizens, especially given that formal protection by the police and other agencies of public safety has become unacceptably weak.

It is against this background that the study hinges its conclusion on the need for public policy to strengthen the custodians of culture to reawaken Africa's traditionally warm neighborly relationships that ensured that no one has to be lonely in the midst of a crowd. With this philosophy enacted, the interest of the afflicted would be safeguarded in all the communities of Lagos and the traditional status of Africans being their brother's keepers will once again appear.

Recommendations

Based on the findings from this study, I recommend that:

i. Government should establish community-based support networks to resuscitate African values, strengthen them, and reconnect community members with crime victims to accelerate their recoveries after criminal attacks.

ii. Children and the elderly should be more effectively protected by government because of their vulnerability.

iii. Victims of crime should be formally empowered to mitigate their trauma, especially immediately after being attacked.

iv. Public policy should focus its attention on supporting and rehabilitating victims of crime.

v. A formal victims' support agency should be established by the government to provide humanitarian assistance to crime victims.

References

1. Wandibba, S. (2004). Kenyan Cultures and Our Values. *Wajibu: A Journal of Social and Religious Concern* **19**(1).
2. Huntingford, G.W.B. (1953). The Nandi of Kenya. London: Routledge and Kegan Paul.
3. Leakey, L.S.B. (1977). The Southern Kikuyu before 1903, Vol. III. London: Academic Press, p. 1014.
4. Hobley, C. B. (1910). Ethnology of Akamba and other East African tribes. Cambridge: Cambridge University Press, p. 78.
5. Dundas, C. (1965). The organization and laws of some Bantu tribes of East Africa. *Journal of the Royal Anthropological Institute* **45** , 234-306 (1915) ; J. Kenyatta, Facing Mount Kenya.
6. Akongo, J. (ed.) (1984). District socio-cultural profiles report: Baringo District draft report. Nairobi: Ministry of Finance and Planning and Institute of African Studies, University of Nairobi, p. 182. (Unpublished document).
7. Petersson, F. (2009). Do you know how supporting victims of crime is helping Scotland? Victim Support Scotland, Edinburgh.
8. Davis, R. C., Brickman, E. and Davis, C. R. (1991). Supportive and Unsupportive Responses of Others to Rape Victims: Effects on Concurrent Victim Adjustment *American Journal of Community Psychology* **19**(3), 443-451.
9. Wortman and Lehman (1985) in Davis, R. C. and Brickman, E. (1991). Supportive and unsupportive responses of others to rape victims: effects on concurrent victim adjustment *American Journal of Community Psychology* **19**(3), 1991.

10. Coates, D., Wortman, C. B., and Abbey, A. (1979). Reactions to victims. In I. H. Frieze, Bar-Tal, & J. S. Carroll (Eds.), New approaches to social problems. San Francisco: Jossey-Bass.
11. Homans (1974). in Davis, R. C. and Brickman, E. (1991). Supportive and unsupportive responses of others to rape victims: effects on concurrent victim adjustment *American Journal of Community Psychology* **19**(3), 1991.
12. Thibaut and Kelley (1959). In Davis, R. C. and Brickman, E. (1991). Supportive and unsupportive responses of others to rape victims: effects on concurrent victim adjustment *American Journal of Community Psychology*, Vol 19, No 3, 1991
13. Rook, K. S., and Pietromonaco, P. (1987). Close relationships: Ties that heal or ties that bind? In W. H. Jones & D. Perlman (Eds.), Advances in personal relationships (Vol. 1, pp.1-35). Greenwich, CT: JAI Press.
14. Dunkel-Schetter, C. (1984). Social support and cancer: Findings based on patient interviews and their implications. *Journal of Social Issues* **40**, 77-98. doi:10.1111/j.1540-4560.1984.tb01108.x.
15. Dukes, E. F. (1999). "Structural Forces in Conflict and Conflict Resolution in Democratic Society," in *Conflict Resolution: Dynamics, Process, and Structure*, ed. Ho-Won Jeong. (Vermont: Ashgate Publishing Co.), 159.
16. Cleen Foundation, 2013. Public Presentation of Findings of the National Crime. Retrieved on January 18th from gallery.mailchimp.com/…/files/Text_Report_of_2013_NCVS_Finding s.pdf
17. Lagos State Government 2011.Population.Lagos State Government. 2011. Retrieved November 3,2012 from http:www.lagosstate.gov.ng/pagelinks.php?p=6
18. Campbell, J. 2012. This Is Africa's New Biggest City: Lagos, Nigeria, Population 21 Million. Retrieved June 8, 2014 from: http://www.theatlantic.com/international/archive/2012/07/
19. Rice, X. 2012.Nigeria's commercial capital's size, its economic importance, and its government's energy in addressing concrete urban problems. *Financial Times in J.* Campbell, J(ed.). This Is Africa's New Biggest City: Lagos, Nigeria, Population 21 Million. Retrieved June 8, 2014 from: http://www.theatlantic.com/international/archive/2012/07
20. Durkheim, E. (1933), "The Division of Labor in Society", Translated by George Simpson. (New York: The Macmillan Publishing Company).

Crime Location and Reporting Practices of Victims in Lagos, Nigeria

Ayodele, Johnson Oluwole* and Aderinto, Adeyinka Abideen**

*Department of Sociology, Lagos State University,
Lagos, Nigeria, johnson.ayodele@lasu.edu.ng

**Faculty of the Social Sciences, Department of Sociology,
University of Ibadan, Oyo State, Nigeria, aderinto@yahoo.com

Abstract

Differences in location influence crime reporting. Yet, how this occurs has not been adequately studied. This study addresses the nexus between crime location and reporting in Lagos, Nigeria. The survey research design included qualitative and quantitative methods. The study used data obtained from 948 respondents selected through a multistage sampling procedure. In-depth interviews, key informant interviews and case studies provided qualitative data. The analysis involved the use of simple percentages, chi square and content analysis. Our findings indicate that 62.5% of the respondents were victimised at public locations, and chi-square analysis confirms that crime location is positively associated with the rate of reporting the crime (X^2 p value < 0.05). The study concludes that location positively influences reporting, and suggests that government should address human safety at public spaces in Lagos.

Keywords: Crime Location, Crime Reporting, Human Safety, Police, Public Spaces, Nigeria

Introduction

Concern with the relationship between crime and place is not new. Crime opportunities are neither uniformly nor randomly organized in space and time. Geography and opportunity are highly relevant. Contextual factors such as the culture of the people residing in a given local in can influence crime reporting (Schaible & Hughes, 2012).

Research outcomes from France can help provide a link between place, victimization, and social responses to crime. Both Guerry (1883) and Quetelet (1842) examined nationwide statistics. The latter established that higher property crime rates were found in affluent locations, and that seasonality had a role to play in crime occurrence. As early as the first half of the nineteenth century, French scholars analyzed the distribution of crime across regions with differing ecological and social characteristics (Guerry, 1833; Quetelet, 1842). Studies in England by Plint (1851) and Mayhew (1862, 1968) also noted spatial variation in crime, as did research in the United States by Lottier (1938, 1938), Shannon (1954), Schmid (1960, 1960), and Harries (1971).

Comparative studies, most notably the work of social ecologists of the Chicago school of sociology during the first half of the twentieth century, found that high delinquency rates corresponded to communities with other social problems (Shaw, 1929). Most of the earliest studies concluded that characteristics of the urban environment are critical to explaining the emergence of crime in specific communities (Burgess, 1925; Thrasher, 1927; Shaw & McKay, 1942) and public response to them as well.

The social ecology perspective evolved into more specifically focused, place-based theories of crime, particularly the "routine activities" theory which connects potential offenders and criminal opportunities. Routine activities have been defined as "any recurrent and prevalent activities, which provide for basic population and individual needs" (Cohen & Felson, 1979:593). This approach is especially effective in explaining the role of spatial interaction between criminal activities and its eventual reporting to the authorities by the victims. Quite often, crime locales take the form of facilities—places that people frequent for a specific purpose—that are attractive to offenders or conducive to offending (Anselin, Cohen, Cook, Gorr & Tita, 2000).

These early attempts to understand the relationship between crime and place took a 'macro' approach. They looked at aggregates of places such as regions, states, cities, communities, and neighborhoods. In contrast, this study uses a 'micro' approach to examine the individual attributes of these places to see how they either promote or discourage crime reporting.

The place in which victims experience crime in their everyday lives connect with their experiences of micro-level interactions to explain how the elements of the larger social structure such as their classes, ethnicity, gender, and age predispose them to victimization and their responses to it. Brantingham and Brantingham (1982) noted the concentration of

crime in specific places. These crime "hot spots" are prime examples of the critical value of place in the analysis of crime.

Sherman, Gartin, and Buerger (1989) published one of the first studies to quantify what many qualitative studies had suggested—that crime in a city is highly concentrated in relatively few small areas. Some places become ecologies of crime because of a multiplicity of factors. They may accommodate "repeat offenders"—those who commit a disproportionate amount of total recorded crime (Spelman, 1994); "hot spots"—places with high rates of crime (Sherman et al., 1989; Weisburd et al., 1992); "crime generators"—places that are high in crime because they are exceptionally busy (Brantingham & Brantingham, 1995); "crime attractors"—places that contain many suitable crime targets without adequate protection (Brantingham & Brantingham, 1995); "crime enablers"—places where management practices allow crime to occur (Clarke & Eck, 2003); "repeat victims"—those who suffer a series of crimes in a relatively short period of time (Farrell & Pease, 1993); and "hot products"—items which are stolen at much higher rates than other assets (Clarke, 1999). Focusing policing resources and crime reporting practices on these issues and on where crime is concentrated may yield the greatest preventive benefits for the communities concerned.

The literature also suggests that certain contextual factors related to an incident influence a victim's decision to report a crime to police. Williams (1984) found that crimes that took place within the home are more likely to be reported to police than similar incidents that occurred in public.

A location can facilitate (or inhibit) crime in two ways. First, the features of a place can decrease the social control capacities of various crime suppressors. Such concerns motivate interest in the design of "defensible space" (Jeffrey, 1971; Newman, 1972). Whether the concentration of crime is largely due to reporting, targets, offenders, or place management, the people with the obligation and authority to make changes that can prevent crime are ultimately the people who control the space (Laycock, 2004; Scott, 2005). But in modern times, the police (their limitations not withstanding) are also key to effective crime management.

It is important to appreciate that locations do not provide equal opportunity for offenders to commit crimes and victims to report the crimes to authorities. Complicating the location, crime, and reporting nexus is the lack of studies in this research area. It is against this background that crime location and crime reporting form the focus of this study. We seek answers to the following questions: (1) How does crime location affect crime reporting? (2) What are the location characteristics that determine crime reporting by victims and witnesses? (3) How can a location be made less attractive to offenders and supportive of victims' reporting?

Data and Methods

This study was conducted in Lagos State in the Southwest geopolitical zone of Nigeria. Crime is sufficiently high in Lagos to warrant this study. A total of 67.0% of Lagos residents fear becoming victims of crimes, and 23.0% claimed to have experienced crime. The crime rate in Lagos increased from 12% to 21% between 2011 and 2012, with robbery representing 28% of all crime and theft 17% (Cleen Foundation, 2013).

This study was based on analyzing both quantitative and qualitative data. A survey questionnaire was administered to 948 respondents who were selected through multi-stage sampling procedure; this survey serves as the main source of primary quantitative data. For qualitative data, we did in-depth interviews which were conducted with 3 traditional rulers and 3 religious leaders selected equally from each of the three Senatorial Districts. We also did 12 key informant interviews conducted with 3 Divisional Crime Police Officers, 3 Chairmen of Landlord Associations, and 6 members of victims' families. We further did 10 case studies conducted with victims of serious crimes.

A multistage sampling technique was used to select respondents, purposefully for the study site (Lagos), and randomly for the local government areas (LGAs) in urban, semi-urban, and rural communities of Lagos. In the first stage, a simple random sampling technique was used to select 1 LGA from each of the 3 senatorial districts, giving a sum of 3 LGAs. In the second stage, areas recognised as the "black spots" of crime in Lagos, based on prior research, were studied. The LGAs were randomly chosen. In stage three, all the 13 wards in Mushin LGA were included, 10 of the wards from Lagos Island LGA were randomly selected, and 5 wards were randomly selected from Ibeju Lekki LGA to reflect population differences in the randomly selected LGAs. In the final stage, two streets were randomly selected from each of the 13 and 8 political wards that have been randomly selected from Mushin and Lagos Island LGAs. Also, 2 communities were randomly selected from the 5 political wards that were randomly selected from Ibeju Lekki LGA. Overall, 42 streets and 10 communities were randomly selected. One household was randomly selected from each of the selected 20 houses, making 520 houses from Mushin LGA, 320 houses from Lagos Island LGA, and 200 houses from Ibeju Lekki LGA. The sum of these equals 1040 houses. In cases where more than one household occupied a house, lottery method (yes/no) was used to select the respondent interviewed. Copies of a questionnaire were administered on each of the 1040 household heads.

The data analysis involved both quantitative and qualitative approaches. The univariate analysis used frequency counts and simple percentages to analyze data. Bivariate analysis involved cross tabulation and the use of inferential statistics such as chi square test to establish correlation between variables. Multivariate analysis involved regression. All these were processed through Statistical Package for Social Sciences (SPSS 20.0 Version).

For qualitative data, raw data from in-depth interviews, key informant interviews, and case studies were transcribed, sorted, and labelled. Verbatim quotations, ethnographic summaries and content analysis were used to enrich the quantitative data.

Results

Characteristics of Respondents

Table 1 provides the selected socio-demographic characteristics of the respondents. The sample included 66.1% male and 33.9% female respondents.

Table 1 - Socio Economic Characteristics of Respondents

Variable	Frequency	Percentage
Sex		
Male	627	66.1
Female	321	33.9
Total	948	100
Age		
Less than 20 years	18	1.9
21 – 30	423	33.2
31 – 40	264	27.8
41 – 50	135	14.2
51 and above	108	11.4
Total	948	100
Education		
No Formal Education	77	8.1
Primary Education	99	10.4
Secondary Education	192	20.3
Tertiary Education	580	61.2
Total	948	100
Marital Status		
Single	441	46.5
Married	423	44.6
Separated/Divorced/Widowed	84	8.9
Total	948	100
Ethnicity		
Ibo	195	20.6
Yoruba	651	68.7
Others	102	10.8
Total	948	100
Religion		
Christian	534	56.3
Islam	405	42.7
Traditional/Others	9	.9
Total	948	100
Residence		
Urban	366	38.6
Semi urban	516	54.4

Rural	66	7.0
Total	948	100
Occupation		
Civil Servant	105	11.1
Business Person	585	61.7
Students	186	19.6
Others	72	7.6
Total	948	100
Annual Income In Naira		
Less than N 2,000,000	219	23.1
N 2,000,001 – N 4,000,000	69	7.3
N 4,000,001 – N 6,000,000	30	3.2
N 6,000,001 – N 8,000,000	74	7.8
N 8,000,001 – N 10,000,000	54	5.7
N 10,000,001 and above	502	53.0
Total	948	100.0

The proportion of male to female has implications for the nature of crime that takes place in the study site, and the kind of respondents' response to reporting the crime. Typically, male adults are more culturally assumed to engage in crime reporting than females. In some important ways, age also affects exposure to, and avoidance and reporting of victimization. In this study, a 10-year age grouping was used. The age patterns of respondents indicated that only 1.9% of respondents were aged less than 20 years; about 44.6% of the respondents is between ages 21 and 30 years, and respondents between the age brackets of 21-30 and 31-40 years account for 72.4% of the total study population. Individuals within these age brackets are frequently more self-reliant than those both younger and older. Their strength makes them more able to easily re-acquire stolen items. They also possess more vigorous power of expression, belong to diverse social networks, and posses a determination that may make them more likely to report crime.

The data indicate that only 8.1% of the respondents did not have the advantage of formal education at all, while 61.2% had tertiary education. Data on the marital status of respondents revealed that 46.5% of respondents are single, 44.6% are married, and 8.9% are separated, divorced or widowed. A total of 68.7% of the respondents are Yoruba, 20.6% are Ibo (20.6%), 10.8% belong to other ethnic groups. Religious affiliation of the respondents showed that Christians constituted 56.3%, Muslims 42.7%, and traditional religions 0.9%. In regards to residence, 54.4% lived in semi urban areas, 38.6% in urban areas, and 7.0% in rural communities of Lagos. The income distribution of the respondents showed that majority (53.0%) earned an annual income of N10,000,001 and above and 23.1% earned less than N2,000,000 per annum. The distribution of occupation showed that respondents engaged in various occupational activities such as businesses (61.7%), students (19.6%), civil servants (11.1%) and other (7.6%)

Respondents' Spatial Experiences of Crime and Reporting Decision-Making in Lagos

This section discusses respondents' spatial experiences of crime, their capacity for crime reporting, and crime reporting activities in the study site. An attempt is made here to explain these phenomena on the basis of occurrence sequences. Victimization comes in before crime reporting. The latter is usually strongly affected by the experiences generated by the former. We seek both qualitative and quantitative evidence to explain the interwoven experiences.

There are 2 distinct kinds of situational forces that determine victims' responses to crime in the communities that constitute the study site. While one precipitates situations that make prospective victims vulnerable to criminal activities, the other regulates the form which the victims' reactions to victimization take.

The data from our case studies, in-depth interviews, and key informant interviews indicate that more victims lived and were victimized in the rural communities of Lagos than semi-urban and urban communities. The extent of victimization of rural community dwellers is understandable considering their inability to access modern crime fighting strategies for their individual or collective safety. Indeed, most of the participants stated that crime reporting was a risky enterprise judging by the level of cooperation that exists between criminals and the police.

Qualitative data support the idea that crime reporting is higher in the rural areas and less in semi urban and urban communities of Lagos. This might be due to variations in the extent to which tradition survives. Given the assumed cultural homogeneity that characterises rural communities, we would expect Durkheim's mechanical solidarity theory to apply.

A female in-depth interview respondent at Ibeju Lekki lamented the criminal atmosphere under which residents lived their daily lives:

> *Crime is consuming more and more people in modern times, most youth have no jobs. Worse, the police are not well equipped to solve crimes. Even where government and public-spirited individuals enable the police, they partner with criminals to make the community unliveable for residents. These make crime reporting very dangerous in our community where one has to sometimes traverse bushy roads and dark terrains to access the police and return home.*

Another key informant interview respondent also at Ibeju Lekki Local Government Area who is a male observed that:

> *Crimes in respect of which residents of Ibeju Lekki commonly report at our station are housebreaking, burglary, gang stealing and assault. There are series of burglary in which young men break the*

> *doors, windows, walls and forced their ways in to dispossess residents of their belongings. These are serious in terms of the trauma to which the acts subject the victims.*

The account of the experiences of respondents differ from location to location within the study sites. Another male in-depth interview respondent who resided in a semi urban community of Lagos added:

> *Victimization becomes more intense with every passing year. The more the police is equipped, the more sophisticated and daring criminals become and the more painful the effects of their violence on their victims. the kind of wild and culturally ignorant young men and women who wander in the community without jobs make life and living in the semi-urban Lagos unbearably fearful. If perchance they offend and you report, they belong to different cult groups, on the collection of your profile from the police, they come back to unleash mayhem on you and your household. Reporting crime is something one either does by proxy or anonymously. If you stick out your neck to report crimes, the end of the reporting may not be witnessed by the crime reporter(s).*

A male key informant interview respondent at Mushin LGA paints the picture of crime reporting in semi urban Lagos thus:

> *The crimes most commonly reported to us in the division included burglary, stealing, assault, malicious damage, car snatching, phones and laptops' theft. We attend to all crime reports but those occasioning injury, we issue police reports for medical attention to be provided by doctors at the hospital. If the case is charged to court, this document can also be tendered. On the times of the day that such crimes are reported, crimes can be reported any time as no specific time is fixed for crime reporting.*

Data from the case study below shows how security becomes unreliable as the victim moves from rural to urban through semi urban topography.

Statistical evidences in table 2 show that 90.2% of the respondents who resided in urban communities of Lagos, semi urban (91.3%) and rural communities of Lagos (87.9%) acknowledged that they, indeed, were victims of crime at some time within the past twelve calendar months from the commencement of this study.

Box 1

I am 37 years old, a Christian and businessman from Ijebu Ode in Ogun State. I specialize in general printing. It was a Thursday, in the month of May. I had an unpleasant encounter with 'One Chance Robbery'. The event which took place when I went to give my family their feeding allowance lasted for about 1½ hours. Accommodation problem caused my family to scot with my brother – in – law in Badagry. Before that time, I had been spiritually cautioned never to go out at night. But moved by the passion to keep my family away from hunger, I left my workplace at 3:00pm on the fateful day. On getting to Badagry, I did not meet my wife; I waited but had to leave when it was 6:00pm. There was heavy traffic on the way. Up to 9:00pm, I was still at mile 2 bus stop. About that time, a bus arrived. People waiting rushed into it without suspecting that one of the women that entered was actually part of the arrangement. As we ascended the overhead bridge to face Oshodi road, a man we believed was a commuter too entered. No one knew he did so with a gun concealed in his bag that looked like a musician's guitar bag. As we continued the journey, a man got up and said he wanted to vomit. I advised him to thrust his head out to do so since he was sitting by the door. Not quite long after, the supposed conductor shut the door and collected his 'fare'. Meanwhile, the man who initially wanted to vomit never did so. He shoved those on our seat painfully to the body of the vehicle. Suddenly, he ordered everybody to face down. At first, we queried why that should be. It was at this point that the man who came in last pulled out a gun. Instantly, everybody cooperated. His other colleagues started to search those of us who were legitimate passengers. We were five in number out of the 'fourteen passengers' in the bus. Before they took my money, they had beaten me to their satisfaction for telling them they were mad to have ordered us to face down. Then, they collected all my money and phone. Around 10:00pm at an area very close to Nissan Company which was usually in total darkness, they dropped us off. We had to trek down to Ilasamaja where I took a motorcycle to my house at around 12 midnight. It was at home I raised money to pay the motorcycle rider because nothing was left on me. Even one of the legitimate commuters who was coming from Cotonou bought jewelleries for his customers. He resisted releasing them, but when he was seriously beaten, he had to let go. When they got that large sum of money from me, they stopped beating me.

The amount involved in the crime was fifteen thousand naira given to me by my customer for a job. The flashback still gives me some fright. Any day I look at my child in respect of whom I went to drop money, I remember that day. The average age of the criminals was about 35 years of age. I suspect the crime was by a cult group. Only one woman was among them. Her actions were more ruthless than her male counterparts. I did not know any of them, prior to that day. I did not report the case because to who is one reporting specifically? If you report, one is just adding to the problem. One should just leave everything to God. I did not report because police cannot untie that kind of crime. Therefore, the slogan 'Police is your friend' is a big public deception. Indeed, the police are my enemies. As a part of my professional services, I used to print jacket for *Hip Up* discs. The police got wind of this; they seized that opportunity to extort money from me. Rather than protecting intellectual property of P square, they got their own illicit royalty. Police collect bribe, there is no doubt about that. Comparatively, policemen at the Ilupeju station are decent. They pay attention to community surveillance. They could be said to be the friends of the public. But the same story is not true of Olosan police station. For example, there is a policewoman at Olosan Police Station, if you are a detainee, and you are released on bail, if you or your people do not give her money, she will not release your clothes and other belongings. My relationship with the police disappointed me. The police, who in a quest to make money illicitly, will visit a workplace of an artisan, carry his generator and invite him to come and grease their palms before the generator could be released. All these happen in a country where everybody is aware that electricity supply is inadequate for productive enterprise. I don't have confidence in the police. And what one sees in the street convinces me that some policemen are the epitome of criminality. Here at Mushin, some people report incidences of crime to the Bale but most commonly, crimes are reported to the police. It is only God that

Table 2 - Respondents and State of Victimization

Variables	Respondents' victimization					
	Yes		No		Total	
Respondents' Place of Residence	N	%	N	%	N	%
Urban	(330)	90.2	(36)	9.8	(366)	100
Semi Urban	(471)	91.3	(45)	8.7	(516)	100
Rural	(58)	87.9	(8)	12.1	(66)	100

Of these, more respondents (62.5%) were victimised at public than other locations in the study area. Thus, crime locations in darkness (49.3%) and those without telephone network coverage to notify the police (49.3%) discouraged crime reporting. Whereas 53.3% of the respondents identified some crime incidents as too trivial to deserve reporting, fewer respondents (46.8%) maintained that serious crimes will be reported no matter the crime location. It reveals the state of public insecurity in the study site is such that only 9.8% in urban, semi urban (8.7%) and rural communities of Lagos (12.1%) admitted that they were not victimized.

In the case of Lagos Island, not all Lagos residents believe that crime reporting is a normative response to crime. In some circumstances, it is considered a display of weakness. A female key informant interview respondent on Lagos Island underscores this:

> *Lagos Islanders prefer retaliation to reporting crime to the police. Crime reporting to the police is not part of the norm of Island indigenes because it is symptomatic of cowardice. In other words, it is not indigenes who report crimes to the police on the Island. JJC (Johnny Just Come) meaning (New Comers) do. Some policemen know the criminals. They smoke, take drugs and share nice time together. They work together. For these reasons, it is rare to see Lagos Island indigenes reporting minor crimes to the police. Even if you ignore the consequences in terms of reprisal and report criminals, they usually get released almost immediately. It is only if the extent of injury sustained by the victim is much and threatens life, a Lagos Island victim may not feel compelled to report to the police.*

The following case study shows that victims of very large sums of money are commonly located in the urban community of Lagos.

Box 2

I am a 51-year-old woman, a Muslim, west African school certificate holder, and trader from Yoruba part of Nigeria. It was on a November afternoon last year that the case of three million naira fraud almost rocked my life. The challenge did not end with that huge financial loss, I was also seriously injured. I had received a call informing me that a new product in which I intend to deal in will arrive in a full container and that I should pay a deposit of one point two million to be a district supplier. The ages of the criminals ranged between 32 and 35 years. They were both male and female. Prior to the incident, the criminals were my online friends. The crime was reported to the police to find a way of retrieving the money. Regrettably, the criminals escaped. The crime has effect on my health and business up to the present time. The police were reluctant to intervene because it was an online transaction which cannot be retrieved. Since I did not seek their advice before the online interaction, I think they made efforts to unravel the crime. The crime was not charged to court because the criminals were faceless. There was no support. Shame did not even give me the courage to solicit help from neighbors and even members of my family. Irrespective of my state of mind, some close family members and friends still assisted me. The kind of support that I seriously needed that I think would have provided me with the fullest opportunity was a complete investigation of the case through Interpol.

Table 3 shows that 46.7% of the respondents who resided in the urban areas reported crimes against them, versus 47.1% for semi urban and 59.1% for rural communities.

Table 3 - Respondents and State of Crime Reporting

Variables	**Respondents' Crime Reporting**					
	Yes		**No**		**Total**	
Respondents' Place of Residence	**N**	**%**	**N**	**%**	**N**	**%**
Urban	(171)	46.7	(195)	53.3	(366)	100
Semi Urban	(243)	47.1	(273)	52.9	(516)	100
Rural	(39)	59.1	(27)	40.9	(66)	100

In rural communities, it is encouraging that the majority of crime victims report the crimes, the reverse is true elsewhere.

A male key informant interview respondent asked a somewhat rhetorical question that appears to address the issue of police complicity in crime:

> *Members of the Nigerian public look at the police they want as a special breed of citizens' purpose made for Nigeria. What kind of police does a society expect to have when it is the derelicts in the family system that are freely released for recruitment into the police? This is a situation which will not fail to re-enact the popular computer parlance—garbage in; garbage out.*

The case study below suggests that victims of criminals who operate in groups abound in the semi urban communities of Lagos.

Box 3

I am a thirty eight year old graduate, Christian and a bachelor. I hail from Cross Rivers Late last year, on the fateful Tuesday, about 1:30am, my sister was watching late night movie while I was sleeping in the bedroom. There was power outage. Shortly after, dogs started barking. I peeped and saw two ladies pretending to be fighting. From their statures and voices, they were not from the neighbourhood. As the barking of the dog became more disturbing, hiding hoodlums then shot and killed the Alsatian dog. Since nobody responded to their baits, as they expected, they resorted to door breaking. The robbers were about 40 to 45 in number with only two ladies. These criminals spread themselves and gave commands in coded instructions. Every house on the Street, except one was raided. The one excluded was already being vandalised before an argument broke out among the criminals that residents of the building were poor. At my house, it took them about 40 minutes before they could enter. I had hidden my sister in the ceiling with my dog. The number of the robbers gave me the impression that if they saw my sister, they might want to rape her serially. When they came in, they took the fifteen thousand naira I had. They then pointed a gun at my mother's belly. I reacted and one of the robbers stabbed me on my left cheek. They left the dagger on me and removed it when they wanted to leave with a warning that if I shouted, they would kill me. Somehow, the police were notified but they did not arrive until after the criminals were done. Six streets away, the police started shooting. So, the criminals leisurely walked away. I did not report the crime because the police knew these hoodlums and their hideouts. If I go to report the hoodlums and the police reveal my identity to them, I might be re-victimised.

On the whole, chi-square analysis in table 4 indicates that location and crime reporting were significantly related in the study setting (X^2 p value < 0.05). This implies that crime location is significantly associated with crime reporting according to the fieldwork.

Table 4 - Distribution of Respondents by Crime Location and Crime Reporting among Lagos Victims

Location in Which Respondents experienced Crime	**Respondents' Report of Incident of Crime**		**Total**
	Yes	**No**	
Urban	46.7% (175)	53.3% (195)	100.0% (366)
Semi Urban	47.1% (243)	52.9% (273)	100.0% (516)
Rural	59.1% (39)	40.9% (27)	100.0% (66)
Total	47.8% (453)	52.2% (495)	100.0% (948)
	X^2 p value < 0.05		

Discussion

Victimization and crime reporting are critical activities in public safety management. Despite the education, social sophistication, and proximity of residents of the urban communities of Lagos to agencies of formal social control, urban victims do not significantly report their crime experiences to the police more than their rural counterparts. This finding is at variance with that of Hart and Rennison (2003) that violence against suburbanites is reported to police at rates lower than violence against urbanites. However, empirical data in this study confirm that *violent* crimes against suburbanites are reported to the police at rates higher than for urbanites.

Gender differences in crime reporting for urban areas—perhaps surprisingly—are quite small. The findings of prior studies which have shown that people who live in economically disadvantaged neighborhoods are less willing to cooperate with the police is not supported by this study. The unwillingness to report crimes in this study was not as substantial as in other studies (Smith, 1986; Goudriaan, Wittebrood, & Nieuwbeerta, 2006; Baumer, 2002; Fishman, 1974; Tankebe, 2009) among rural community dwellers.

The theory of "distance decay" argues that citizens distant from law enforcement stations and urban centers of administration and culture are less likely to report crime. This theory, however, does not match what was found in this study.

Several researchers have argued that informal social control is inversely related to formal (governmental) social control. This line of reasoning can be found mostly in studies on differences in reporting percentages between urban and rural areas in the United States (Boggs, 1971; Laub, 1981). The residents of urban areas appear to feel more dependent on formal police control than residents of rural areas, as the latter can rely on the support of their direct personal environment more. In areas where informal social control is limited, residents are assumed to feel more of a need for formal social control mechanisms to help solve the problems they are confronted with. Data in this study show that over half of the urban and semi urban respondents did not report their crime victimization. However, the majority of rural respondents accepted the idea that the location in which the crime took place influenced witnesses or victims to report their victimization experiences.

While the majority of respondents noted that some incidents might not be substantial enough to warrant reporting, fewer respondents observed that the perception of crime as normal in some locations may weigh heavily against some location being a significant correlate of crime reporting. Williams (1984) found that crimes that took place within the home are more likely to be reported to police than similar incidents that occurred in public. Our findings for Ibeju Lekki, a rural community of Lagos, contradicts Williams' findings. In one case, the driver of a female crime victim reported her victimization to the police, but the woman politely told the police she did not welcome their investigation of the event.

Conclusion and Recommendations

We studied 3 types of locations: urban, semi-urban and rural, each of which had a different relationship to crime attraction, generation, and victim and community response. Our study clarified the link among locations in the three senatorial districts constituting Lagos by drawing attention to the specific situation which provides the context for criminal victimization. The study shows that response to crime is related to the specific crime location.

The attributes of locations and spaces were studied to provide an analytical framework for evaluating the spatial variations of the interaction between crime events and the way community people respond to them. If crime becomes more predictable at specific locations, then public response can be used intelligently to improve the efficiency of policing agencies, reduce crime at such locations in which community dwellers are vulnerable and strengthen public safety. No previous study has documented, the way this study has done, that citizens' sentiments drive crime reporting in the different locations identified in Lagos.

Some Yoruba sayings were found to impede effective crime reporting, though with varying effects, especially among respondents in the study site. For example, *"eni ti o se inkan ti enikan o se ri; oju re ari inkan t'enikan o ri ri"*, meaning that he who attempts what someone had not done before will interact with experiences no one had had, may be scary enough to dissuade victims from reporting crime. In the rural communities of Lagos, citizens who are victims of minor crimes are usually reminded of the need to avoid crime reporting which may end up in litigation because,. *"a kii de lati ile ejo wa dore",* meaning that we do not emerge from the background of a court case to become best of friends. In spite of the overwhelming presence of stereotypes that inhibit crime reporting in the rural communities of Lagos, it is a paradox that rural respondents reported their victimization experiences to the police more than semi-urban and urban respondents. To promote a positive and relatively uniform crime reporting pattern among the diverse locations making up the study site, public policy should weaken stereotypes that discourage crime reporting especially in the rural communities of Lagos, stimulate semi-urban and urban community dwellers to embrace crime reporting, and commit policing agencies to pay increased attention to human safety so as to promote more secure communities.

References

Alemika, E. E. 2009a. National Criminal Victimization and Safety Survey, Summary of Findings Lagos: Cleen Foundation

_____2009b. Robbery, corrupt policemen: A burden on Lagosians Survey on SECURITY and crime issues bothering residents of Lagos State by the CLEEN Foundation, a Non-Governmental Organisation (NGO) in conjunction with the Lagos State Security Trust Fund (LSSTF). Retrieved on 20/01/2010 from http://www.comp

assnews.net/Ng/index.php?option=com_content view=article&id =37751:robbery-corru pt-policemen-a-burden-on-lagosians-&catid=38:life-a-style&Itemid=689

Anselin, L. Cohen, J., Cook, D. Gorr, W. and Tita, G. (2000). Measurement and Analysis of Crime and Justice. Criminal Justice.

Baumer, E. 2002. "Neighbourhood disadvantage and police notification by victims of violence". *Criminology*. 40:579-616.

Black, D. 1976. The behaviour of law. New York: Academic.

Block, R. L. and Block, C. R. ( ).Space, Place and Crime: Hot Spot Areas and Hot Places of Liquor-Related Crime

Boggs, S. L. 1971. Formal and informal crime control: An explanatory study of urban, suburban, and rural orientations. *Sociological Quarterly*, *12*, 319-327.

Brantingham, P. L. and Brantingham, P. J. (1975). "Residential Burglary and Urban Form." Urban Studies 2:273-84.

_____ (1977). "Housing Patterns and Burglary in a Medium Size American City." In: J.E. Scott and S. Dinitz (eds.), Criminal Justice Planning. New York, NY: Praeger.

_____ (1981). "Notes on the Geometry of Crime." In: P.J. Brantingham and P.L. Brantingham (eds.), Environmental Criminology. Beverly Hills, CA: Sage.

_____ (1982). Mobility, notoriety, and crime: A study of crime patterns in urban nodal points. *Journal of Environmental Systems* 11:89–99.

_____ (1995). Criminality of place: Crime generators and crime attractors. *European Journal on Criminal Policy and Research, 3,* 1-26.

Burgess, E.W. (1925). "The Growth of the City." In: R.E. Park, E.W. Burgess and R.D. MacKenzie (eds.). The City. Chicago, IL: University of Chicago Press.

Canter, P. R. (nd).Geographic Information Systems and Crime Analysis in Baltimore County, Maryland. Retrieved on Friday, 2013 from www.popcenter.org_library_Crime Prevention_Volume_08_06-Canter

Clarke, R. V. (1999). *Hot products: Understanding, anticipating and reducing demand for stolen goods*. London: Home Office, Research Development and Statistics Directorate.

Clarke, R. V., & Eck, J. E. (2003). *Become a problem-solving crime analyst: In 55 small steps*. London: Jill Dando Institute of Crime Science.

Cohen, L. E., and Felson, M. (1979). Social-change and crime rate trends: Routine activity approach. *American Sociological Review*, 44(4), 588–608.

Duffala, D. C. (1976). "Convenience Stores, Armed Robbery, and Physical Environmental Features." *American Behavioural Scientist* 20:227-46.

Eck, J. E. (2001). Policing and crime event concentration. In R. Meier, L. Kennedy and V. Sacco (Eds.), *The process and structure of crime: Criminal events and crime analysis* (pp. 249-276). New Brunswick, NJ: Transactions.

Farrell, G., & Pease, K. (1993). *Once bitten, twice bitten: Repeat victimization and its implications for crime prevention*. London: Home Office.

Felson, R., Messner, S. F., Hoskin, A. W., and Deane, G. 2002. Reasons for Reporting and Not Reporting Domestic Violence to the Police. *Criminology*, 40(3), 617-650.

Fishman, G. 1979. Patterns of Victimisation and Notification. *British Journal of Criminology*, 19(2), 146-157.

Goudriaan, H. Wittebrood, K. and Nieuwbeerta, P. 2006. Neighbourhood Characteristics and Reporting Crime: Effects of Social Cohesion, Confidence in Police Effectiveness and Socio-Economic Disadvantage. *British Journal of Criminology*. Volume: 46 Issue: 4 Pp 719 - 742

Guerry, A. (1833). Essai sur la Statistique Morale de la France. Paris, FR: Crochard.

Harries (1971). Cited in Canter, P. R. (nd).Geographic Information Systems and Crime Analysis in Baltimore County, Maryland. Retrieved on Friday, 2013 from www.popcenter.org_library_Crime Prevention_Volume_08_06-Canter

Hart, T. C. and Rennison. C. M. 2003. Reporting Crime to the Police, 1992-2000. Special Report NCJ-195710. Washington, DC: Bureau of Justice Statistics.

Hunter, R. D. (1988). "Environmental Characteristics of Convenience Store Robberies in the State of Florida." Paper presented at the annual meeting of the American Society of Criminology. Chicago, IL.

Jeffrey, C. R. (1971). Crime Prevention Through Environmental Design. Beverly Hills, CA: Sage Publications

Laycock, G. (2004, October 30). *Clarifying responsibility for crime and safety problems: Who is responsible for what?* Paper presented at the 15th Annual Problem-Oriented Policing Conference, Charlotte, NC.

Le Beau, J. L. (1987). "The Methods and Measures of Centrography and the Spatial Dynamics of Rape." Journal of Quantitative Criminology 3:125-141.

Lottier, (1938a, 1938b). Cited in Canter, P. R. (nd).Geographic Information Systems and Crime Analysis in Baltimore County, Maryland. Retrieved on Friday, 2013 from www.popcenter.org_library_Crime Prevention_Volume_08_06-Canter

Mayhew, (1862, 1968). Cited in Canter, P. R. (nd).Geographic Information Systems and Crime Analysis in Baltimore County, Maryland. Retrieved on Friday, 2013 from www.popcenter.org_library_Crime Prevention_Volume_08_06-Canter

Mayhew, P., Clarke, R. V. Sturman, A. and Hough, J. M. (1976). Crime as Opportunity. Home Office Research Study No. 34. London, UK: Her Majesty's Stationary Office.

Newman, O. (1972). *Defensible space.* New York: Macmillan.

Plint (1851). Cited in Canter, P. R. (nd).Geographic Information Systems and Crime Analysis in Baltimore County, Maryland. Retrieved on Friday, 2013 from www.popcenter.org_library_Crime Prevention_Volume_08_06-Canter

Rengert, G. (1980). "Theory and Practice in Urban Police Response." In: D.E. Georges-Abeyie and K. Harries (eds.), Crime: A Spatial Perspective. New York, NY: Columbia University Press.

_____ (1981). "Burglary in Philadelphia: A Critique of an Opportunity Structure Model." In: P.J. Brantingham and P.L. Brantingham (eds.), Environmental Criminology. Beverly Hills, CA: Sage.

Schaible, L. M., and Hughes, L. A. (2012). Neighborhood disadvantage and reliance on the police. *Crime & Delinquency*, *58*, 245-276.

Schmid (1960a, 1960b). Cited in Canter, P. R. (nd).Geographic Information Systems and Crime Analysis in Baltimore County, Maryland. Retrieved on Friday, 2013 from www.popcenter.org_library_Crime Prevention_Volume_08_06-Canter

Scott, M. S. (2005). Policing for prevention: Shifting and sharing the responsibility to address public safety problems. In N. Tilley (Ed.), *Crime prevention handbook*. Cullompton, Devon, UK: Willan.

Shaw, (1929). Cited in Canter, P. R. (nd).Geographic Information Systems and Crime Analysis in Baltimore County, Maryland. Retrieved on Friday, 2013 from www.popcenter.org_library_Crime Prevention_Volume_08_06-Canter

Shaw, C. R. and McKay, H. D. (1942). Juvenile Delinquency and Urban Areas. Chicago, IL: University of Chicago. (Reprint ed. 1969.)

Shannon (1954). Cited in Canter, P. R. (nd).Geographic Information Systems and Crime Analysis in Baltimore County, Maryland. Retrieved on Friday, 2013 from www.popcenter.org_library_Crime Prevention_Volume_08_06-Canter

Sherman, L. (1995). In Canter, P. Using a Geographic Information System for Tactical Crime Analysis

Sherman, L. S., Gartin, P. R., & Buerger, M. E. (1989). Hot spots of predatory crime: Routine activities and the criminology of place. *Criminology, 27,* 27-55.

Shorris, E. 2000. Riches for the Poor. New York: Norton.

Spelman, W. (1994). *Criminal incapacitation*. New York: Plenum.

Stoks, F. G. (1981). "Assessing Urban Public Space Environments for Danger of Violent Crime." Doctoral dissertation, University of Washington, Seattle.

Thrasher, F.M. (1927). The Gang: A Study of 1,313 Gangs in Chicago. Chicago, IL: Phoenix Books. (Abridged ed. 1963).

Quetelet, A. J. (1842). A Treatise on Man. Gainesville, FL: Scholar's Facsimiles and Reprints (1969 ed.)

Weisburd, D., Maher, L., Sherman, L., Buerger, M., Cohn, E., & Petrosino, A. (1992). Contrasting crime general and crime specific theory: The case of hot spots of crime (pp. 45-70). In *Advances in Criminological Theory.* vol. 4. New Brunswick, NJ: Transaction.

Williams, L. S. 1984. “The Classic Rape: When do Victims Report?” *Social Problems* 31(4):459-67.

Journal of Physical Security 7(3), 62-126 (2014)

Unconventional Security Devices*

Roger G. Johnston, Ph.D., CPP and Jon S. Warner, Ph.D.

Vulnerability Assessment Team
Argonne National Laboratory

Introduction

This paper briefly describes 33 different unconventional security devices that we have devised and/or constructed. These devices are divided into 4 categories: tamper-indicating seals and traps (covert seals), tags, real-time monitoring devices, and access control techniques. Devices 1 and 25 - 33 are our newest concepts or prototypes, or the ones we have most recently made progress on.

For each of the security devices or techniques described in this paper, we only briefly sketch their design concept. We don't have the space to discuss the subtler issues associated with these devices and concepts, including details of their design, likely vulnerabilities, or possible countermeasures. Some of these designs might not ultimately prove practical, but we hope that discussing them might nevertheless encourage new approaches to physical security that we believe are sorely needed.

At the start of the discussion of each device, we list 3 pieces of information: the type of device, its current status (working prototype, patented, demonstrated, proof of principle, concept only, etc.), and an indication of the likely level of security offered by that design, i.e., how hard it might be to defeat. The latter is only speculation, though speculation based on our considerable experience with conducting vulnerability assessments on many different kinds of physical security and nuclear safegaurds devices and technologies.[1-12] The problem with estimating levels of security is that none of these devices are fully developed (because of a lack of funding), yet vulnerabilities depend critically on exact details of the design, how the security product is to be used, and for what applications and to counter what adversaries.[1,6,10]

Most of these devices could be fairly inexpensive. When we list the cost of components, it is always in retail quantities of 1. Component costs tend to fluctuate over time (but usually decrease), and almost always drop dramatically when purchased in volume.

---

* This paper was not peer reviewed.

Seals

Tamper-indicating seals play an important role in nuclear safeguards, physical security, IT security, and cargo security.[5,6,9,10] Seals are used to detect (after the fact) unauthorized access to containers, packages, envelopes, records, computer media, instrumentation, rooms, and transport vehicles. Unlike locks, seals are not meant to delay or complicate unauthorized access, just record that it occurred. Unlike intrusion detectors, seals do not detect unauthorized access in real-time, i.e. immediately.

Unfortunately, many (perhaps all) seals currently available are easy to spoof using rapid, low-tech methods.[1,13-16] Better seals are both necessary and possible. Some of the designs discussed below probably could provide better security. Some of these seals can be used as "traps", i.e. covert seals, where the tamper-indicating hardware is placed inside the container or transport vehicle, with no evidence of tamper detection on the outside.

A number of these new types of seals are based on the "anti-evidence" concept discussed in detail elsewhere.[1,13,16,17] Anti-evidence seals are designed to overcome the chief vulnerability of conventional seals—that adversaries can often readily hide or erase the fact that tampering was detected, or else make fresh counterfeit seals that show no evidence of tampering. With anti-evidence seals, in contrast, secret information (called the "anti-evidence") is stored in or on the seal when it is first installed. This information indicates that no tampering has yet been detected; it is immediately erased should unauthorized access occur. The "good guys" can determine that unauthorized access occurred by noting the absence of the anti-evidence. The "bad guys" gain nothing by counterfeiting the seal hardware unless they can determine the secret anti-evidence. And the act of trying to get to the secret information causes its immediate erasure.

Device #1 - Time "Lock"

Type: electronic, reusable time-out seal
Status: duplicate working prototypes
Applications: low to medium level security

Oddly, small battery-powered, padlock-size time locks do not seem to be commercially available. All commercial time locks seem to be large and expensive, and intended for high-level security applications.

The device shown in figure 1 is a re-usable, electronic, tamper-indicating seal we developed that we call a "Time Lock". We call it a "lock" because it looks like a lock and is used somewhat like a lock, and because people (including security professionals) are often confused about seals and tamper detection. This working prototype was developed by modifying a commercial infrared padlock and adding an additional microprocessor and our custom firmware and electronics.

Figure 1 - One of our working Time Lock prototypes. The shackle and some of the interior is metal, while the outside is plastic. The prototype shown is 6 x 4 x 10 cm, much larger than is necessary. The prototype uses less than $20 of parts (quantities of 1).

The device has two modes of operation. A switch in the battery compartment of the device selects the mode. In "time-out mode", the seal opens automatically after a set period of time (the "countdown period"). No key or combination is necessary, so there is nothing for the user to lose or forget, respectively. Moreover, the person who originally "locked" the seal does not need to be present when it opens. Thus, there are also no key- or combination-control issues associated with the use of this device.

Examples of its use might be to lock up the cookie jar to keep children from accessing it prior to dinner, or in an office setting, to seal containers or filing cabinets when going out to lunch.

The second mode of operation is "vault mode". This is where the "lock" can only be opened after a set period of time, using the fob with an infrard LED that comes with the original commercial infrared lock. The fob transmits a unique, fixed ID number.

The length of the countdown period for the prototype shown in figure 1 is adjustable from the battery compartment. 5 different time lengths are available, from 20 seconds (for demonstration purposes) to several days. The final design would have more time options, including a continuous choice of time.

Changing the mode or the time duration once the countdown period starts does not affect the time of opening.

The battery strength is tested by our microprocessor prior to starting the countdown to make sure there is sufficient power to open the lock after the countdown period. Very little power is used during the countdown period, as the microprocessor is mostly asleep. If the batteries go dead, the user can always insert fresh batteries and the countdown will continue from where it stopped.

The device has various tamper-indicating and anti-counterfeiting features which are not discussed here, nor fully implemented in the prototype.

Device #2 - Time Trap

Type: hash time trap (anti-evidence, covert tamper-indicating seal)
Status: working prototypes with 3 different designs
Applications: high level security

As discussed elsewhere in more detail[1,16,17], a Time Trap is a type of anti-evidence seal based on the realization that unauthorized access by bad guys must occur prior to the good guys opening the container or vehicle, and the fact that the vector of time points only in the forward direction in the real world.

The battery-powered Time Trap prototype shown in figure 2 uses a Microchip 16F819 microprocessor (~$1.80 each), programmed in PIC BASIC Pro.

The microprocessor is programmed to compute a new hash value for each minute that the seal is in use. (Roughly speaking, a "hash" is a fixed length number computed from a larger number in a complex and irreversible manner.[16]) The computation uses a secret key that is unique for each seal and each shipment. The key is chosen randomly by the seal based on the exact microsecond when a button on the seal is pressed by the user. Knowing the hash algorithm is of little help to an adversary if he does not also know the secret key chosen by the seal for the current use period.

Figure 2 - One design for our working prototype Time Trap.

The seal can go inside a container or transport vehicle (and thus can be a Type 1 Trap), or it can go overtly on the outside hasp. It does not require a password or reader, nor does it have to be queried about tampering prior to opening the container or vehicle.

Once the seal detects that the container or vehicle has been opened (by either the good guys or the bad guys), it immediately erases (< 1 μsec) the secret key used by the hash algorithm. This erasure of this "anti-evidence" prevents an intruder from being able to predict future hash values. After erasure, the display permanently shows the time that the container or vehicle was opened and the hash value (2 letters of the alphabet) that authenticates that time.

A single hash value is of no help in determining future hash values, because there is considerable degeneracy built into the hash algorithm. There are an average of 400 different secret keys that produce the same hash value for a given time (even assuming the adversary fully understands the hash algorithm in use). Thus, intruders will not be able to determine what hash value will need to be on the display when the good guys later gain access to the container or vehicle.

It turned out to be surprisingly challenging to choose a hash algorithm that has this high degree of degeneracy, and also selects fairly uniformly from among the possible 2-letter hashes as the secret key and the elapsed time vary. Once a suitable algorithm is found, slight modifications can ruin its behavior. This is also something we did not expect.

The prototype shown in figure 2 reports the time and hash value via the liquid crystal display (LCD). For this prototype, these values are read visually. The seal, however, could easily be designed to report the time and hash remotely via (for example) radiofrequency (rf), infrared (ir), acoustic signals, or electrical contact. Figure 3 shows an implementation that relies on the latter.

Seal inspection after opening the the container or vehicle involves determining if the time on the display is the correct time of opening (in absolute or relative time). Then, the 2-letter hash is noted. To check if this hash is correct, the time of opening and the value of the secret key can be sent back to headquarters where the hash can be computed. Alternatively, the hash can be checked in the field with a computer program we have written (figure 4), or by using a handheld device (prototype shown in figure 5).

The Time Trap has an interesting verification ("anti-gundecking") feature. If the seal inspectors are required to report the opening time and 2-letter hash back to headquarters, this automatically verifies that they actually checked the seal for tampering (instead of just claiming to have done so). They do not need a secure communications channel to do this.

While it is monitoring for intrusion, the Time Trap measures its battery voltage, and will instantly erase the anti-evidence secret key should the battery voltage drop below a certain threshold. This feature is needed because certain attacks on electronic seals involve removing the battery or slowly reducing its voltage. (Battery failure cannot be reliably distinguished from tampering in any electronic seal.) In addition, the seal monitors for

rapid or extreme changes in temperature that might indicate a thermal attack on the seal or battery.

Figure 3 - This figure shows a $2 verson of the Time Trap inserted into a briefcase. It uses a light sensor to determine when the briefcase is opened. This kind of sensor is not very effective for good security, but it is inexpensive. A quarter in the bottom of the briefcase shows the scale. The Time Trap inside the briefcase can be read electronically by a direct electrical connection through the briefcase.

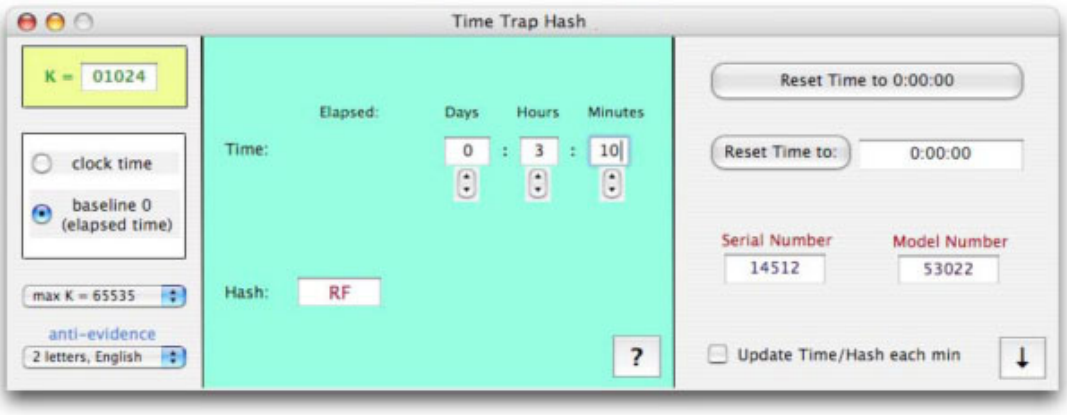

Figure 4 - A computer program we wrote to determine the correct 2-letter hash for a given secret key (K) and opening time. If desired, the program can run continuously, updating the hash as the time automatically advances.

Figure 5 - A prototype device for computing the 2-letter hash algorithm after the secret key and the elapsed time are entered.

To reuse the Time Trap, the device is turned off , then turned back on. It will select a new random key based on the (unpredictable) exact microsecond that the user presses a button.

For a few more dollars in parts, the prototype Time Trap in figure 3 can simultaneously monitor up to 14 additional sensors. When multiple sensors are used, they are polled in a random, constantly changing order so that an adversary cannot predict when a given sensor will be read by the seal.

We have demonstrated a number of different sensors that can work with the Time Trap. One is a small, solid-state Hall Effect magnetic sensor (Honeywell SS94, ~$2 each). This sensor can monitor the opening of a container lid or a truck door. A small permanent magnet is placed on the lid or door; when opened, the Hall Effect sensor detects the change in magnetic field caused by the movement of the magnet. Unlike simple magnetic door switches, the Hall Effect sensor cannot be easily spoofed by just bringing another magnet close. This is due to its high sensitivity, about 200 nanoTesla (nT). By way of comparison, the Earth's magnetic field at the surface is about 55,000 nT.

Changes in the magnetic vector as a moving transport vehicle changes orientation with respect to the Earth's field can either be ignored by raising the alarm threshold of the sensor, or by correcting for the apparent change in the Earth's field using a second Hall Effect sensor located far from the magnet on the lid or door. If a magnet is placed on the assets of interest instead of the lid or door, then the Hall Effect sensor can detect the removal or movement of the assets if it is sufficiently close.

Another sensor that can be used with the Time Trap is a solid state tilt sensor (accelerometer) with 0.001g resolution (MEMSIC MXD2020E/FL, ~$12.50 each). If one of these sensors is placed on the container lid or vehicle door, and another is placed on a

nearby perpendicular surface, they can be compared to tell when the lid or door has been opened as compared to jostling from overall movement of the container or vehicle.

A miniature Passive Infrared (PIR) sensor can also be used to detect the presence of people or a hand in a container. These typically cost approximaltey $2 each and cover the thermal ir wavelength range 7 to 14 μm. Inexpensive ultrasonic motion detectors also work fairly reliably if used inside a closed container.

A solid state colorimetric sensor (~$2.50 each) described in the section on Device #19 (the Tie-Dye Seal) can also be very effective at detecting tampering or movement of assets, lids, or doors.

Other possible sensors include:

hall effect magnetometer $0.85
1-wire temperature sensor $2
thermistor $0.70
force sensor $3
solid state CO2 sensor $18
IR proximity sensor $12
gyro (angular rate sensor) $22
triple axis accelerometer, $7
temp and humidity sensor $12
high-resolution 2-axis magnetometer $50
vibration sensor $2.50

Device #3 - Flashing Lights Seal

Type: password (anti-evidence) seal
Status: demonstration prototype
Applications: medium level security

Password seals are a kind of anti-evidence seal that requires the good guys to uniquely identify themselves with a password (or PIN or mechanical combination) before the seal will report the secret anti-evidence.[16] Both the anti-evidence and the password must be kept secret for the duration of the cargo shipment or period of tamper monitoring.

This working prototype device shown in figure 6 is such a password, anti-evidence seal. It typically would go on the outside of a container. At the start of each use, the seal chooses a 4-digit password and the 4-digit anti-evidence and flashes them to the user with LED lights.

Prior to when the seal is removed or the container or vehicle is opened, the user inputs the password using the push buttons. The seal then responds by flashing the 4-digit anti-evidence if the seal has not been opened, and the wrong 4-digits if it has (or the password

is wrong). Only 3 wrong passwords are allowed before the seal permanently erases the 4-digit anti-evidence.

The device in figure 6 uses a light sensor, but many other kinds of intrusion sensors are possible, as with the Time Trap.

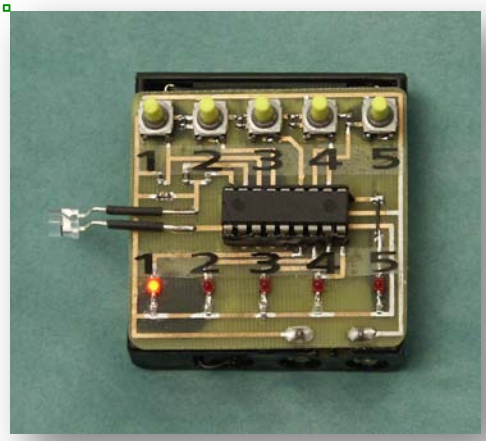

Figure 6 - A demonstration prototype for the Flashing Lights Seal. This microprocessor-based seal uses less than $4 of parts. It measures 5 x 4.5 x 2 cm, though it can easily be reduced in size by a factor of 5. The seal would ordinarily go inside a light-tight seal outer case.

Device #4 - Blinking Lights Saturation Seal

Type: saturated response (anti-evidence) trap
Status: demonstration prototype
Applications: low to medium level security

Figure 7 shows a schematic of a Saturated Response Trap [16] called the Blinking Lights Seal. It consists of a two-dimensional array of light emitting diodes (LEDs) driven by a programmed microprocessor. Like the Time Trap, this seal can be located inside the container or transport vehicle being monitored for unauthorized access. In that case, it is a Type 1 trap. It can also be used (as an overt seal) on a hasp outside the conainer or vehicle with a slight redesign.

The device can use the same sensors as the Time Trap. Also like a Time Trap, it does not require a password, nor does it have to be queried about tampering prior to opening the container or transport vehicle.

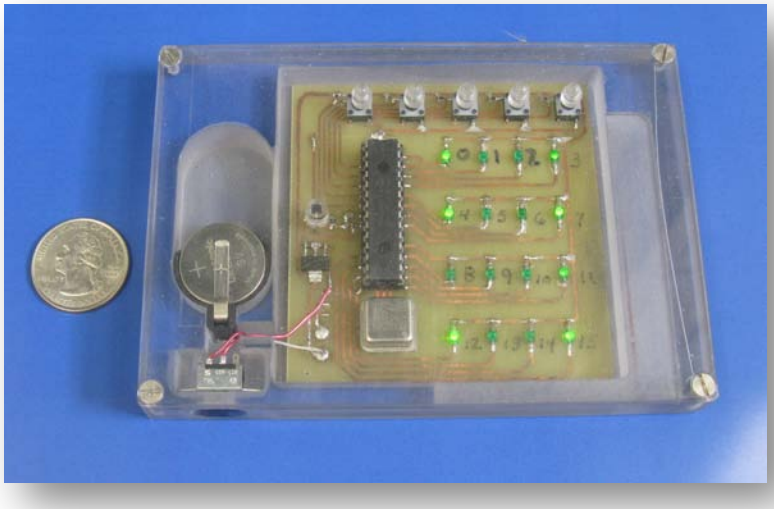

Figure 7 - The Blinking Lights Saturation Seal. The blinking LED lights indicate whether tampeirng has been detected by hiding this information among other extraneous blinking.

Unlike the Time Trap, however, the Blinking Lights Seal does not need to keep track of time nor compute (or look up) hash values. Instead, when requested, the Blinking Lights Seal unleashes a high bandwidth stream of data. Hidden somewhere in the data is one or a few bits that represent the anti-evidence. This bit or bits tells the seal inspector whether the container or transport vehicle has been opened previously. All the other data is just random noise.

In the case of the prototype seal shown in figure 7, the high bandwidth data is a complex temporal two-dimensional pattern of blinking lights. This pattern is shown only once on demand (by pushing a button), or else repeated only a small number of times before the pattern is permanently erased from the seal's microprocessor. Each seal, each time it is used for a shipment, has a different blinking pattern chosen by the microprocessor prior to use, or downloaded to it.

The punch card shown inserted in figure 8 is one possible way for the seal inspector to interpret the blinking lights. It is designed to slide in front of the two-dimensional array of LEDs. (Each seal, and possibly each shipment, has a different card.) This card allows the seal inspector to focus on (for example) just 3 of the blinking LEDs. The lack of previous tampering can be indicated a number of different ways (otherwise tampering is indicated). Here are just a few of the possibilities:

- All 3 of the LEDs turn on or off in unison.
- The 3 LEDs turn on and off in sequence.
- The first LED blinks once, the second one twice, the third one three times.

- If the LEDs are 3-color LEDs, they all show the same color simultaneously.

An adversary who does not know which of the LEDs are relevant is faced with a complex two-dimensionally array of rapidly blinking lights. To try to hide the fact that he has previously gained unauthorized access, he can record the complete pattern of blinking lights, then program the original seal or a counterfeit to replay that same pattern. This is certainly possible, but it requires at least some capability in electronics and microprocessors, plus it may not be easy to do rapidly.

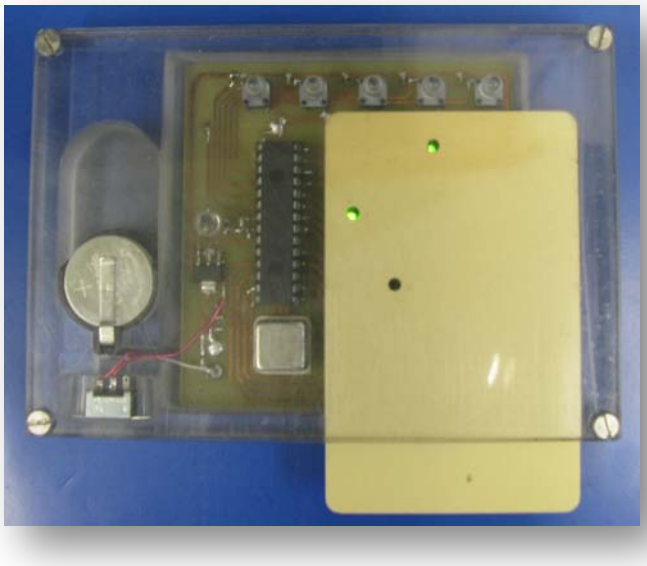

Figure 8 - The inserted punch card focuses the inspector's attention on the only LEDs that matter.

The Blinking Light Seal has the advantage of being electronic, yet still engaging the seal inspector in a careful visual examination of the seal. If desired, the card shown in figure 8 can be punched out just minutes before it is needed, based on information securely transmitted to the cargo's destination.

Ordinarily, the blinking light pattern will be displayed only when the seal inspector pushes a button on the seal. In our demonstration prototype, however, there are 5 different buttons. Each one generates a different light pattern (but convey the same anti-evidence). All the other patterns would then be erased once a button choice was made.

Device #5 - Talking Truck Cargo Seal

Type: password (anti-evidence) seal

Status: working prototypes of several different designs
Applications: high level security

Figure 9 shows a working prototype of one type of password seal called the Talking Truck Cargo Seal. The unit at the left is the handheld unit, which remains outside the truck (or container) being monitored for unauthorized access. It can communicate with up to 1000 different seals using 434 MHz radiofrequency (rf) signals. The unit at the right of figure 9 is the actual tamper-indicating seal that goes inside the truck (or container) to be monitored. It includes a light sensor like our Time Trap, but it can also simultaneously poll up to 12 additional intrusion sensors, including those discussed in the Time Trap section.

Figure 9 - Prototype Talking Truck Cargo Seal, with the handheld seal reader on the left.

Our prototype Talking Truck Cargo Seals were designed for a fictitious trucking company called "Near Miss Trucking". The anti-evidence consists of one randomly chosen slogan out of 135 (or more) possible slogans used by Near Miss Trucking Company. These slogans are not secret. In fact, it is advantageous if the seal inspector is quite familiar with all the slogans. What is kept secret is exactly which slogan was chosen for each container in any given shipment. A new, random choice of slogan is made each time a seal is reused.

Examples of the Near Miss Trucking slogans we use in our prototype (some admittedly facetious) include:

- The “go” in cargo.
- We’ll make it fit!
- It’s not our fault.
- Sleep, what’s that?
- Fewer felons work for us.
- If it falls out of our truck, you can keep it.
- The center lane marker is only a suggestion.
- At least one fire extiguisher per dozen trucks.

After the container or truck is sealed up, the handheld unit in figure 9 chooses the secret, random 4-byte password and one of the slogans. This information is transmitted wirelessly by radio frequency (rf) to the seal inside the truck through the truck wall (even if metal). The seal then stores it until unauthorized access is detected.

The secret password and slogan chosen by the handheld unit can be duplicated or read out a variety of ways so that the secret information can be sent (using encryption or a secure communications channel) to the cargo’s destination where it will be needed for seal inspection. Alternately, the original handheld unit can be physically transported to the cargo’s destination.

The prototype in figure 9 has the handheld unit speak the slogan through a built-in speaker, although an earphone can also be used in noisy environments. Other possible versions of the Talking Truck Cargo Seal could have the truck itself do the speaking. This simply requires that a small speaker be added to the seal, or to the inside or outside wall of the truck.

For the speaking, we use a digitally recorded human voice, rather than synthesized speech because this makes the slogan easier to understand. The slogan is repeated 3 times to be sure it is heard.

Only if the correct password is sent by the handheld unit to the seal in the correct rf format AND if there was no unauthorized access, will the correct slogan be spoken at inspection time. Otherwise, a different slogan is spoken so as not to tip off the bad guys that their intrusion was detected. For ease of use, the inspector can check off which slogan was heard from an alphabetized checklist of the 135 possible slogans.

Having a spoken slogan keeps the seal inspection process at a very human level. This is advantageous from a psychological standpoint. Too often, automated high-tech seal readers distract the seal inspector, or mentally remove him from personal involvement in the details of the shipment. This is not conducive to good security.

With 135 possible slogans, an adversary has a 1 in 135 (0.7%) chance of guessing the correct slogan. Then he must program the original seal or a counterfeit to say the correct slogan when the secret password is presented. He does not get a second chance. If even better odds are desired, up to 4000 possible slogans can be stored in the seal.

We also made a "food" version that says 3 different kinds of food out of 256 possibilities. Thus, if the inspector hears, for example, "hamburger-waffles-bananas" he can be assured there was no tampering, but if he hears 3 other foods (or nothing), then unauthorized access is indicated. With 256 possible food choices, the odds of an adversary correctly guessing the 3 foods in the correct order is approximately 1 in 17 million. (One disadvantage of this design is that it tends to make the user hungry!)

Device #6 - Triboluminescent Seal

Type: password (anti-evidence) seal
Status: U.S. patent 6,394,022 [18]
Applications: high level security

Triboluminescence is the phenomenon where a material produces light (visible, ultraviolet, or infrared) when mechanically agitated.[19,20] (The word "tribo" means "to rub" in Greek.) While most materials are triboluminescent to some degree when sufficient pressure is applied, there are many compounds that can produce visible sparks in daylight conditions when merely dragging a fingernail across them.

Some of the most strongly triboluminescent compounds include zinc sulfide (sphalerite) doped with manganese, cholesteryl salicylate, various europium and terbium compounds and complexes, N-isopropylcarbazole, triphenylamine, and silicon carbide (carborundum).[19,20] Wintergreen Life Savers (powdered sugar doped with methyl salicylate) have also been known for hundreds of years to generate sparks when crushed in the mouth[21], though this triboluminescence is 2-3 orders of magnitude less efficient.

The idea behind the Triboluminescent Seal is that any attempt by an adversary to open, drill, saw, cut, grind, or chemically attack the seal will produce triboluminescence. This light can be used to trigger an erasure of the anti-evidence.[16,18]

A schematic for one possible implementation of the seal is shown in figure 10. The seal consists of two halves (male and female) that snap together irreversibly through a hasp via an internal C-locking ring. This locking ring is stronger than the seal material itself so that any attempt to pry the two halves apart results in damage to the seal and the generation of triboluminescent light. An alternate design appears in figure 11. In this case, the two seal halves are attached by the use of tight threading. A considerable amount of light will be generated when the seal is screwed or unscrewed. With this design, the user does not need a special tool to open the seal, and the two seal halves can be reused.

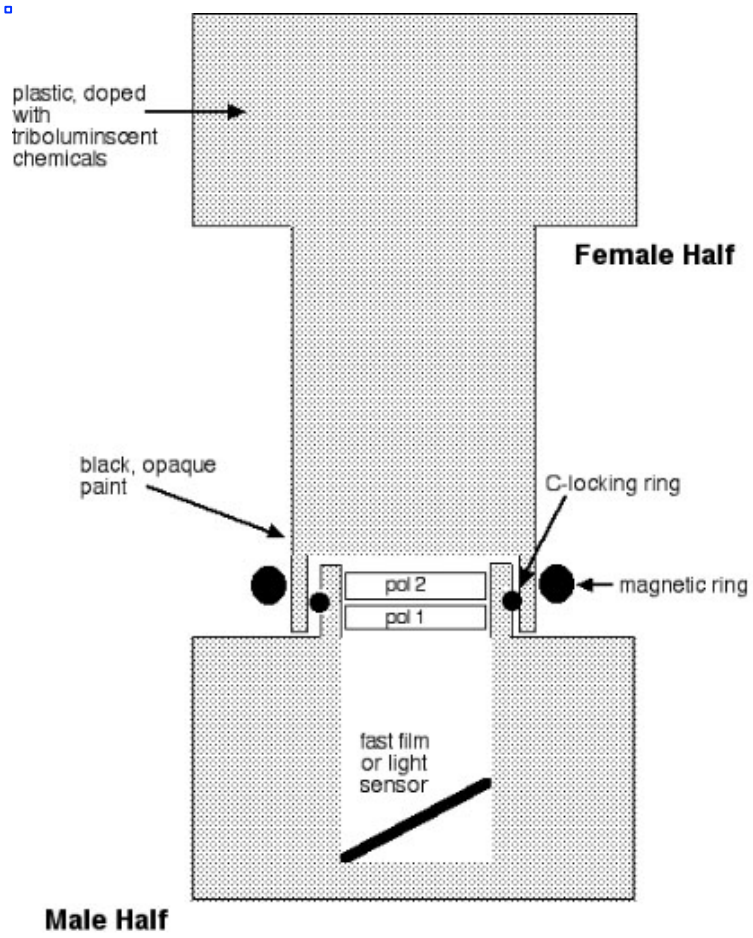

Figure 10 - Cross-sectional view of one version of the Triboluminescent Seal shown assembled. The male (bottom) and female (top) halves have been snapped together through the hasp of the container or truck/railcar door.

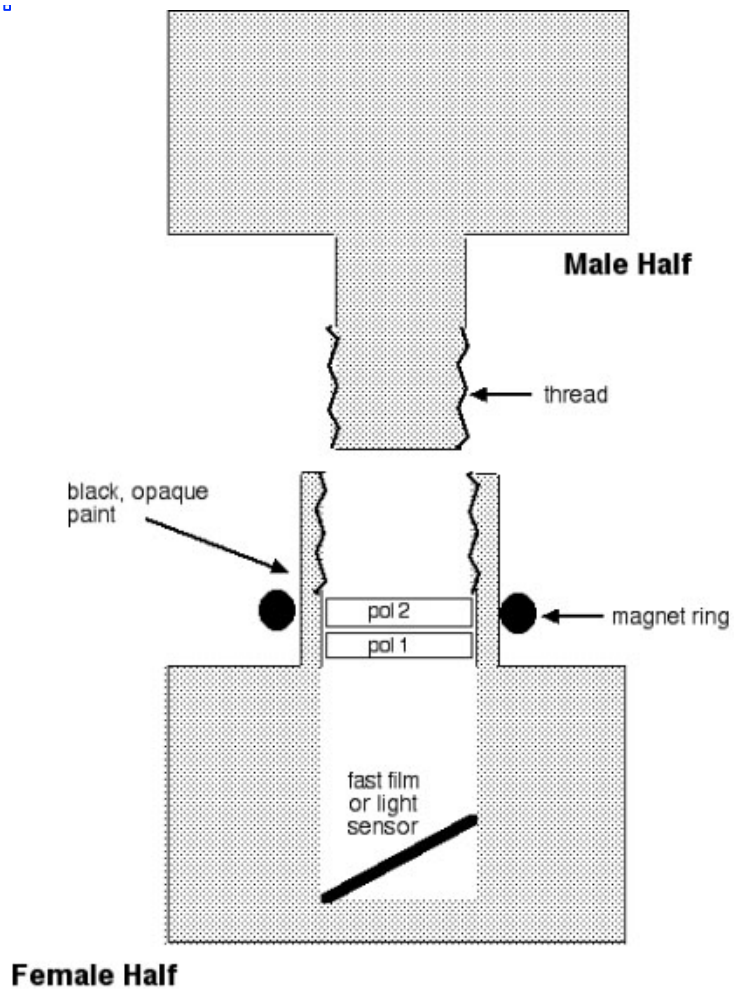

Figure 11 - Threaded version of the Triboluminescence Seal shown prior to use. Each half of the seal is painted on its exterior with an opaque paint or epoxy layer (and also on certain interior surfaces). This prevents light from entering the seal and exposing the undeveloped photographic film which is located at the bottom of the male half of the seal.

The two halves of the seal are made from transparent or translucent glass or plastic that is doped with strongly triboluminescent powders. Inside the seal are two inexpensive plastic polarizers. The first polarizer (pol 1 in figure 10) is fixed and cannot rotate. The second polarizer (pol 2) can be rotated in a non-contact manner by rotating the magnetic ring on the outside of the seal. We can get any orientation we want (even after the seal is closed) for pol 2 by rotating the external magnetic ring. The ring interacts magnetically with pol 2 to permit this non-contact rotation. There is enough friction on pol 2 to prevent it from rotating inadvertently.

Here is one way the seal can work: Prior to sealing a container or door, we take two identical photographs of some detailed scene using very fast (high sensitivity) film. The film is then removed from the camera. One of the pieces of film is developed and then placed in secure storage. The second (identical) piece of film is left undeveloped, and then placed into the bottom of the male half of the seal. This must be done in the dark to avoid exposing the film to light.

Next, we insert the two polarizers, again in the dark. The 2 polarizers are initially crossed so that virtually no light passes through them because of the high extinction coefficient. This keeps the film inside the male half of the seal safe from room light, and the seal can then be taken out of the darkroom. (It might nevertheless be a good idea to place a temporary cap on the male half of the seal to minimize light exposure.)

When the seal is ready for use, the two halves of the seal are snapped or screwed together through the hasp of the container being sealed. The external magnetic ring is rotated to orient pol 2 to some arbitrary, unpredictable angle, where it is no longer crossed with pol 1.

Markings (or numbers) on the outside of the magnetic ring tell the seal user how much to rotate the magnetic ring back in order to cross the polarizers when it is time to examine the seal for signs of tampering. Unauthorized personnel, however, do not know which is the correct orientation required for the magnetic ring to cross the two polarizers. (Each seal is different.) The markings or numbers on the magnetic ring are thus a bit like a combination that only authorized personnel are supposed to know.

When it is time to inspect the seal for tampering, here is the process: The seal user rotates the external magnetic ring back to the (secret) proper orientation to cross the two polarizers. This orientation is the secret “combination” or “password” that makes it safe to open the seal. He/she then cuts, saws, or grinds the seal off at the female half, just above the polarizers in figure 10, or unscrews the two halves for the figure 11 design. This will generate considerable triboluminescent light (plus let in room light), but it won’t matter because the cross polarizers will keep light from reaching the film.

The seal is then taken to a darkroom for analysis. A technician (in the dark) removes the polarizes to access the piece of film. The film is then developed, and compared with the film that has been in secure storage.

After being developed, the two images are compared (e.g., with a blink comparator discussed below) to verify that they are identical and that the film coming from the seal was not exposed to light. Because an adversary does not know what was on the film (the image shot for each seal is completely different), he will have trouble counterfeiting the image if he exposes the film in the seal to light. If the film in the seal has been around intense radiation, it may be necessary to allow a correction for fogging caused by radiation exposure.

Note that the assumption in this invention is that an adversary cannot determine the proper orientation of pol 2 without using light that will expose the fast film. X-raying the seal will not easily tell an adversary the polarizer orientations. The X-rays, first of all, would fog the film. Secondly, trying to determine the molecular orientation of thin plastic sheet polarizers from outside the seal with X-rays should be a daunting task. If desired, barium sulfate an be added to the seal to block X-rays to further complicate X-ray imaging.

Probably a more practical and cost-effective approach would be to do away entirely with the photographic film and polarizers. Instead, a miniature solid-state light sensor and microprocessor is used at the location of the film. Once the seal is closed up, the light sensor begins monitoring. When light is detected, the microprocessor instantly erases the secret anti-evidence. The seal user (possessing the secret password) can check on the anti-evidence via rf before opening the seal. This is similar to the Talking Truck Cargo Seal described above. On the other hand, this microprocessor version would require a battery, unlike the film version which is fully passive.

This seal concept can be scaled up or down. A tamper-indicating “safe” or “vault” made of triboluminescent walls could, for example, be constructed. Other potential variations on this seal include the use of color filters or circular polarizers (instead of linear polarizers) so that the seal can be opened only in the presence of certain wavelengths and/or a certain handedness of light.

Device #7 - Magic Slate Seal

Type: password (anti-evidence) seal
Status: working prototypes of 2 different designs
Applications: medium level security

Perhaps surprisingly, anti-evidence password seals do not need to be electronic. See figure 12. The Magic Slate Seal [22] is solely mechanical, yet fully reusable. The seal is named after the novelty toy that allows children to write or draw on a grey plastic sheet with a plastic or wooden stick, then erase the “slate” by lifting the plastic sheet.

The Magic Slate Seal is a unique "combination" seal [16] where only the good guys know the proper way (i.e., the combination) to open the seal without destroying the secret information that indicates the absence of tampering. The bad guys, however, will destroy the secret information in the processing of opening the seal.

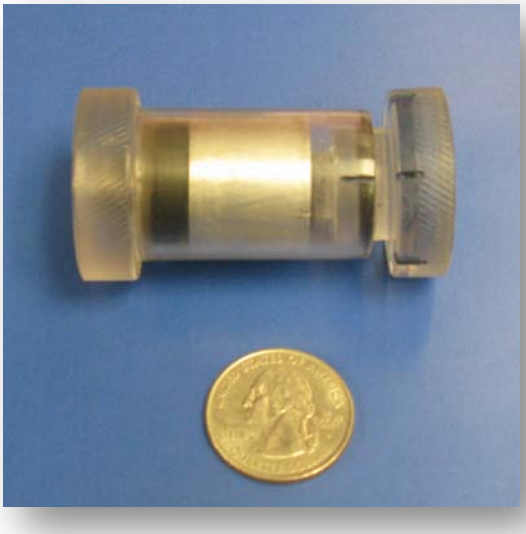

Figure 12 - A prototype Magic Slate Seal that is intended to go through the hasp on a container or transport vehicle.

The seal in figure 13 consists of a male and female half that snap together. No tools are required to close or open the seal. The O-rings shown in figure 13 provide enough friction to keep the seal from opening accidentally, and also protect the interior from moisture and dirt.

Inside the seal is a cylinder with erasable writing. The cylinder can be made of metal or else slippery plastics such as polytetrafluoroethylene or polyethylene. For this prototype, 6 different random digits or symbols are written around the circumference of the cylinder. This is the anti-evidence.

The cylinder sits inside a larger diameter tube called the "sled". At one end of the sled is the eraser. This is a buna rubber and felt washer which has had a single slot cut in it, as shown in figure 14.

To open the seal, the user rotates the male end to whatever angular position he wishes. (See figure 14 for the end-on view.) The male and female halves are then pulled apart by hand. The cylinder goes with the female half of the seal, while the sled goes with the male half. In doing this, the sled drags along the outside of the cylinder, causing the eraser to erase all the writing, except for the digit or symbol that aligns with its slot. As a result, all but one of the digits or characters written on the cylinder gets erased. The erased "anti-evidence" is no longer available to an adversary to counterfeit.

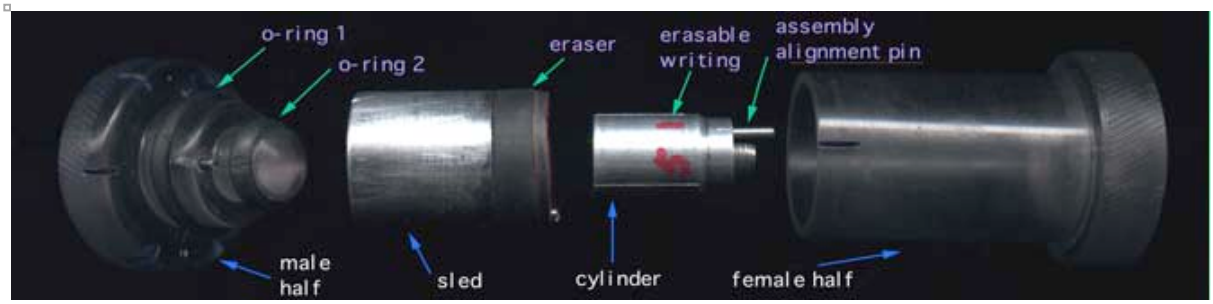

Figure 13 - Exploded view of a different prototype Magic Slate Seal.

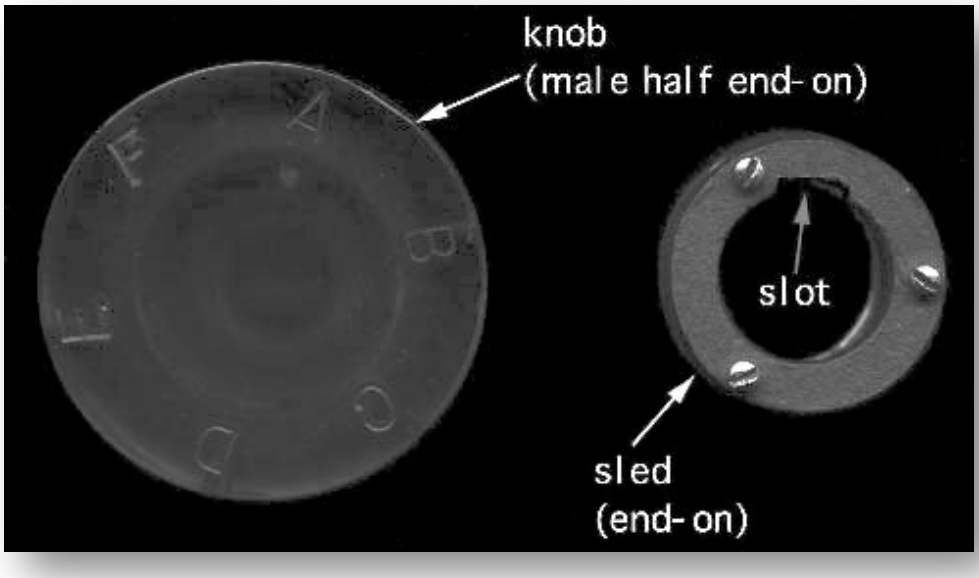

Figure 14 - End-on view of a prototype Magic Slate Seal.

The seal inspector can report the letter (that is, the angular position in figure 14) where he opened the seal, and the digit or symbol that was left on the cylinder. If the seal was previously opened by the bad guys at a different letter, or the writing incorrectly counterfeited, the digit or symbol left on the cylinder will be wrong or missing.

Alternatively, the seal inspector can be told in advance at what letter to open the seal, and what digit or symbol he should then see on the cylinder.

There are several options for reusing the seal:

1. If desired, the seal inspector can re-close the seal, keeping the correct letter aligned. He then would randomly rotate the knob. The seal can then be checked again at a later date

for tampering. (Although 5 of the 6 digits would have been erased for the prototype shown in figures 13 and 14, we don't care, since we are only interested in one of the digits, and which one that is will be kept a secret.)

2. The user can discard the cylinder (or return it to the factory for reuse) and open a blister pack with a fresh cylinder previously printed at the factory.

3. The original cylinder can be reused in the field by writing new random digits or symbols on the cylinder by hand.

4. The user can print new random digits or symbols on the cylinder using a small ink printer or a one-time use “carbon” paper provided by the seal manufacturer.

We found it most effective to use “white board” dry erase markers for the erasable writing in our prototypes because a great deal of engineering has gone into making the “ink” completely erasable, even many months after being applied to a surface. Dry erase markers are also quite inexpensive. Other types of erasable “inks” are also possible, however, including carbon black and frangible paints such as Torque Seal (Organic Products Company, Irving, Texas). Pre-oiling the cylinder prior to applying the writing enhances the erasability of most inks.

Note that with the prototype shown in figures 13 and 14, the adversaries have a 1 in 6 chance of opening the seal at its correct angular position. (This is because there are 6 letter positions on the end of the male half of the seal in figure 14.) They do not get a second chance if they guess wrong.

If better odds are desired than 1 in 6, the Magic Slate Seal can be designed much like the common bicycle lock shown in figure 15. There would be 3-5 different rings that the user would rotate (instead of just the male end of the seal). Only if the slots in all the rings correctly lined up would the erasable writing be safe from destruction when the seal was opened.

Figure 15 - A commercial 4-digit combination lock that uses alignment slots. Each of the 4 disks has an internal slot. Only when the slots align (at the correct combination) will the lock open. This type of design could be used to increase the number of possible "combinations" for the Magic Slate seal, though a more secure design would be necessary than exists on this inexpensive bicycle lock.

Device #8 - Skunk Seal

Type: novel conventional seal
Status: concept
Applications: low to medium level security.

The skunk seal concept is based on using the human sense of smell to detect if a seal has been opened. For this seal, a semi-volatile chemical which has a strong, definitive odor at low concentrations is placed inside the seal. Many odorous chemicals can be detected and identified by the nose at part-per-billion (ppb = 10^{-9}) to part-per-million levels. [23] For example, mercaptans, which are often added to natural gas as a safety measure to impart an odor (and used by skunks as a defensive measure) can typically be detected at concentrations of a few ppb. Pleasant odors could also be used.

When the seal is opened, a small chamber or vial containing the liquid chemical is ruptured. Alternately, microencapsulated forms of the chemical ("Scratch-n-Sniff" technology) could be crushed to release the chemical vapor.[24] Yet another approach is to let two chemicals react when the seal is opened to produce the odor of interest.

Whatever the odor-generating mechanism, the vapor would be allowed to escape slowly through microscopic holes in the seal. If the chemical—either prior to rupturing the chamber/vial or after—is allowed to soak into a porous membrane, fabric, or material with large surface area, deep capillaries, and/or fissures (such as porous Vycor glass[25]), the smell will persist for some time. If designed correctly, an adversary would have difficulty rinsing out the seal sufficiently to mask the odor, especially if the interior of the seal, or printing on it, was designed to dissolve in water or other liquids.

Replacing the seal with a counterfeit, on the other hand, leaves the adversary with the problem of putting enough of the correct chemical (which might not be easy to identify without high-tech methods) into the counterfeit seal to provide a strong odor when the seal inspector opens the seal. He might also try to capture enough of the released odor from the original seal to load up the counterfeit seal, but that might be challenging, especially outdoors.

Inspection involves sniffing the seal prior to opening it to be sure no odor is present, then opening the seal, followed by sniffing it again to be sure the correct odor gets generated. (If not, the seal is probably a counterfeit, or else has previously been opened and "aired out" for a long time.) A companion "Scratch-n-Sniff" sticker (kept separately by the seal inspector) could help him recognize the correct odor in the field.

An adversary might be tempted to chill the seal so that the chemical freezes and its vapor pressure drops to nearly zero. When the seal eventually warms up, however, the chemical will start to vaporize. Moreover, it should be possible to design the seal so that the chamber or vial contains water (or a water/anti-freeze solution) and fractures when excessively chilled due to the expansion of the liquid as it freezes. This would release the scent chemical.

If the exact smell used for each seal was kept secret, adversaries would not know in advance which chemical to expect. The seal inspector could report to headquarters what he/she smelled when the seal was opened (strawberry, vanilla, toluene, mercaptans, etc.), perhaps by matching with a number of "Scratch-n-Sniff" stickers. In this way, headquarters would know that the seal was actually inspected.

It is also possible to use commercial, hand-held, battery-powered organic vapor detectors instead of the human nose. Units that cost between $200 and $6000 can (depending on the chemical) typically detect concentrations in air 1 to 2 orders of magnitude lower than can be detected by the sense of smell. Such instrumentation, however, complicates the inspection process. It also removes the inspector from direct interaction with the seal—something that is not conducive to optimal security.

Device #9 - Anti-Evidence Skunk Seal

Type: password (anti-evidence) seal
Status: concept
Applications: low to medium level security

It should be possible to design the Skunk Seal as an anti-evidence, password seal (either mechanical or electronic). The correct password or mechanical combination would be needed to safely open the seal without releasing the odor. (If the seal was mechanical instead of electronic, it might be designed similar to the mechanical Magic Slate Seal discussed above.) The seal could then be opened multiple times by the good guys without releasing the odor. In effect, the lack of odor is the "anti-evidence"[16] that gets "erased" when the odor is generated by the act of opening the seal.

Device #10 - Inverse Skunk Seal

Type: novel conventional seal
Status: concept
Applications: low to medium level security

If a highly volatile chemical is placed in the skunk seal, instead of a semi-volatile chemical as described above, the inverse approach can be used. When the seal is opened, the chemical will be released and rapidly evaporate away, leaving no smell when the seal is later opened by the seal inspector. In this case, the absence of the correct smell indicates tampering.

Device #11 - Anti-Evidence Inverse Skunk Seal

Type: password (anti-evidence) seal

Status: concept
Applications: low to medium level security

The inverse skunk seal can be designed so that the correct password or combination would allow the good guys to safely open the seal multiple times without releasing the volatile chemical.

Device #12 - MagTag

Type: complexity (anti-evidence) seal (and tag)
Status: U.S. patent 6,784,796 [26]; demonstrated with various prototypes
Applications: medium to high level security; can monitor volumes, not just portals as with conventional seals

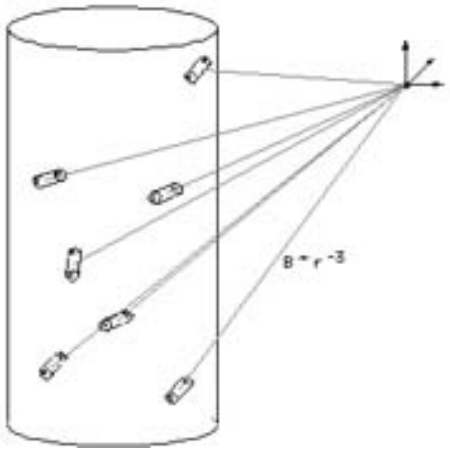

Figure 16 - The MagTag concept. A complex arrangement of randomly oriented permanent magnets of varying strengths creates a very complex magnetic field outside the container. This will change if one or more of the magnets is moved or rotated.

The MagTag seal is based on the fact that DC (constant) magnetic fields, such as those generated by permanent magnets, are virtually unattenuated by most materials including wood, plastic, water, concrete, soil, and only weakly attenuated by most metals. Thus, if we place permanent magnets randomly throughout the interior volume of a container (or transport vehicle), we can tell—from the outside—if they have been removed or slightly moved based on changes in the external magnetic vector field generated by the magnets. At each point in space, the magnetic field is the vector sum of the magnetic fields of all the magnets.

For a sufficiently complex configuration of magnets inside the container, an adversary can't restore the original magnetic vector field (at all points in space) with a different configuration. See figure 16. In other words, a tamperer must put the magnets back

exactly the way he found them, with the same magnetic strength, 3-dimensional (3D) location, and orientation, or the tampering will be detected. Depending on the strength of the magnets and the distance from the gaussmeter (magnetometer), the 3D positions and orientations of the magnets may need to be replicated with considerable accuracy.

The more magnetic field measurements that the seal inspector can make at different points in space (including out of the horizontal plane), the more difficult it is for an adversary to counterfeit the magnetic field readings. If these point are kept secret, the tamperer will have even greater difficulty. For routine applications, measurements at one or two different points in space outside the container (or transport vehicle) are probably sufficient. For better security, measurements should be made at 3-8 locations. Kinematic mounts can be used to accurately position the gaussmeter probe. (See the discussion about kinematic mounts in the section entitled, "Device #20 - Adhesive Label Seal with Blink Comparator".)

For this kind of approach, it is important that the cargo be well tied down. Otherwise, movements of the magnets due to cargo shifting will be misinterpreted as tampering.

Note that rare earth magnets (the strongest kind of permanent magnet) are very brittle. If they are well epoxied to the cargo, or to containers or pallets inside the cargo area, an adversary may find it challenging to remove them for reuse without causing damage. We have also designed mechanical "hysteresis" mounts that make it difficult to exactly reposition a container or its lid once the container has been moved or opened.

There is a way, however, to obtain even better tamper detection. If we design a magnet to move irreversibly when the transport vehicle's door is opened or closed, or when the cargo is moved, or when a container lid is removed, then it will be even harder for a tamperer to escape detection. We have successfully demonstrated such "chaotic scrambling mechanisms" on doors, filing cabinets, and drawers.[26] These randomize the magnet's orientation and sometimes also its position. To avoid detection, an adversary may need to put the magnet back to within a few μmeters and arc-seconds of orientation, especially if we can get the gaussmeter close to the magnet. The adversary cannot simply glue down the magnet in its correct location and orientation, because this would keep it from moving the next time the door or lid is opened. Simple capture mechanisms guarantee that a magnet will become trapped in place when the door, drawer, or container is fully closed and thus will not move during transport (unless tampering occurs).

For either the static magnet application, or the chaotically scrambled magnets, the magnetic field can be measured outside the container or transport vehicle using commercial handheld, battery-powered room-temperature gaussmeters (1 nT resolution along 3 axes, ~$5000), with commercial magnetometer sensors (10-100 nT resolution along 2 axes, ~$20), or with solid-state Hall Effect sensors (~200 nT resolution, ~$2) mentioned in the section on the Talking Truck Cargo Seal.

With the most sensitive commercial, room-temperature gaussmeter, a single rare earth magnet (residual induction=13300 gauss) of cylindrical dimensions 2.5 cm in diameter by

2.5 cm long (~$7 each) can be detected—or its absence noted—from 5 meters away, even through a container, truck, or transportainer wall.[27] Larger magnets can be detected at even greater distances. Table 1 shows the sensitivity to translation and rotation for this same 2.5 cm x 2.5 cm cylinder magnet, assuming 20 nT sensitivity, for various distances from the gaussmeter. When it is possible to get to within a few cm of the magnet, as will be the case when a single magnet is applied to a door or a container lid, the magnet can be quite small and of about the same strength as a refrigerator magnet.

Table 1 - Sensitivity to translation and rotation of a rare earth magnet, 2.5 cm in diameter and 2.5 cm in length, assuming 20 nT resolution.

distance from magnet (meters)	minimum detectable magnet displacement*	minimum detectable magnet rotation
0.20	0.1 μm	0.6 arc mins
0.25	11 μm	0.9 arc mins
0.50	160 μm	7 arc mins
1.0	2.6 mm	0.9°
1.5	1.3 cm	2.9°
2.0	4 cm	6.8°

* Along a line between the magnet and the gaussmeter.

Neither the orientation of a transport vehicle with respect to the Earth's magnetic field, nor the naturally occurring drifts in the Earth's field (typically < 1% in magnitude and 0.1° orientation per year) need concern us. This is because we can make a quick calibration measurement of the background field before measuring the MagTag magnet(s). AC magnetic fields from motors and electrical equipment also present no problem because we are making DC measurements.

Some of the attractive attributes of MagTag include:

- There is nothing outside the closed container to suggest tamper detection. The magnetometer or gaussmeter can be taken away between measurements; it is not necessary to monitor the magnetic field continuously.

- We can "read" the tag/seal as many times as we want from the outside without having to open the container or transport vehicle.

- No electrical power or batteries are needed until we wish to check the MagTag, and then only for the seal reader (the gaussmeter/magnetometer).

• The (rare earth) permanent magnets are reusable, relatively inexpensive, and will last for decades.

• In addition to detecting tampering, the arrangement of magnets also serves as a kind of tag to uniquely identify the container or transport vehicle, or its contents.[26,27]

Device #13 - Tempered Glass Seal

Type: novel conventional seal
Status: U.S. patent 6,553,930 [28]; partially working prototypes have been constructed
Applications: low to medium level security

It is unfortunate that glass has been largely overlooked for use in tamper detection. Glass has many desirable properties including:

- inexpensive
- full transparency (so the interior of the seal can be inspected without opening it)
- chemical inertness (thus outstanding resistance to corrosion and aging)
- resistance to ultraviolet light & ionizing radiation
- can handle temperature extremes
- relatively light weight
- great strength and hardness (though considerable brittleness)
- ability (in tempered glass) to store enormous stresses that can be released when the glass is cut or drilled, thus severely damaging the glass; this can be a very successful tamper-detecting mechanism
- can be tricky to repair in the field
- is an electrical insulator, making it safe to use around electricity
- each batch of glass has a unique chemical "fingerprint" due to trace impurities
- requires glass blowing skills to manufacturer & is non-machinable (making counterfeiting by novices difficult)

The idea with the Tempered Glass Seal is to create two glass tubes that can be irreversibly snapped together using an internal locking ring.[28] See figure 17. Note that once the two halves of the seal are snapped together, an adversary only has access to glass, not to the internal locking ring. It is thus extremely difficult to pick the seal open.

The glass tubes are manufactured so as to contain the appropriate level of internal stresses. This can be carefully adjusted by controlling the amount of tempering. Tempering means to cool the glass relatively quickly, in a controlled manner, from above the annealing temperature so as to generate internal compression and tension areas due to differential cooling. Automobile windshields or glass bathroom shower doors, for example,

are tempered to create great strength, and to allow them to fail in a safe manner, i.e., without sharp shards.

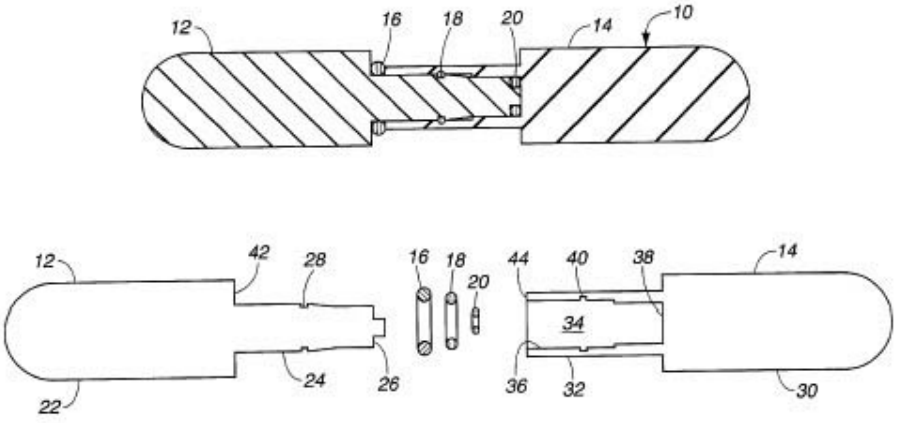

Figure 17 - Schematic of the Tempered Glass Seal. The two halves of the seal (bottom) are shown snapped irreversibly together (top) using the internal locking ring, 18. Elements 16 and 20 are airtight O-rings that keep pressure in and moisture and dirt out. From U.S. Patent 6,553,930.

The tempered stresses in the glass tubes are not so high as to cause the glass to explode—simply to break into multiple pieces if cut, sawed, or drilled. The tempering is adjusted to make sure that the seal can withstand the usual forces encountered in routine handling and transport.

A serial number can be placed inside the seal with a printed band or tube, etched on the outside or inside of the glass (before tempering) using mechanical or chemical etching, or printed on the outside of the glass using ink.

If tempered correctly, the glass seal will disintegrate if the surface is scored, sawed, cut, drilled or ground, yet the seal can be handled very roughly without damage if the surface is not gouged. Proper tempering will prevent the seal from fracturing into sharp shards when the surface is damaged. If shards are nevertheless a concern, or if the seal will be subject to severe banging and abrasion in regular use, a clear plastic coating or sleeve can be placed around the glass to protect it.

The seal is removed by simply scoring it with a file, or giving it a sharp blow with a hard tool that damages the surface.

Device #14 - Glass and Powder Seal

Type: complexity (anti-evidence) seal
Current status: mockups constructed; another possible embodiment of U.S. patent 6,553,930 [28]
Applications: medium level security

The Glass and Powder Seal is a variation on the Tempered Glass Seal. Lightly packed inside each seal half are various bands of fine colored powder. See figure 18. Each band is a different color and perhaps thickness. The bands may be made from different materials, with a different texture and average particle size. (Exotic chile powders and other spices work well and are inexpensive.) Each seal half has a different set of bands, so that no Glass and Powder Seal is identical to any other. One of the bands inside each seal can be a desiccant powder to keep the other bands dry.

The powder bands can be packed by mechanically stuffing them into the glass tubes with a rod (something like loading an old style musket). Alternately, the powders can be more quickly loaded into the tubes by placing the tubes on a slow-spinning centrifuge, and introducing each powder into the tube through a small Teflon tube down the center of the centrifuge. (High speed centrifuging is not desired since we do not want the powders to become too densely packed.) After all the powder bands are in place, the end of each seal half is plugged with steel or glass wool, cotton fibers, a thin plastic stopper, or an epoxy plug to keep the bands from moving.

Each tube might contain one or more small air pockets, particularly at the closed end of the tubes. These air pockets can be protected from the powders by a glass frit with microscopic holes. The air pockets are under modest pressure. This can be easily achieved by cooling the glass tubes prior to sealing. The pressurized air pockets are intended to launch the powders if the glass tube fractures. (There may, however, be enough air in the spaces between powder particles to accomplish the same thing without any macroscopic air pockets.)

Figure 18 - Mock-ups of the Glass and Powder Seal, with powder bands of varying color, composition, and particles shown.

If an adversary tries to cut, saw, drill, or grind the seal, the tempered stresses causes the glass seal to break into many pieces. Also, the internal (unknown) positive pressure inside the seal, launches the powder. Both mechanisms disperse and mix the powders and destroy the bands. Trying to gather up the powders so as to recreate the band pattern is not impossible, but it would be a time-consuming, non-trivial task for an adversary. Accurately counterfeiting the correct color or reflectance for each powder would also be non-trivial, as would chemically counterfeiting the powders.

To check the seal for signs of tampering, the seal inspector holds up a smaller glass tube, containing the same bands of colored powder. This tube was loaded at the same time as the seal with the same powders in the same sequence. (Alternately, a color image of the bands printed on a slip of paper can be used for comparison.) He/she then does a side-by-side comparison with the seal—rather like comparing tree rings. Another way to read the powder bands is to scan them with a commercial hand-held colorimeter or reflectance meter.

If desired a small compressed metal or glass spring can be placed in the glass tubes prior to loading the powder. When the seal is cut, sawed, or drilled, the tempering causes the glass to fracture. The force stored in the spring is then released and further helps to disperse and mix the powdered bands.

For a higher level of security, the powders and/or glass can be analyzed for trace impurities to verify their authenticity.

Device #15 - Glass Rivet

Type: novel conventional seal or complexity seal
Current status: concept only; another possible embodiment of U.S. patent 6,553,930
Applications: low to medium level security

Rivets conventionally used on the handle of truck and transportainer doors are a problem for effective cargo security. See figure 19. Especially where ocean salt air is involved, the rivets are often severely corroded and nearly ready to fall off. When dirty and corroded, they are difficult to inspect. Commercial cargo thieves know this and often drill out the rivets or cut them off with a zip gun. They can then open the truck or transportainer door by rotating the vertical locking rod without disturbing the lock or seal on the handle. Counterfeit rivets are easy to put back, if the thieves wish to hide their attack.

Figure 19 - Transportainer showing a lock on the handle. The arrow points to the handle's rivet that is a source of vulnerabilities for cargo theft.

It would make more sense to directly lock or seal the vertical locking rod in figure 19 than to lock or seal the handle. There is, however, often considerable resistance on the part of cargo handlers to changing the long tradition of checking the lock or seal at the handle. One way to fix this problem is to replace the steel rivet on the handle with a solid glass "rivet". This rivet consists of two tempered, solid glass pieces with an internal containment (locking) ring to snap them irreversibly together, similar to how the two halves of the Tempered Glass Seal snap together irreversibly. See figure 20.

Being made of glass, the rivet will not corrode. Its transparency permits a full inspection of the glass rivet's integrity inside and out. The glass strength is sufficient to withstand ordinary cargo handling, yet if the glass rivet is drilled, cut, sawed, or ground, the tempered stresses will cause the rivet to severely fracture. Unique "fingerprint" identifiers can be added to the glass rivet such as internal or external serial numbers on the back of the rivet, or dyes or internal reflective particles blended into the glass. A trace analysis of the glass itself is also an excellent, hard to counterfeit fingerprint.

If the interiors of the rivet halves are partially hollow, a series of powder bands, or else a 2-dimensional array of powders, like a 2D sand painting, can be used to make each rivet unique. See figure 21.

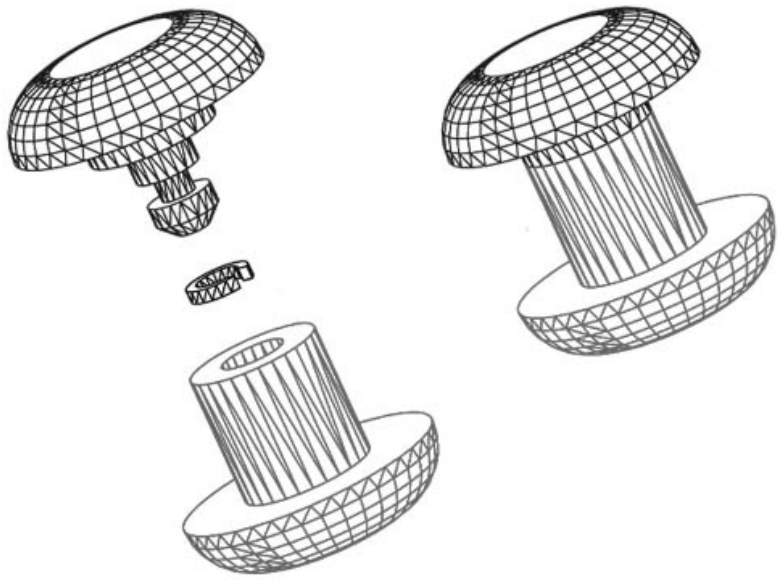

Figure 20 - Glass Rivet with internal locking ring, shown unassembled (left) and assembled (right).

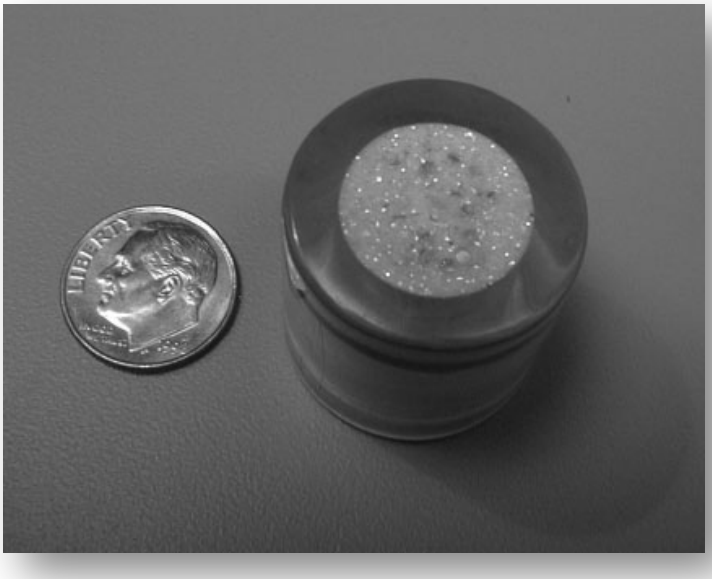

Figure 21 - Mockup of a tempered glass cap (one-half of a glass rivet) with a two-dimensional complex powder pattern. (What is shown here is slightly larger than would be used for a glass rivet.) The powder includes glitter particles. The tempering means that any attempt to cut, drill, saw, or otherwise damage the glass rivet will cause the powder to become scrambled. The other half of the rivet (not shown) snaps irreversibly to this glass cap via an internal metal locking ring.

Device #16 - Haspless Plug Seal

Type: novel conventional seal or lock
Status: working prototypes of several different designs have been constructed
Applications: low level security, or to delay an adversary

Many conventional seals (as well as locks) require a hasp. Without a hasp, there may be nothing to attach the seal (or lock) to. A lot of containers, however, are not specifically designed with a hasp. They can sometimes be retrofitted with a hasp using welding or an epoxy, or by drilling a hole through the container lid, but such add-on hasps are often highly vulnerable to attack. Moreover, certain containers cannot be modified in this way because it would change their geometry, affect their safety, and/or void their certification.

Containers that do not intrinsically come with a hasp often have a lid, cover, or cap that is attached to the main body of the container with bolts or screws. To gain access to the container contents, these screws or bolts must first be unscrewed so that the lid, cover, or cap can be removed.

Our Plug "Seal" allows a seal (or lock) to block access to a screw or bolt holding on the container lid, cover, or cap. The plug device is inserted into the body hole used for the screw or bolt. No modification to the screw/bolt, body hole, or container lid is necessary. Depending on the container design, more than one Plug Seal may be needed if multiple screws or bolts require protection.

Figures 22 and 23 show one possible design. The concept is basically as follows: the plug shown on the right in figure 22 is inserted into the body hole for the bolt. The nut on the device is tightened using the "wrench" shown to the left in figure 23. This forces the washer to squeeze on the rubber plug, causing it to expand radially and become wedged into the body hole. The nut can be tightened to the point that several hundred pounds of force (or more) are required to pull the plug out of the hole.

Spikes can be attached to the circumference of the rubber so that the forced expansion of the rubber plug drives the spikes into the body hole wall, further resisting the removal of the plug. This may, however, damage the body hole.

The plug can be attached to a stainless steel tube, as shown in figure 23, prior to compressing the rubber. After compressing the rubber, a conventional padlock or seal is inserted through the hole (hasp) in the hardened steel tube. This padlock or seal blocks access to the plug nut so that it cannot be easily removed from the hole without removing the padlock or seal first. The wrench is then used to loosen the nut on the plug. This relieves the pressure on the rubber and the plug can then be pulled out of the hole with minimal force.

Figure 22 - One implementation of the Plug Seal. The "wrench" at the left is used to rotate the nut at the left end of the plug after the plug has been inserted into a bolt hole. This compresses the rubber, causing it to expand inside the bolt hole. There are other possible mechanisms for compressing the rubber as well.

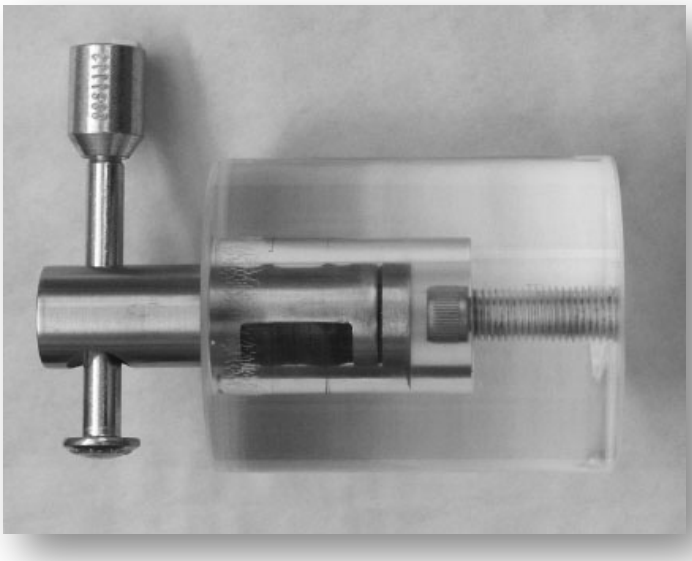

Figure 23 - The plug is shown mounted to a hardened steel tube, which is placed inside a simulated bolt body hole. After the plug's rubber is expanded, a standard commercial bolt seal, passing through a hasp in the steel tube, blocks easy access to the plug. This makes making removal of the plug (so that the bolt can be accessed) more challenging if an adversary wishes to leave no evidence of accessing the container contents.

Figure 24 shows another approach that makes use of the Tempered Glass Cap that was shown in figure 21. The assembly is then totally flush with the container wall, leaving nothing for an adversary to tug on.

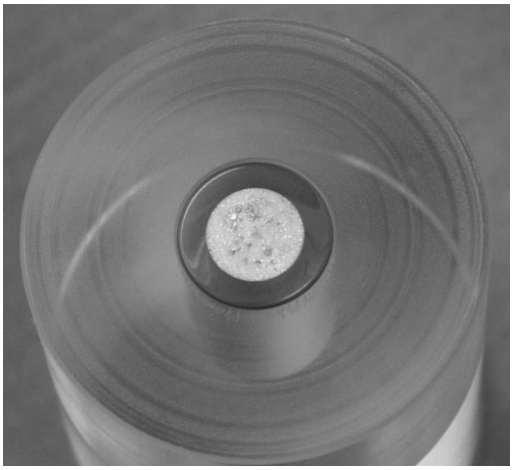

Figure 24 - Another way to protect the plug in the bolt hole is with the Tempered Glass Cap from figure 21. It snaps irreversibly to the plug using an internal locking ring. Being flush, there is little for an adversary to grab onto in order to attempt to remove the plug, which is being held tightly in place because of the expansion of the plug's rubber. To gain access to the bolt, the glass cap can be struck with a center punch. The tempering makes the blow cause the cap to disintegrate, destroying the unique two-dimensional powder "sand painting" seen in the photo.

Device #17 - E-Cup Insert

Type: enhancement of conventional seals, particular the metal (E-cup) seal
Status: U.S. patent 6,588,812 [29]; a working prototype has been constructed
Applications: low to medium level security

The E-cup seal, also known as the "metal cup seal, type e" or the "cup wire seal" has been widely used for U.S. domestic nuclear safeguards for several decades. See figure 25. The International Atomic Energy agency (IAEA) has its own, more complex version of the seal.

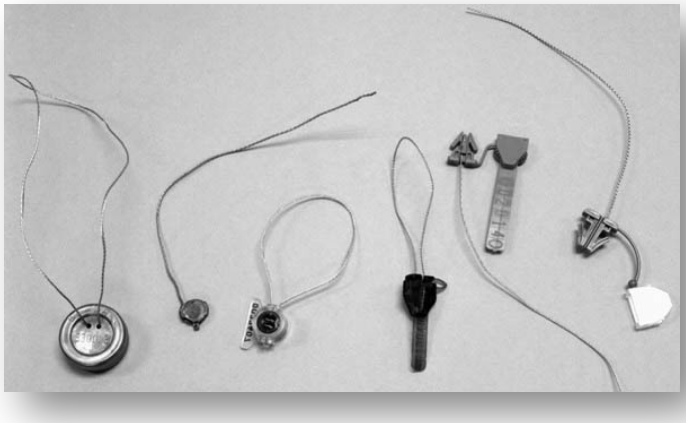

Figure 25 - Some commercial wire loop seals, including the E-cup on the left.

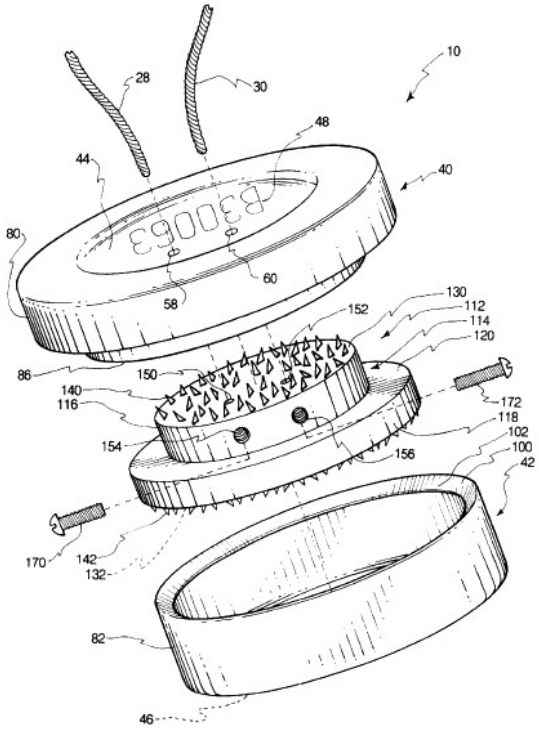

Figure 26 - The insert, with its sharp barbs, is shown between the two halves (Elements 40 & 42) of the E-cup. From U.S. Patent 6,588,812.

The E-cup seal consists of a string, single wire, or strand of wires, together with two small metal cups that are meant to snap together in a (supposedly) irreversibly manner. Prior to snapping the two metal halves together, the wire or cord passes through the hasp on the container to be sealed. The two ends of the wire or cord are then passed through separate holes in one of the cups. The ends of the wire or cord are then crimped or tied together, and the two cup halves are snapped together.

Some of the potential attacks on the E-cup may involve flexing, skewing, or compressing the metal halves. To counter this, an insert of the kind shown in figure 26 with sharp, hard barbs can be placed inside the two cups prior to snapping them together. This insert will cause obvious damage to one or both of the cups should such manipulation of the E-cup be attempted.[29,30] The insert does not interfere with the normal sealing process, nor does it require any changes in the manufacture of the E-cup seal.

An additional advantage of the insert is that it can, if desired, be used to more securely and repeatably capture the ends of the seal's wire or string.[29]

The same insert concept would work for other kinds of seals that have an internal inner cavity between two halves that snap together.

Device #18 - Multi-Strand Wire Loop Seal

Type: enhancement of conventional wire loop seals
Status: concept
Applications: low to medium level security

One possible category of attacks on conventional "wire loop" seals (such as the E-cup in figure 25) involves splicing the wire that passes through the hasp. An adversary can do this quite a number of different ways, including using soldering, brazing, welding, epoxies, or other wire repair methods. A competent splice attack can be difficult and time-consuming to spot with manual inspection.

For robustness, many wire loop seals use strands consisting of 2-4 wires, sometimes twisted around each other. The idea with the Multi-Strand Wire Loop Seal is that the individual "wires" should be made of highly dissimilar materials, instead of the same materials as is currently done. This can potentially complicate and delay a splicing attack.

For example, if the individual wires have melting or flammability temperatures that are very different, thermal splicing methods like soldering, brazing, or welding that would work on one of the wires might destroy an adjacent wire made of a different material with a much lower melting or flammability temperature. If nothing else, materials with highly disparate properties require an adversary to become proficient at executing a wide variety of different splicing skills.

Materials that can be made into bendable "wires" with very dissimilar properties that would require very diverse (and sometimes difficult) splicing techniques include plastics and other polymers, glasses, ceramics including aluminum oxide, clays, aluminum alloys, pewter, stainless steels, titanium, self-lubricating micro-pore brass, plant stalks or fibers, textile fibers, and liquid- or gel-filled tubes. Tungsten is a potentially interesting material for tamper-detection because tungsten wires fray longitudinally when cut transversely.

Device #19 - Tie-Dye Seal

Type: novel conventional seal or complexity seal
Status: partially demonstrated
Applications: medium to high level security; can monitor volumes or areas, not just portals as with conventional seals

Color can be a difficult property to accurately counterfeit, thus making it of interest for tamper detection. Small, inexpensive solid-state color sensors with remarkable color resolution are now commercially available. These perform precise color measurements that were previously available only with expensive handheld colorimeters. For example, the TAOS TCS230 color sensor (~$2.50 each) outputs RGB color values from an electronics package approximately 5 x 6 x 1.7 mm in size.[31]

For a Tie-Dye seal (prototype shown in figure 27), the color sensor is placed inside the hollow body of the seal and rigidly mounted. A white LED is used to provide illumination inside the seal, though this does not need to run continuously, but can instead be turned on a random, unpredictable times so that a color spectrum can be measured intermittently.

Figure 27 - Working Tie Dye Seal prototype.

The inside of the seal is painted with a complex varying color pattern, not unlike the "Tie-Dye" T-shirts popular in the 1960's. Because this interior color pattern is so complex, it is difficult for an adversary to counterfeit it in order to try to defeat the seal. Moreover, any movement or change in location of the sensor with respect to the colored background is instantly detected as a substantial change in the color spectrum. (This might not be the case if the background was uniformly painted.) Any object such as a pick tool, even if quite small, that passes between the color sensor and the colored background will also instantly cause a change in the color spectrum. There is no one color that the tool could be painted that would allow it to blend into the background as it moves. Moreover, any ambient light that is allowed inside the seal when the seal is cut open will also be detected by the color sensor.

To make things even more difficult for an adversary, we can use 3 different LEDs, one red, one green, and one blue to provide the illumination inside the seal. They will be turned on in unison at random, unpredictable times to allow a color measurement. Each time they are turned on, however, each LED will have its own random intensity. Thus, the color spectrum seen by the color sensor at any given time cannot be easily predicted by the adversary in advance.

The microprocessor in the seal, on the other hand, can calculate the expected color spectrum for any combination of LED intensities. This is because it has run through color

calibration curves (when the seal was first installed) by illuminating each LED one at a time. This is a luxury not available to the adversary.

To spoof the color sensor, an adversary needs to measure the intensity of the 3 different LEDs, then figure out what color spectrum to counterfeit. This must be repeated each time the LEDs light up.

Note that this approach doesn't need to be limited to the interior of a seal. The concept can be scaled up to large containers, or even entire vaults or cargo-holds.

Device #20 - Adhesive Label Seal with Blink Comparator

Type: improved conventional seal & complexity seal
Status: demonstrated
Applications: medium level security

Pressure sensitive adhesive labels seals are popular for many security applications, including nuclear safeguards. These seals are inexpensive, and considered to be easy for relatively untrained personnel to apply. In our view, however, adhesive label seals do not provide reliable tamper detection.[32] We have demonstrated on many different products—including those used for nuclear safeguards—that they are typically easy to counterfeit, and even easier to lift and replace without leaving any noteworthy evidence.

Highly frangible label seals are sometimes used based on the hope that they can more reliably detect tampering. Such seals, however, are usually difficult for the seal user to apply without causing more initial damage than an adversary needs to inflict in executing an attack. Highly frangible seals, moreover, are not sufficiently robust for most transport applications.

Adhesive label seals become far more useful if "before" and "after" images of the seal can be compared visually using a blink comparator. Blink comparison is a 120-year old technique for quickly spotting any differences between two similar images.[33,34] The technique was used to discover the planet Pluto and is still used to efficiently discover new asteroids and other astronomical objects, and for medical imaging.[34,35]

For a blink comparison, registered images are alternately displayed, typically alternating at a rate of 4-40 times per second. Any difference appears quite dramatically as movement. This is the visual phenomenon that makes television and movies work: Still images are shown in rapid sequence. Any difference is interpreted by the human brain as movement.

In a mechanical blink comparator, separate photographs are viewed through a half-silvered mirror. The photos are alternately illuminated, typically so rapidly that they appear to be one image. Nowadays, a blink comparator is most easily implemented on a computer screen using digital images. We have written and demonstrated our own blink comparator program for use with seals, including adhesive label seals.

A blink comparator can be a remarkably powerful tool for allowing an observer to instantly spot even minor differences between two images. This is done at a subconscious level, so that it is nearly effortless for the observer to interpret blinker images. For many applications, a human observer properly using a blink comparator can outperform even very sophisticated computer image comparison algorithms, both in terms of speed and accuracy. It might seem likely that seal examinations would be highly subjective using a blink comparator. In practice, however, there is usually little or no disagreement between experienced users of blink comparators as to whether tampering is indicated.

For adhesive label seals, a blink comparator would be used as follows. First, the seal user applies the adhesive label seal, then records its digital image. If the seal (or container it is on) is likely to receive rough handling, or be exposed to a harsh environment or considerable dirt or dust, it is a good idea to protect the seal with a cover or removable plastic sheet. When it is time to inspect the adhesive label seal, a second image of the seal is recorded. At some point, the "before" and "after" images are compared using a blink comparator. This can be done quickly and easily in the field using a notebook computer if the "before" image can be securely transmitted to the seal inspector, perhaps using encryption. (If an adversary can tamper with either the before or after image, he can easily spoof the tamper detection.)

High resolution images are not needed for reliable blink comparisons of adhesive label seals. Images with 300 x 400 pixels are usually quite satisfactory, if in good focus. In our experience, the most effective blink comparisons occur on black and white images; color just distracts the observer. If color information about the seal is thought to be of interest, the red, green, and blue (monochrome) planes should each undergo a blink comparison separately.

We are convinced that the absolute key to blink comparisons is using a good kinematic mount. This is a simple, inexpensive mechanical mount that can be used to reproduce the camera position and orientation with remarkable accuracy.[36] If designed correctly, the kinematic mount is even self-temperature compensating.

It is common to try to use a blink comparator for other (non-seal) applications without using a good kinematic mount or even no kinematic mount at all. This is a big mistake, and we suspect accounts for why some people find blink comparators only marginally useful. Attempting to register (that is, "align") the images after the fact in a manner that corrects for different camera optics, locations, angles, or even skew, is invariably unsatisfactory, even though the registration may look visually acceptable.

Another advantage of a good kinematic mount is that lighting conditions are relatively unimportant. We have demonstrated for adhesive label seals that a blink comparator can allow us to detect very subtle evidence of tampering even if the before and after images were recorded with very different mean illumination levels, and severely different spatial gradients in the lighting.

It is possible to use different cameras, and even different kinematic mounts at the shipping and receiving ends. The cameras, however, should be the same model and use identical optics. The kinematic mounts need to be well designed.

Device #21 - Beads-In-A-Box Seal

Type: complexity seal
Status: demonstrated, including for moving cargo
Applications: medium to high level security; can monitor volumes, not just portals as with conventional seals

Figure 28 shows a polycarbonate box (25 x 25 x 25 cm) containing transparent, compressible toy balls of various colors. These balls are multi-faceted and close-pack fairly efficiently when pressure is applied from above by the layer of foam located at the top of the box, just inside the hinged lid. (For real cargo, the polycarbonate box can be replaced with an ordinary crate or box having at least one window so that the contents can be photographed.)

Also visible in figure 28, near the center of the polycarbonate box, is a wooden jewelry box. This contains the "assets" that we wish to check for tampering. In order to get to the assets, an adversary must move the multi-faceted balls. To cover his tracks, he must then put them all back with considerable accuracy, in terms of both 3-dimensional position and angular orientation. Indeed, even just opening the lid causes enough change in the tension that a number of the balls move irreversibly.

An adversary cannot glue the balls individually back into position, because when it is time to inspect the container, the seal inspector will check that the balls are all independent when he opens the container.

The most effective way to detect movement of the balls is with a digital camera and a blink comparator. It is very easy to tell the difference between a box that has not been opened, one that has had the lid briefly opened, and one where an adversary removed, then later replaced the assets at the center of the box. This is true even for a box that has been handled very roughly during transport.

Figure 28 - An example of a beads-in-a-box seal. The "beads" in this case are multi-faceted silicone balls. Any access to the box disturbs the balls, which can be easily detectected with a blink comparator.

Figure 29 - Another approach for roughly-handled cargo shipments where multi-faceted plastic jewelry beads are hung in a plastic bag that is allowed to freely swing. The beads are relatively stationary with movement of the container or vehicle the bag is in, but readily move when the bag is disturbed or opened.

If the box will be subject to dropping or severe shaking, a few of the balls move slightly from such rough handling, but it is easy to tell the difference between this and tampering. Nevertheless, if desired, the amount of movement likely to occur during shipment can be tested prior to shipment by deliberately shaking or dropping the box, then comparing the "before" and "after" images with a blink comparator. This will indicate which of the few balls should be discounted if they move slightly after the real shipment reaches its destination. (None of this is relevant, of course, if the assets remain stationary during the period of time we are concerned about tampering.)

For especially rough shipments, a better technique is depicted in figure 29. In this case, multi-faceted jewelry beads are used. These, along with the asset(s) of interest, are vacuum packed inside a clear, thin-walled plastic bag. The tension on the plastic bag, caused by the pressure differential between the inside and outside of the bag, keeps the beads virtually frozen in place. If the bag is suspended from a pendulum mount, the beads are virtually immune from inadvertent movement short of handling so rough that it damages the cargo.

Either the box or bag technique can be scaled up or down over a considerable size range. The balls or beads are totally reusable, making this a very inexpensive seal. With a good kinematic mount, only a few seconds are required to record a digital camera image and compare it with the "before" image using a blink comparator on a notebook computer. Of course, both the before and after image must be securely transported or transmitted to the same location (not necessarily the cargo destination) so that they can be compared to determine if tampering took place.

Neither the balls nor the beads in figures 28 or 29 interfere with gamma ray measurements, or rf communications. Also, the balls or beads can pack around electronic cables leading to or from the interior, or camera lenses. Thus, the Beads-in-a-Box seal might make be useful as inexpensive, reusable, "transparent" tamper detection for safeguards monitoring equipment.

Device #22 - Theodolite Seal

Type: complexity seal
Status: concept
Applications: medium level security

The Theodolite "Seal" is a remote, non-contact, optical method for determining if a container in a vault, warehouse, or cargo hold has been disturbed. (If the containers are in a moving transport vehicle, they must be tied down well.)

The idea behind the Theodolite Seal is that it can be difficult and time-consuming for an adversary to exactly reposition one or more containers (or their lids) after tampering. This is especially the case if the lid or underside of the container is designed with a mechanical hysteresis mechanism that does not allow it to return to its original position or orientation

when the load is lifted. There are many possible mechanical designs for such hysteresis container or lid supports.

Changes in a container's position or orientation (or that of its lid) as small as a few μmeters and a few arc-seconds, respectively, can be measured with a nearby digital camera, using a good kinematic mount and a blink comparator technique.

Even from a considerable distance, the position of a container or lid can be quickly measured with good accuracy. At a distance, a camera with a telescopic lens, plus a blink comparator can be used. Another approach is to use a commercial 3 arc-second theodolite used for surveying (cost< $5K). This can detect a translation as small as 700 μm (perpendicular to the line of sight) from a distance of 50 meters. At the same distance, a rotation of 5 arc-minutes can be detected for a container or lid of diameter 1 meter. (This is near the diffraction limited resolution of the theodolite.)

Checking for tampering by using a theodolite or camera with a blink comparator can be done in a non-contact manner that does not interfere with other tamper or intrusion detection devices. A clear line of sight, however, must be available to the container or lid being checked.

The camera or theodolite can be taken away between measurements, especially if a good kinematic mount is used for accurate repositioning. Different theodolites or digital cameras can be used at the shipping and receiving ends to make the "before" and "after" measurements, thought identical models should be used.

The exact position of containers can also be mapped out with a variety of commercial 3D profiling instruments, including laser 3D scanners, holographic and interferometric devices, structured light profilers, and coordinate measurement machines.[37] Typical resolutions are 3 mm at a distance of 100 meters, to a few μm at 1 meter.

Device #23 - Epoxy Mixer Seal

Type: novel conventional seal
Status: concept
Applications: low to medium level security

The Epoxy Mixer seal contains two colored liquids that get mixed when the seal is opened. An adversary would find it difficult to separate the liquids once they mixed in order to try to hide the fact that the seal had been opened. (This is especially true if the liquids are designed to react chemically, or change color when in contact.) This might leave counterfeiting as the adversary's simplest attack.

The most efficient way to mix the liquids for a passive seal is to use an epoxy mixing baffle of the sort shown in figure 30.

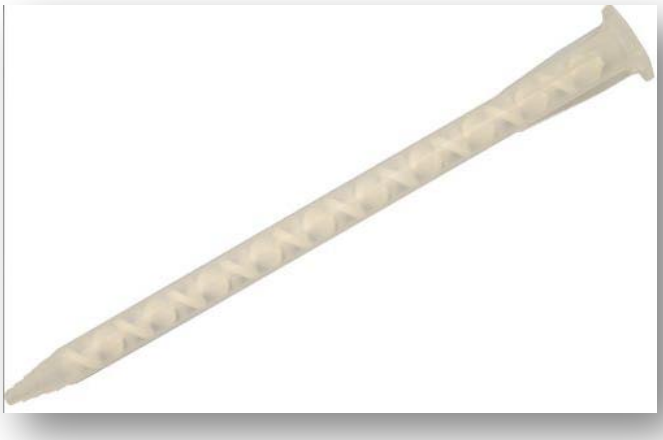

Figure 30 - An epoxy mixing tube. This is a baffle used to mix two-component epoxies as they flow down the tube.

Device #24 - Aeolipile (Spinning Gas Jet) Seal

Type: password (anti-evidence) seal
Status: concept
Applications: high level security; can monitor volumes, not just portals as with conventional seals

In 50 AD, Hero of Alexandria invented the world's first steam engine, called an aeolipile.[38] Water was heated such that the resultant steam could pass through pipes into a hollow sphere. See figure 31. The sphere had two jets through which the steam could escape, generating thrust that caused the sphere to rapidly rotate about its axis. It's not clear if Hero's device was ever actually built. In any event, the aeolipile was never considered anything but a toy until more than a thousand years later.

Now in order to keep a valuable asset (or cargo) safe from intrusion or tampering, it is generally placed inside some container. We and others have shown how easy it is to quickly penetrate container walls without leaving obvious evidence. These surreptitious entries, however, are substantially more difficult if the walls are constantly moving. Constantly moving the heavy walls of a conventional container, isn't practical, but constantly spinning a lightweight aeolipile requires little energy. The hollow, spinning aeolipile sweeps out a volume in space that cannot easily be penetrated by an adversary without interfering with the rotation of the aeolipile shell.

Figure 31 - Hero's Aeolipile. of Alexandria invented the world's first steam engine, called an aeolipile.[38] Water was heated such that the resultant steam could pass through pipes into a hollow sphere. The sphere had two jets through which the steam could escape, generating thrust that caused the sphere to rapidly rotate about its axis. It's not clear if Hero's device was ever actually built. In any event, the aeolipile was never considered anything but a toy until more than a thousand years later.

The assets to be monitored for tampering go inside the aeolipile, on a stationary platform supported by an internal frame mounted to the hollow rotation axis of the aeolipile. The spinning aeolipile shell—the equivalent of the sphere in figure 22—can be made out of thin plastic or aluminum, balsa wood, or even paper. It can be a sphere, cylinder, or other cylindrically symmetric shape, and scaled up or down to the appropriate size.

The aeolipile's rotation is powered—not by steam—but by a small electric motor and battery, or by a tank of compressed gas or a small external air pump. (If blades are attached, the aeolipile can even be driven in a non-contact manner by a nearby fan or air jet.) The lightweight spinning aeolipile represents no safety hazard because it can be stopped simply by reaching out and touching it, without harming one's hand. The reduced rotation rate, however, will be detected and interpreted as tampering.

To monitor the rotation rate, a small battery-powered microprocessor is placed inside the spinning aeolipile on the stationary support platform, along with the assets of interest. It can detect a change in rotation rate various ways, including with a photodiode, a shaft encoder, or with a Hall Effect magnetic sensor measuring the rotation of a weak magnet

placed on the spinning axle or aeolipile's shell. Any attempt by an adversary to gain access to the assets (including attacking along the rotation axis of the aeolipile) necessarily requires altering the rotation speed. This is immediately interpreted by the microprocessor as intrusion or tampering. The microprocessor then erases the anti-evidence stored in its memory.

The good guys can check on the status of the anti-evidence at any time, including while the aeolipile is still rotating, by sending the password to the microprocessor using rf signals. The microprocessor can respond by talking (as with the Seal #4 - the Talking Truck Cargo Seal), or it can instead transmit the secret anti-evidence by a return rf signal.

Tags

Device #25 - Time Trap as A Product Anti-Counterfeiting Tag

Type: a product anti-counterfeiting tag
Status: working prototype
Applications: countermeasure to product counterfeiting; requires some technical sophistication to defeat

The Time Trap (Device #2) is a trap or seal. It can, however, also be used as a product anti-counterfeiting tag. The 2-letter hash that authenticates the time can be thought of as a time-varying product "serial number". The customer would only be allowed to view the authentication hash a few times. The hash could be looked up on the Internet or called in over the telephone. Alternatelly, the hash could be checked using a computer program or handheld device that would only show authentication hashes for the current time.

In order to counterfeit the product, the bad guys would need to know future authentication hashes for at least one legitimate product. This would require reverse-engineering the device and beating the intrusion detectors.

Device #26 - Virtual Random Numeric Tokens

Type: a product anti-counterfeiting (virtual buddy) tag
Status: concept
Applications: countermeasure to product counterfeiting; difficult to defeat in volume

The idea of virtual random numeric tokens is deceptively simple.[56] The manufacturer of a mass-produced product, lets say pharamaceuticals as an example, puts an extra "Bottle ID" on each bottle. This is a unique, random, unpredictable number chosen for each bottle in a given lot. (The manufacturer starts over again with each new lot.) The number of Bottle IDs must be at least 1000 times greater than the number of bottles in the lot.

Customers anonymously "call-in" to the manufacturer (or his representative) via the Internet or telephone to see if they have a valid Bottle ID for the given lot number.

Product counterfeiters have the problem that if they guess Bottle ID numbers, most of the ones they guess will be invalid and the customers will be immediately alerted that they have a fake.

Product counterfeiters can presumably get hundreds of valid Bottle ID numbers, but this does not help them to do mass counterfeiting because the fact that duplicate valid bottle numbers keep getting called in will make it possible to tell the calling-in customers that they probably have a fake with high probability. Typically, more than 98% of the counterfeit products called in will be detected. Malisciously calling in fake Bottle IDs has very little impact.

Volume customers of the product can also check their past and current stock for duplicate Bottle IDs without calling in. This works well to detect fakes because counterfeit products tend to cluster in the supply chain.

There are several important points about virtual random numeric tokens that are often overlooked. This is NOT the same thing as serialization! It is not track & trace nor a provenance method, though it can be use in conjunction with such techniques. The virtual random numeric token is a buddy tag that does not need to be physically attached to the bottle, co-located with it, or generated at the factory. Also, manufacturers that try to implement something like virtual random numeric tokens typically make a number (or most!) of approximately 3 dozen mistakes in doing so. Please contact the authors for more information.

We use virtual random numeric tokens for our wine authenticity device shown in figure 33.[1,39]

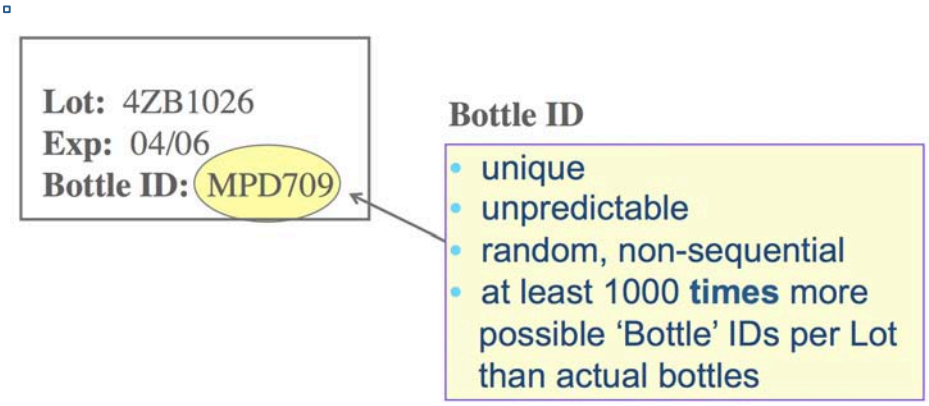

Figure 32 - A virtual random numeric token requires a product ID (or bottle ID for bottles) that is not the same thing as serialization.

Figure 33 - Wine authenticity prototype. The inexpensive, reusable silver cap on top of the wine bottle can determine if the wine bottle has ever been opened (using an anti-evidence seal), and if it is an authentic bottle (using a virtual numeric token). The cap is connected to the Internet using a cable to "call-in" the virtual numeric token.

Real-Time Monitoring

Device #27 - Town Crier Monitoring

Type: an anti-evidence type of real-time monitoring
Status: working prototypes of different designs
Applications: high level security for vaults, warehouses, and moving cargo. Also, a possible technique for complicating attacks on intrusion sensors.

The anti-evidence approach can also be used for real-time monitoring.[17,40,41] A "real-time monitor" is a device or system that watches over an object or container, and then produces an immediate alarm if the object or container is removed, tampered with, or experiences unauthorized intrusion. The alarm is typically intended to scramble a guard or police force.

The alarm signals issued by most conventional real-time monitoring systems are often easy to block or jam. More sophisticated systems may rely on high-bandwidth two-way communication, radio frequency signals, sensor status and state of health checks, data authentication or encryption, and/or complex hardware and software. The resulting

complexity often opens up new attack vectors for an adversary, increases costs, and can impede transparency and negotiability for nuclear treaty monitoring.[17,40,41]

With the "Town Crier" (anti-evidence) approach to real-time monitoring (see figure 34), when unauthorized access, tampering, or theft is detected, we don't send an alarm that can be easily blocked or jammed. Instead, as long as everything is fine, we have the real-time monitoring system occasionally transmit a simple "All OK" byte called the "bingo number". The correct bingo number at any given time is known only to the monitoring system and to the good guys listening in. Should the correct bingo number fail to arrive when expected, trouble is indicated. Unlike blocking an alarm signal, the bad guys gain nothing by blocking the "All OK" signals. They can try to counterfeit the bingo number, but have only a 1/256 (0.4%) chance of guessing one bingo byte correctly, 1/65536 (0.002%) chance of guessing two correctly, etc.

Figure 34 - The real-time Town Crier prototype monitor on the left is meant be inside or attached to the assets to be monitored. It wirelessly sends a pseudo-random "bingo number" every 4 seconds to the listening unit on the right which is located at a guard station or with a guard. (In actually usage, it would be more like one bingo number transmitted per minute). For demonstration purposes only, the transmitted bingo number (A7 at this instant) is displayed on both the real-time monitor (left) and the listening unit (right). (The bingo number is also spoken by both units, again only for demonstration purposes.) The bad guys don't know which bingo number is due up next, and if they break into the real-time monitor, their trespassing is detected and information about future bingo numbers is erased in less than 1 μsec. If the real-time monitor is disturbed (one of many possible indications of "tampering"), the unit erases information about future bingo numbers and stops sending them. When no bingo numbers or the wrong ones are received by the listening unit, tampering or theft is suspected, and the listening unit sounds a conventional alarm (though it, too, could alternately pass along an anti-evidence "All OK" signal to a higher level.) The retail cost of parts for each unit is less than $55, and less than $15 if the superfluous voice module and LCD display are eliminated.

The advantages of this Town Crier monitoring approach include simplicity, low-cost, the use of only very low bandwidth (a few bits to ~1 byte per minute), one-way communication (we listen for the bingo numbers but don't try to talk to the real-time monitor), and high security. Blocking an alarm, counterfeiting the real-time monitoring hardware, or hacking into the monitor through a communications channel are no longer useful attacks for the adversary.

It is interesting to note that if sensors inside a security device communicate to the CPU using a Town Crier approach, it would be much harder for an adversary to spoof the sensors by shorting or jumpering them.

The name "Town Crier" comes from the town criers of medieval European towns. If Vikings were to attack, they might be able to overpower the sentries before the sentries could yell out a warning. The town crier, however, would cry out an "All OK" message at predetermined times. If the town's people failed to hear the familiar voice of the Town Crier giving the "All OK" signal at the correct time, they would grab their weapons and prepare to defend their town.

Device #28 - Chirping "Tag & Seal"

Type: A Town Crier type of real-time monitor that has certain attribues of a tag and a seal.
Status: working prototypes
Applications: high level security for vaults, warehouses, sealed radiological sources, nuclear material, and cargo

Radio frequency (rf) communication can be difficult to work with.[16] Indeed, rf is a battery power hog, prone to interference, tends to attenuate or detune when near metals or liquids, often doesn't work well around corners, and can create safety and security problems (real or perceived) inside nuclear facilities. Spoofing, hacking, counterfeiting, blocking, jamming, or eavesdropping of rf signals remotely is a continual concern and relatively easy to do, especially for radio frequency identification devices (RFIDs).[16] Complicating the use of rf for international applications is the fact that different countries have disparate regulations and spectrum allocations for rf signals.

To avoid all these problems with rf, we believe alternative communication methods should be considered, especially for relatively short range monitoring, e.g., across a storage vault, inside a cargo hold, or within a nuclear work area or facility. Infrared or acoustical/ultrasonic signals have, we believe, many potential advantages over rf that have not been fully explored or exploited.

Figure 35 shows a prototype Town Crier real-time monitoring device that we call the "Chirping Tag and Seal". (This is something of a misnomer since it is primarily a real-time monitor). Instead of using rf, this device sends the anti-evidence "All OK" signal using acoustical chirps. The acoustical chirps are generated using a commercial resonant chirp

buzzer, model PKM24SPH3805 made by Murata manufacturing.[42] These "chirpers" are often found on smoke detectors, where they chirp once per minute for many months to indicate that the battery is nearly dead. It costs approximately $1.50 in retail quantities and operates at approximately 3.8 Hz. Most environments (including nuclear facilities and moving trucks) are relatively quiet at this frequency, with human voices lying mostly in the range 100 – 1000 Hz.[43]

Figure 36 shows the acoustical signal generated by the chirper, which lasts approximately 23 msecs. Figure 37 shows the FFT frequency spectrum, with the peak centered around 3.8 kHz.

Figure 35 - The Chirping Tag and Seal, top view (left) and bottom view (right). This prototype device is based on the use of an inexpensive PIC 12F629 microprocessor and a $1.78 (retail cost) resonant chirping buzzer. The device operates for many months on 2 coin batteries.

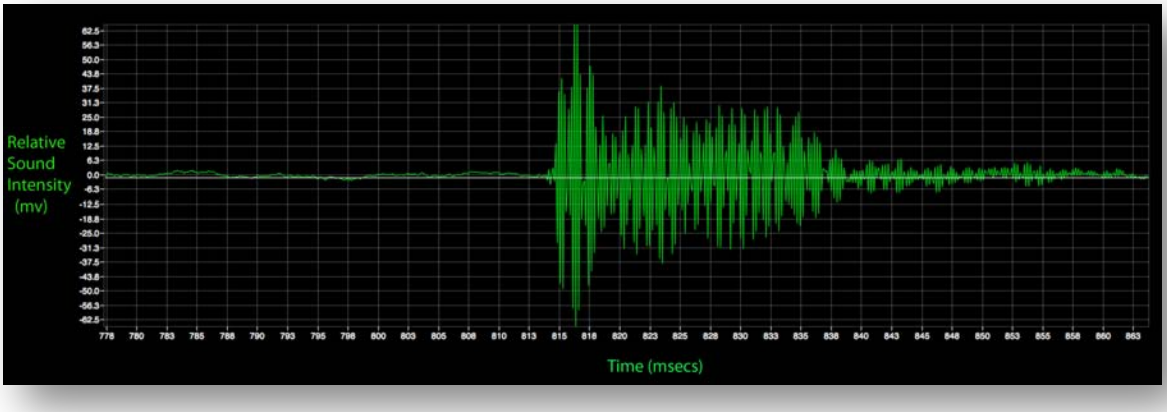

Figure 36 - The relative sound intensity of 1 chirp as a function of time as recorded by a microphone.

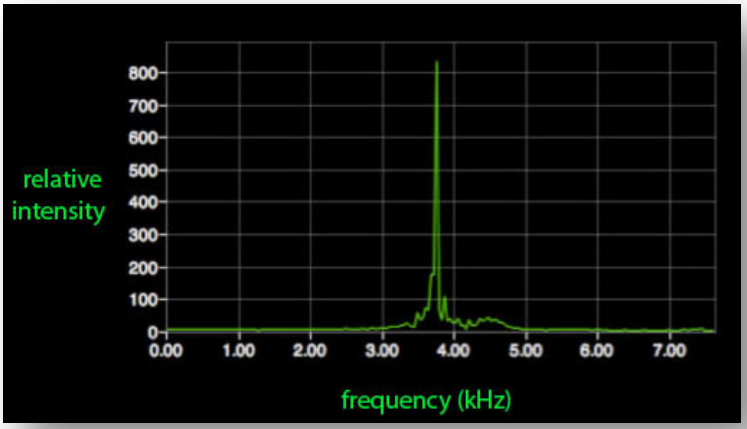

Figure 37 - The frequency spectrum of 1 chirp.

The maximum sound output of the chirper is 90 dB at a distance of 10 cm, though it uses very little battery power. The chirps go around corners quite effectively. Along a straight line, we have demonstrated the ability to detect the chirps using an inexpensive microphone at a distance in excess of 250 meters, outdoors in a noisy environment.

The parts for the Chirping Tag and Seal shown in figure 35 cost under $5 in retail quantities. This includes a light sensor that can determine if the device has been picked up or moved. Depending on what other tamper/intrusion sensors one wanted to add to the device (and there are many options), the retail cost of parts might be higher.

The Chirping Tag and Seal is a much simpler version of the Town Crier prototype that was shown in figure 35 not just because it avoids the use of rf, but also because it doesn't even need to transmit an actual bingo number or modulate the (acoustical) chirp it emits. The "All OK" signal for our Chirping Tag and Seal is the exact time when the chirp is generated. As long as everything is fine, the device will "chirp" at pseudo-random, unpredictable times. Only the good guys know when the next chirp is due. For the demonstration prototype shown in figure 35, the chirps come once every 3 seconds on average. In a real application, however, a chirp might only be generated once every minute or two on average. Once tampering/intrusion is detected (or if the device is removed), the chirping stops, the remote listening microphone fails to hear the next chirp when it is due, and the information needed to determine when future chirps are due to occur is erased in less than 1 μsec.

Note that it is only the time to the next chirp that matters, not the absolute time. Thus, highly accurate clocks are not needed. The time to the next chirp can be determined using a pseudo-random number generator (PRNG). An adversary would have to collect chirp data for many weeks before he would have sufficient data to confidently be able to figure out the PRNG. For the best security, however, the times

between chirps should be random numbers generated in advance by hardware, and stored on the device as a kind of one-time keypad.

The sound chirps are short enough that many different chirping devices can be operating in the same volume, all chirping away on different schedules. Only 1 microphone is needed to listen to hundreds of different Chirping Tags and Seals simultaneously. The chirps would overlap very infrequently given their short duration, but the good guys know when each overlap is coming and can deal with the situation appropriately. (The average time before any two chirpers overlap, each chirping randomly once per minute on average, is almost 2 days.) Should overlapping nevertheless become a problem, the chirp duration (23 ms) could be decreased, the average time to the next chirp increased, and/or different frequencies used for different units.

It is not necessarily desirable to conclude that tampering, intrusion, or theft has occurred after just one missed chirp. Two or three missing chirps in a row might be a better threshold for any given Chirping Tag and Seal.

Note that the acoustical chirp could be replaced with an ultrasonic chirp (to be less annoying to people), but the range would be less. Alternatively, an ultra-short flash from an infrared LED could be used. Rise times can be a short as 100 pico-seconds. The ability to go around corners, however, would not be as good in either case as is possible with acoustical chirps.

Because of its simplicity, low cost, and small size, we believe the Chirping Tag and Seal would be particularly useful for monitoring sealed radiological sources. Instead of attaching a security device directly to the sealed radiological source (which presents a number of practical problems), we are instead designing a thin, lightweight plastic case to hold each source. For many authorized radiological applications, the sealed radiological source could be used without having to even remove it from the case. Our Chirping Tag and Seal would do the random audible chirping to assure that the sealed source was still present, and also check whether the case has been opened or compromised, and that the Chirping Tag and Seal was still attached to the case. Any evidence of tampering would cause the chirping to stop. The unauthorized removal of the case and chirper would cause the chirps to no longer be detected.

While the Chirping Tag and Seal is fundamentally a real-time monitor, it can also be used as a tag and as a seal. It can serve a tag function by identifying the asset it is attached to, not with a unique serial number such as done with an optical barcode or an RFID, but rather by chirping at a specific time. It can act as a seal if the chirps from one or more such devices are collected by a microphone and analyzed by a microprocessor that is itself part of an anti-evidence seal. We can envision, for example, a truck cargo area full of valuable assets in transit, each with a Chirping Tag and Seal attached. (Reasonable road noise causes little acoustical interference.) When the truck arrived at its destination, the listening microprocessor would be queried as to whether tampering, intrusion, or theft had occurred based on its monitoring of the

chirps. While there would be real-time monitoring inside the truck, the results would be available only after an inquiry occurred at the receiving location.

Device #29 - Live & Local Video Authentication

Type: technique for athentication of surveillance video (or other high-bandwidth sensors)
Status: proof of principle
Applications: high level security for nuclear treaty monitoring, and for vaults, warehouses, and cargo-holds

Current video surveillance techniques for nuclear treaty monitoring and other high-level security applications make extensive use of expensive custom monitoring cameras, tags, seals, tamper-evident enclosures, and encryption/data authentication (often resulting in poor spatial and temporal resolution), and secret keys & passwords. These are costly, complicated, time-intensive, not conducive to negotiability and transparency for nuclear treaty monitoring, and the security they provide is often illusionary. Moreover, the need for a secure chain of custody for the hardware and software, starting at the factory, is usually unmet.

Potentially, these things are unnecessary—or at least their use could be greatly reduced—if real-time streaming video is allowed and can be recorded for future analysis. This would make it possible to use comercial-off-the-shelf video cameras (with the low cost and excellent quality control). Various challenge/resoponse tests at nanosecond to second time scales can help veryify that the video is both live (not pre-recorded) and being generated locally (to within a few kilometers).

The streaming of the video frames, combined with these challenge/response tests leave the adversary with inadequate time to counterfeit or tamper with the video images on the fly. No other tamper detection or encryption/data authentication is needed (at least for the video camera) if the temporal response of the steaming video system is understood.

We have conducted a preliminary proof of principle for this concept. It could potentially also work for other kinds of high-bandwidth sensors—not just video cameras.

Device #30 - Rapid Sampling Tool

Type: field tool
Status: 3 U.S. patents, working field units
Applications: counter-terrorism, nonproliferation, emergency responders, drug raids, waste management

We have designed and built simple field tools that work with standard battery-powered hand drills. They allow the user to sample liquids or flowable powders without opening

the container, or allowing any of its contents to escape. Very types of containers can be sampled, up to 1.4 cm thick and 8-atmospheres of internal pressure. See reference [57] for more information.

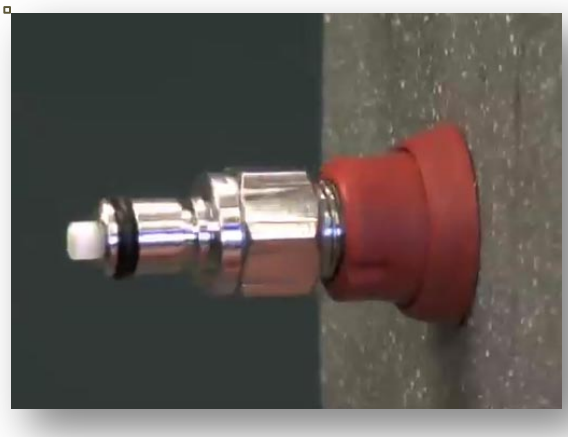

Figure 38 - One version of the Rapid Sampling Tool.

Access Control

Device #31 - Image Algorithm Password

Type: an alternate kind of graphical "password" for access control for rooms, buildings, or computer log-ons
Status: demonstration software
Applications: high level security for limited access areas or secure computing systems

There are numerous concepts for passwords based on graphical images or other cognitive authentication approaches.[44-55] We believe our approach has two strong strong advantages over other approaches: (1) It is very difficult for an adversary to figure out the "password", even if he knows the person well and has watched her enter the "password" many times, and (2) The algorithm is easy to remember even after a long time of not being used.

With our approach, each authorized person has to remember only 2 things: An "anchor algorithm" question about what is on the display monitor, and a vector. Examples of an anchor algorithm question can include:

1. Which object costs less than $5?
2. Which object can typically be found in the kitchen?
3. Which object contains a lot of wood?

4. Which object did not exist in the year 1900?
5. Which thing is alive?
5. Which object has a name (label) with 2 vowels in it?
6. Which icon is "facing" to the left?

Each time a subject wishes to gain physical or computer access, she is shown a grid of cllipart images ("icons"), such as in figure 38. Her job is to scan the grid and find the one icon that answers her anchor algorithm question. This is called the "anchor". If she cannot find an appropriate anchor, she is allowed to request a new set of icons (without selecting any from the original grid). Once an anchor is identified, she then selects a different icon that is displaced from the anchor by her personal vector. She may need to repeat the process for multiple grids with different icons to gain access if better security is desired.

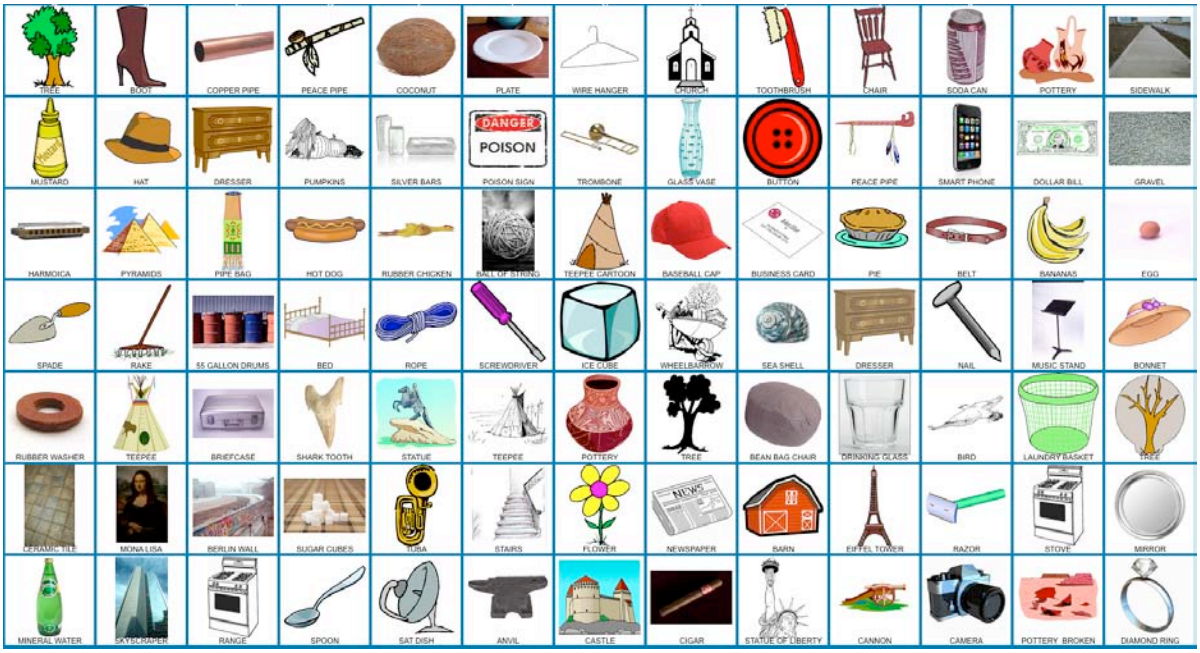

Figure 38 - 91 different icons. Each icon (or "clip art") has a name (label) that defines what it is.

It is a complex problem for an adversary to try to work backwards and figure out the anchor, then figure out the algorithm. There are, for example, 25 possible vectors away from the anchor, given no more than 3 total steps: ±3 Vertical icons (up or down) + 0 Horizontal; ±2 Vertical + 0 or ±1 Horizonal (left or right); ±1 Vertical + 0, ±1, or ±2 Horizontal; 0 Vertical + 0, ±1, ±2, or ± 3 Horizontal).

Before using the system, the user must enter a ID badge or PIN or password to identify the person and thus let the system look up her anchor question and vector.

Our demonstration software for this technique randomly fills the grid with icons that unambiguously do not fit each person's anchor question. This has previously been determined by going though all the icons and asking a panel of people whether each icon

fits a given anchor question well, poorly, or it is unclear. Only when there is very strong consensus is an anchor question assigned affirmatively to a given icon.

Once the grid is filled with icons that unambiguously do not fit the relevant anchor questons (with no duplication of icons allowed), one of the icons is randomly chosen and replaced with an icon that *does* unambiguously fit the anchor question. The person looks through the grid, finds the one icon that fits her anchor question, then using the vector to select an icon.

Anchor questions can be re-used for different people if they are given different vectors. If the vector takes the user off the grid, she simply wraps around. A rotatable sphere for displaying the icons would eliminate the confusion of wrapping around.

Preliminary experiments suggest that most people can learn how this concept works and learn their anchor question and vector in just a few minutes of explanation followed by some practice. Most people had little problem in quickly finding the relevant icon for their anchor question. There is evidence that people could remember their anchor and vector even after sevearal months of not using the system, especially if we used particularly vivid training methods.

While this system would probably not be practical for access control for a large number of employees—because of the effort required to set it up and train the users—this approach might make some sense for high security applications where there are only a modest number of authorized individuals.

Device #32 - Physical Isolation from Ethernet and the Internet

Type: cyber physical access control
Status: working unit
Applications: slight improvement in cyber security; security awareness tool

A RJ45 switch box (~$9 retail) can be used to disconnect a computer from its Ethernet connection for times when you don't need to be connected (for example) to the Internet, yet want to instantly re-connect when you do. See figures 39 and 40. In addition to the switch box, two Ethernet patch (8P8C) cables are needed.

With the switch box, there is no need for fumbling with cables or software to disconnect/reconnect the Ethernet port when it is not needed. Of course this doesn't address wifi or Bluetooth connections, nor help all that much if you are being personally targeted by hackers, but it can potentially cut down on opportunities for cyber attacks or mistaken release of sensitive data.

Figure 39 - Front view of a commercial RJ45 switch box with labels added by the authors.

Figure 40 - Rear view of the switch box. A cable is used to connect the I/O port to the Ethernet router, while another cable connects the A port to the computer's Ethernet port. No cable is connected to B for this application.

Device #33 - Sticky Bomb Detector for Vehicle Security

Type: vehicle access control
Status: proof of principle on 2 different concepts
Applications: counter-terrorism, vehicle and cargo security

We have conducted a proof of principle for 2 different methods of detecting when an improvised explosive device has been attached to a parked vehicle.[58] One technique is based on detecting an increase in tire pressure when even a very small amout of weight is added to (or subtracted from) a vehicle. The other techique is based on detecting the magnet that is often used to attach such "sticky bombs".

Both techniques are relatively inexpensive and could possibly also work on moving vehicles, with a reduce level of sensitivity. Both techniques can work as either tamper detectors (after the fact detection) or real-time monitors.

There are other potential applications for vehicle and cargo security. See reference [58] for more information.

Acknowledgements

This work was supported by the U.S. Department of Energy (DOE), Office of Basic Sciences, and the National Nuclear Security Administration (NNSA) under contract #DE-AC02-06CH11357. The views expressed in this article are those of the authors and should not necessarily be ascribed to Argonne National Laboratory, DOE, or NNSA.

We are grateful to Anthony Garcia, Leon Lopez, Ron Martinez, Adam Pacheco, and Sonia Trujillo for ideas, design concepts, machining, and other assistance. Nate Briston made major contributions to the design and construction of the Time Lock and helped with other technical details. Veronica Manfredi conducted much of the testing of the Image Algorithm Password technique and assisted in other ways. Jim Vetrone did much of the experimental testing on the sticky bomb detection techniques. We also benefited from the help of Marissa Faler, Sam Fuchs, Christopher Folk, Gregory Bylsma, and Eric Baca.

References

1. Argonne Vulnerability Assessment Team, http://www.ne.anl.gov/capabilities/vat/

2. Phil Rogers, "Most Security Measures Easy to Breach", http://www.youtube.com/watch?v=frBBGJqkz9E

3. Boonsri Dickinson, "At Argonne National Lab, Closing the Curtains on 'Security Theater'", November 9, 2010, http://www.smartplanet.com/technology/blog/science-scope/at-argonne-national-lab-closing-the-curtains-on-security-theater/5167/

4. RG Johnston and JS Warner, "Debunking Vulnerability Assessment Myths", *SecurityInfoWatch*, August 6 & 13, 2013,
Part 1:
http://www.securityinfowatch.com/article/11078830/experts-discuss-commonly-held-misconceptions-about-vulnerability-assessments
Part 2:
http://www.securityinfowatch.com/article/11108983/experts-discuss-the-characteristics-of-good-vulnerability-assessors

5. RG Johnston and ARE Garcia, "An Annotated Taxonomy of Tag and Seal Vulnerabilities", *Journal of Nuclear Materials Management* **28**(3), 23-30 (2000).

6. RG Johnston, ARE Garcia, and AN Pacheco, "Efficacy of Tamper-Indicating Seals", *Journal of Homeland Security*, April 16, 2002, http://www.homelandsecurity.org/journal/Articles/displayarticle.asp?article=50

7. JS Warner and RG Johnston, "Why RFID Tags Offer Poor Security", Proceedings of the 51st INMM Meeting, Baltimore, MD, July 11-15, 2010.

8. RG Johnston, "Lessons for Layering", *Security Management* **54**(1), 64-69, (2010).

9. RG Johnston, "New Research on Tamper-Indicating Seals", International Utilities Revenue Protection Association News, **16**(1), 17-18 (2006).

10. RG Johnston, "Tamper-Indicating Seals", *American Scientist* **94**(6), 515-523 (2005).

11. RG Johnston and JS Warner, "The Doctor Who Conundrum: Why Placing Too Much Faith in Technology Leads to Failure", *Security Management* **49**(9), 112-121 (2005).

12. RG Johnston and JS Warner, "What Vulnerability Assessors Know That You Should, Too", *Asia Pacific Security Magazine* **50**, 40-42 (2013)

13. JS Warner and RG Johnston, "Chirping Tag and Seal", Proceedings of the 51st INMM Meeting, Baltimore, MD, July 11-15, 2010.

14. RG Johnston, EC Michaud, and JS Warner, "The Security of Urine Drug Testing", *Journal of Drug Issues,* **39(4)** 1015-1028 (2009), http://jod.sagepub.com/content/39/4/1015.full.pdf+html

15. RG Johnston, "Tamper Detection for Safeguards and Treaty Monitoring: Fantasies, Realities, and Potentials", *The Nonproliferation Review* **8**(1), 102-115 (2001), http://www.autoid.org/1_2003%20Documents/Sep/104sc4wg2n0121_Johnston.pdf

16. RG Johnston, "The 'Anti-Evidence' Approach to Tamper-Detection", *Packaging, Transport, Storage & Security of Radioactive Material* **16**(2), 135-143 (2005).

17. RG Johnston and JS Warner, Unconventional Approaches to Chain of Custody and Verification", Proceedings of the 51st INMM Meeting, Baltimore, MD, July 11-15, 2010.

18. RG Johnston and ARE Garcia, *Triboluminescent Tamper-Indicating Device*. U.S. Patent 6,394,022, April 28, 2002.

19. AJ Walton, "Triboluminescence", *Advances in Physics* **26**(6), 887-948 (1977).

20. G Bourhill, LO Palsson, IDW Samuel, IC Sage, IDH Oswald, and JP Duignan, "The Solid-State Photoluminescent Quantum Yield of Triboluminescent Materials", *Chemical Physics Letters* **336**(4), 234-241 (2001).

21. I Sage, R Badcock, L Humberstone, N Geddes, M Kemp, and G Borhill, "Triboluminescent Damage Sensors", *Smart Materials and Structures* **8**(4), 504-510 (1999).

22. RG Johnston, *Magic Slate Seal*, Los Alamos National Laboratory Report LAUR-02-6848 (2002).

23. JE Amoore and E Hautala, "Odor as an Aid to Chemical Safety", *Journal of Applied Toxicology* **3**(6), 272-290 (1983).

24. RJ Versic, "Microencapsulation and Scented Fragrance Inserts", *Drug & Cosmetic Industry* **144**(6), 30ff (1989), http://www.rtdodge.com/fr-insrt.html

25. TH Elmer, *Porous and Reconstructed Glasses in Engineered Materials Handbook*, Volume 4: *Ceramics and Glasses*, pp. 427-432 (1992), ASM International, Materials Park, OH, http://www.corning.com/lightingmaterials/products/vycor.html

26. RG Johnston and ARE Garcia, *Magnetic Vector Field Tag and Seal*. U.S. Patent 6,784,796 B2, August 31, 2004.

27. RG Johnston, *MagTag: Magnetic Vector Field Tag and Seal*. Los Alamos National Laboratory Report LAUR-02-6848 (2002).

28. RG Johnston, and ARE Garcia. *Tamper-Indicating Device Having a Glass Body*. U.S. Patent 6,553,930 B1, April 29, 2003.

29. ARE Garcia and RG Johnston, *Enhanced Tamper Indicator*. U.S. Patent 6,588,812 B1, July 8, 2003.

30. CA Sastre, *The Use of Seals as a Safeguards Tool*. Brookhaven National Laboratory Report BNL 13480 (1969).

31. Texas Advanced Optoelectronic Solutions (TAOS), http://www.taosinc.com/product_detail.asp?cateid=11&proid=12

32. RG Johnston and JS Warner, "How to Choose and Use Seals", *Army Sustainment **44**(4), 54-58 (2012),* http://www.almc.army.mil/alog/issues/JulAug12/browse.html

33. A Terzan, M Chatagnat, and D DubetLe, "Nouveau Comparateur a Eclipses De L'Observatoire de Lyon", *J. Optics (Paris)* **9**(2), 21-126 (1978).

34. ER Craine, "Video Comparator System for Early Detection of Cutaneous Malignant Melanoma", *Proceedings of the SPIE* **1653**, 399-409 (1992).

35. Croswell, K. "The Pursuit of Pluto", *American Heritage of Invention and Technology* **5**(3), 50-57, 1990.

36. Newport Corporation. *Kinematic Mounts*. http://www.newport.com/servicesupport/Tutorials/default.aspx?id=84

37. *Simple 3D: 3D Scanners, Digitizers, and Software for Making 3D Models and 3D Measurements*. http://www.simple3d.com

38. *Thermodynamics*. http://www.scitoys.com/scitoys/scitoys/thermo/thermo.html

39. "New Bottle Cap Thwarts Wine Counterfeiters", WebWire, August 4, 2008, http://www.webwire.com/ViewPressRel.asp?aId=71479

40. RG Johnston, ARE Garcia, and AN Pacheco, "The 'Town Crier' Approach to Monitoring", *International Journal of Radioactive Material Transport* **13(2),** 117-126 (2002).

41. RG Johnston, ARE Garcia, and AN Pacheco, "Improved Security Via 'Town Crier' Monitoring", *Proceedings of Waste Management '03,* Tucson, AZ, February 24-27, 2003, www.osti.gov/servlets/purl/827636-nWiBFO/native/

42. Murata, "Piezoelectric Sound Components", page 25, http://www.murata.com/products/catalog/pdf/p37e.pdf

43. G Elert, "The Nature of Sound", *The Physics Hypertextbook,* http://physics.info/sound

44. H Asgha, S Li, J Pieprzyk, & H Wang, (2011). "Cryptanalysis of the Convex Hull Click Human Identification Protocol", *Information Security*, pp 24-30.

45. X Bai, W Gu, S Chellappan, X Wang, D Xuan, & B Ma (2008), "PAS: Predicate-Based Authentication Services Against Powerful Passive Adversaries", *Computer Security Applications Conference*, *ACSAC 2008*, pp 433-442.

46. R Biddle, S Chiasson, & P Van Oorschot, (2011), "Graphical Passwords: Learning from the First Twelve Years", *ACM Computing Surveys*, **44**(4).

47. P Golle, & D Wagner, (2007), Cryptanalysis of a Cognitive Authentication Scheme", *IEEE Conference on Security and Privacy*, *SP'07*, pp 66-70.

48. JA Haskett (1984), "Pass-Algorithms: A User Validation Scheme Based on Knowledge of Secret Algorithms", *Communications of the ACM* **27**(8), 777-781.

49. "HIPs." *HIPs*. N.p., n.d. Web. 26 July 2012. http://www.aladdin.cs.cmu.edu/hips/

50. D Hong, S Man, B Hawes, & M Mathews (2004), "A Graphical Password Scheme Strongly Resistant to Spyware", *Proceedings the of International Conference on Security and Management*, Las Vegas, NV.

51. N Hopper, & M Blum, (2001), "Secure Human Identification Protocols", *Advances in Cryptology—ASIACRYPT 2001*, pp 52-66.

52. H Jameel, H Lee, & S Lee, (2007), "Using Image Attributes for Human Identification Protocols", *Arxiv Preprint* arXiv:0704.2295,

53. H Jameel, R Shaikh, L Hung, Y Wei, S Raazi, N Canh, et al. (2009), "Image-Feature Based Human Identification Protocols on Limited Display Devices", *Information Security Applications*, pp 211-224.

54. S Li, H Asghar, J Pieprzyk, AR Sadeghi, et al. (2009), "On the Security of PAS (Predicate-Based Authentication Service)", *Computer Security Applications Conference*, 2009. ACSAC'09, pp 209-218.

55. S Wiedenbeck, J Waters, L Sobrado, & JC Birget (2006), "Design and Evaluation of a Shoulder-Surfing Resistant Graphical Password Scheme", *Proceedings of the Working Conference on Advanced Visual Interfaces*, pp 177-184.

56. RG Johnston, "An Anti-Counterfeiting Strategy Using Numeric Tokens", *International Journal of Pharmaceutical Medicine* **19**, 163-171 (2005).

57. RG Johnston, ARE Garcia, RK Martinez, and ET Baca (1999), "Sealed-Container Sampling Tools*", Practice Periodical of Hazardous, Toxic, and Radioactive Waste Mgmt.* **3**, 18-22 (1999).

58. RG Johnston, J Vetrone, and JS Warner, “Sticky Bomb Detection with Other Implications for Vehicle Security”, *Journal of Physical Security* **4**(1), 36-46 (2010).