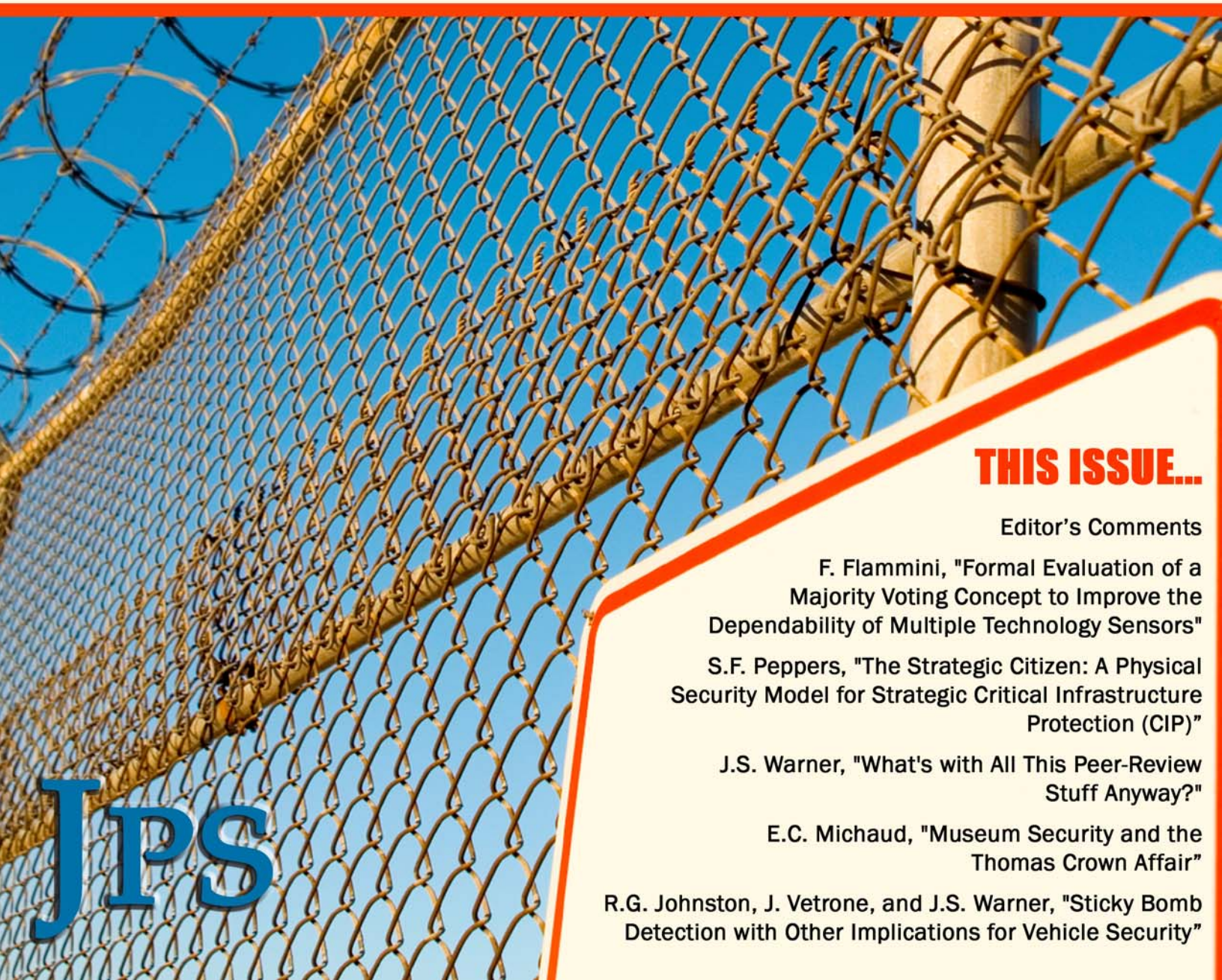
Argonne NATIONAL LABORATORY

The Journal of Physical Security

Volume 4(1), 2010



JPS

THIS ISSUE...

Table of Contents
Journal of Physical Security, Volume 4, Issue 1

Editor's Comments

Welcome to the latest issue, 4(1) of the Journal of Physical Security. This is a very eclectic issue. It includes papers about museum security, using private citizens to neutralize shooters and armed assailants, and how to combine data from various security sensors to decide on an intrusion threshold. There is also a paper about techniques for detecting sticky bombs on motor vehicles, and a discussion of the peer-review process and physical security.

The latter paper, by Associate Editor Jon Warner, is meant *inter alia* to address questions that our contributors and potential contributors have frequently asked about the peer review process used by this journal and many others. While a peer review process is common in science and engineering (and often familiar to researchers in cryptography, criminology, or cyber security), people who work in physical security may not have previously encountered the concept.

Jon's paper also contains a brief analysis of the type and number of journals and papers about physical security. One of the reasons we started the Journal of Physical Security (JPS) was because of a perceived lack of journals devoted to physical security, especially peer-reviewed journals. Jon's analysis suggests their continues to be a need for this type of journal.

As usual, the views expressed by the authors and the editor in the Journal of Physical Security are their own, and should not necessarily be ascribed to Argonne National Laboratory, UChicago LLC, or the United States Department of Energy.

Some authors and readers have asked why there is no consistent formatting style between various papers in a given issue of JPS. We decided early on not to have strict formatting requirements for authors in terms of fonts, page layout, headings and reference styles, etc. There are 3 reasons for this: (1) Many contributors and potential contributors to JPS find it challenging enough to write and submit a paper without a lot of extra work required to format it to some strict style they may not be comfortable or familiar with. (2) Letting each author format as she sees fit reduces the amount of editing work we must do. If the journal continues to grow, we might be able to have a professional editorial staff assist with this, but for now, editorial work is done primarily outside business hours and on our own time. And (3) the field of physical security (arguably) suffers enough from conformity that a little variation in individual style is probably healthy.

Editorial:

After September 11th, the United States indicated it would undertake an effort to reach out to the world to communicate our values and discourage the development of violent fundamentalism. Where is this effort?

Some of the things that Americans have always been very good at are advertizing, entertainment, pop culture, video, music, the Internet, and mass marketing. Why aren't the Internet and the airwaves (domestically and internationally) filled with slick, tightly edited, engaging songs, jingles, movies, and "commercials" discouraging terrorism and violent fundamentalism—painting these immoral acts in the most unfavorable light for the benefit of young people worldwide? A recent article by Bob Drogin and Tina Susman in the Chicago Tribune (March 14, 2010, page 23) indicates that radical fundamentalists and terrorists are effectively using the Internet and social web sites, often in conjunction with fast moving videos and loud music, to recruit young people to their cause. Why aren't Americans—highly skilled at these kinds of things—countering in kind?

Where are the heart-wrenching, personalized stories about the victims of terrorism, including children, people of Islamic faith, and family members of suicide bombers left behind after an act of political murder? Where are the interviews with psychologists and those who have been recruited as terrorists about techniques used by cults and terrorists for "brain washing"? Where are the pronouncements for young people from respected religious leaders that their religion does not condone killing innocents? Where is the geopolitical analysis indicating that terrorism has been largely ineffective; indeed, the United States is now more firmly entrenched in the Middle East, Iraq, Afghanistan, and Pakistan than before 9/11. Other than making air travel an adventure in bureaucratic foolishness, what has terrorism actually accomplished?

The United States (and Hollywood) has a huge effect on popular culture and on how even people in third world countries view the world. Why is this not being put to good use in fighting terrorism, in making violent radicalism, suicide bombing, and cult programming decidedly "uncool"?

As vulnerability assessors, we often see examples of where the concept of "layered security" (also known as "security in depth") is used as a kind of magical mantra that neutralizes all security concerns, and mitigates the need to improve security. If only layered security where indeed a silver bullet!

I authored a paper in the January issue of *Security Management* [RG Johnston, "Lessons for Layering", Security Management 54(1), 64-69 (2010)] that discusses some of the potential problems with layered security. In continuing this theme, here is my "self assessment tool" to help you decide if a given layer (or additional layers) of security makes sense.

Like my previous "self-assessment tools" (see for example, "How Flawed is Your Security Program", CSO Online, http://www2.csoonline.com/quizzes/security_assessment/index.php, or the Vulnerability Disclosure Index, pp. 17-35 of JPS Volume 3), this self-test shouldn't be taken overly seriously, but I believe it does raise important points that are worth contemplating.

Self-Assessment Survey:
Does Layered Security Make Sense for Your Security Application?

The following self-assessment can be used to determine if a new security layer makes sense (or if an existing layer should be maintained alongside other security layers). This self-assessment shouldn't be taken overly seriously—it's not all that rigorous and the scoring is somewhat arbitrary—but it can nevertheless be useful for encouraging careful thinking about the layer in question.

Directions: Examine each of the 21 questions below about the security layer (or measure) of interest. For each question, decide if the answer is yes, no, or maybe/unknown. Circle your answer for each question. Scoring: Add up the number of circled answers in column B which we call NB. Add up the number of circled items in column D which we call ND. Your total score is (2*NB) + ND. (Column B contains the "ideal" answers if the security layer in question makes sense to implement or keep.)

Interpreting the score: The maximum possible score is 42. If the score is greater than 36, the security layer in question is probably a good idea. If the score is less than 29, the security layer is probably not a good idea and will likely decrease overall security. If the score is between 29 and 36 (inclusive), the security layer needs more analysis or modifications in terms of its effectiveness and interactions *vis a viz* the other security layers; thinking carefully about the questions in the table might help clarify the issues. Thus:

Score 37 to 42, the security layer in question is probably a good idea.

Score 29 to 36, the security layer needs more study, analysis, or refinement.

Score 0 to 28, the security layer is probably not a good idea and will likely decrease overall security.

Question	A	B	C	D
1. Is introduction of the new layer being used (consciously or unconsciously) to avoid having to think carefully about existing security vulnerabilities or how to optimize the existing layers?	yes	no		maybe/unknown
2. Is the new layer being installed out of fear or desperation or urgency or cognitive dissonance (mental tension between our hopes and our fears)?	yes	no		maybe/unknown
3. Is the new layer being installed primarily because funds become available for it, or because non-security mangers or executives ordered it?	yes	no		maybe/unknown
4. Is the motivation for the new security layer essentially a "vitamin mentality"—"if some security is good, then more must be better"?	yes	no		maybe/unknown
5. Do you think the new layer is undefeatable?	yes	no		maybe/unknown
6. Have you taken steps to insure that alarms generated from the other security layers won't be ignored or discounted because of the existence of the new layer?		yes	no	maybe/unknown
7. Will the new layer distract security personnel or cause less attention to be paid to the other layers of security?	yes	no		maybe/unknown
8. Does the new layer have buy-in from the security personnel or others who must use it?		yes	no	maybe/unknown
9. Will the new layer dramatically increase the complexity of providing security, or the time and/or costs involved?	yes	no		maybe/unknown
10. Will installation of the new layer and the learning curve associated with it introduce an extended period of weakened security?	yes	no		maybe/unknown
11. Is the new layer specifically designed to deal with known vulnerabilities or attack modes for the other layers of security?		yes	no	maybe/unknown
12. Are there specific, rigorous reasons to believe the new layer will improve your security (as opposed to just relying on hope, speculation, sales hype, hearsay, or assumptions)?		yes	no	maybe/unknown
13. Can you summarize in 2-3 sentences (without relying on sales hype) exactly how the new layer will improve your security?		yes	no	maybe/unknown
14. Are the vulnerabilities and attack modes for the other layers of security well understood by you, and have you tried to defeat them?		yes	no	maybe/unknown
15. Are the vulnerabilities (including any software vulnerabilities) and attack modes for the new security layer well understood by you?		yes	no	maybe/unknown
16. Do you have a good understanding of how the new security layer works?		yes	no	maybe/unknown
17. Is the new layer of security relatively untested, and is it high-tech and generating a lot of buzz/hype/excitement?	yes	no		maybe/unknown
18. Are you clear on whether the new layer is meant to be serial, parallel, redundant (backup), or some combination?		yes	no	maybe/unknown
19. Are the skills and methods an adversary would use to attack the new layer similar to the other layer(s)?	yes	no		maybe/unknown
20. Are there serious common modes of failure, e.g., can one event neutralize multiple layers of security? (For example, if the electrical power is shut off by an adversary, will the new layer and other layer(s) stop working?)	yes	no		maybe/unknown
21. Does the new layer compete or interfere with existing security layers in terms of physical space (e.g., there isn't enough room in the hasp for both a lock and a seal), maintenance, upgrades, funding, attention by frontline personnel, power requirements, or electrical/radio frequency interference?	yes	no		maybe/unknown

Instructions: 1. Total up the number of items circled in column B = NB. 2. Total up the number of items circled in column D = ND. 3. Score = (2 * NB) + ND.		NB =		ND =
Final Score = 2NB + ND =				

We are often asked in the Vulnerability Assessment Team at Argonne National Laboratory how we do vulnerability assessments (VAs) and what constitutes "best practice" for doing VAs. Here are the tips and philosophy that we offer:

Tips for Doing Effective Vulnerability Assessments

1. Do them early, iteratively, and often (ideally continuously). Frequently, we are handed a security device or system to evaluate only when it is ready to be fielded or manufactured—and when it is too late economically, politically, and emotionally to make any changes.

2. Use independent, ideally external vulnerability assessors who want to find problems and solutions, and who have no conflicts of interest (not just financial) or wishful thinking.

3. No "shoot the messenger".

4. Don't allow promoters, developers, manufacturers, or vendors of the security device/system to do the VA (though they should provide input).

5. Use the personnel with the right mindset and/or skill set: hackers, hobbyists, creative types, troublemakers, questioners of authority, loophole finders, skeptics/cynics, physicists, chemists, computer geeks, artisans, graphic artists, nerds, hands-on technicians, antique & auto body repair experts, …

6. Engineers are not typically very good at VAs or designing for effective security. The mindset is all wrong.

7. Follow good brainstorming and creativity practices based on modern research into how innovative ideas (attacks and countermeasures in this case) are generated.

8. Do the VA in context: understand the adversaries, the facilities, the personnel, their training, and the overall security goals.

9. Don't underestimate the adversary.

10. Don't let the good guys define the problem. The bad guys can attack how, where, and when they want. They don't have to attack at the point of your greatest strength, or attack security devices and systems just because you have installed them.

11. Don't view the VA as a test to pass, a certification procedure, a scapegoating mechanism, or a rubber stamp. VAs are for the purpose of improving security only.

12. Don't accept a VA that finds no vulnerabilities. It is wrong. Vulnerabilities are always present in large numbers.

13. Don't think you can find all the vulnerabilities, or that you won't find more next time, or if different people do the VA.

14. Pay special attention to what the promoters, developers, manufacturers, and vendors are most proud and/or confident about, and to the high-tech features. Those are usually the easiest to attack.

15. Concentrate on low-tech attacks, even on high-tech devices, systems, and programs (because high-tech attacks will not be needed).

16. Do VAs holistically, not by module, sub-component, or function. Vulnerabilities are often found at the interfaces.

17. There should be no unrealistic constraints on time and resources available for the VA. And no blocking the review of certain features or sub-assemblies.

18. The VA should point out possible countermeasures, not just vulnerabilities.

19. But the vulnerability assessors probably don't have the best understanding of the most practical countermeasures to implement.

20. The VA should lead to more many more vulnerabilities and countermeasures than can be implemented at one time.

21. Don't forget that true counterfeiting is rarely necessary for an adversary, just token counterfeiting, i.e., the device needs only be superficially mimicked. This is much easier than true counterfeiting (which itself is rarely as difficult as people think).

22. View security from the standpoint of the adversary: Really get inside their heads. Use Method Acting techniques.

23. The best attacks and countermeasures come late!

24. A good VA report should point out the good things first (so they will continue, and so there is a willingness to hear about the weaknesses).

25. Vulnerabilities are good news, not bad news! Finding a vulnerability means you can do something about it.

26. Distrust anybody who does “rigorous”, formalistic, or “reproducible” VAs, who claims to be able to find all the vulnerabilities, or who is enamored with standards or certifications for VAs. Nobody currently has enough understanding of security or VAs to warrant these things.

27. In the end, a vulnerability assessment is not so much about technology and security strategy as it is an exercise in psychology and predicting human behavior: how the bad guys will attack.

28. That being said, you usually will have better security if you concentrate on vulnerabilities (security weaknesses) than on threats (who might attack with what probability). If you get the vulnerabilities right, you will be ok even if you get the threats wrong. But if you only analyze the threats without an appreciation for the vulnerabilities, you are probably in trouble.

Philosophy on Vulnerability Assessments
(Especially for Buildings, Facilities, Infrastructure and Security Programs)

1. There are a number of conventional tools for finding security vulnerabilities, especially in critical infrastructures or security programs. These include security surveys, risk management, design basis threat, CARVER Method, Delphi Method, software vulnerability assessment tools, security audits, infrastructure modeling, etc.

2. These tools have some value, and indeed we have used them all.

3. Experience has shown, however, that these methods do not usually result in dramatic improvements to security, nor do they reliably predict catastrophic security incidents that are novel and rare. Even worse, they often completely miss obvious vulnerabilities. In the case of computer modeling of vulnerabilities, the models themselves are rarely validated in any meaningful way.

4. There are a number of reasons why these tools fall short, including that they are too often:

- unimaginative
- full of sham rigor
- not context oriented
- inflexible & close-ended
- not sufficiently predictive
- ignorant of the insider threat
- used to justify the status quo
- not focused on the right issues
- harmed by the fallacy of precision
- blind to critical ground-level details
- limited to protecting physical assets
- dominated by groupthink & bureaucrats
- plagued by “shoot the messenger” syndrome
- hampered by arbitrary, made-up probabilities
- not validated by hands-on or real-world testing

- ineffective at estimating true consequence costs
- not done from the perspective of the adversaries
- unable to recommend effective countermeasures
- confused in thinking that a VA is a test to be passed
- obsessed with past security incidents, not future ones
- binary in outlook (something is either secure or it is not)
- overly focused on barriers, technology, & physical layout
- distracted by tables, matrices, spreadsheets, & software programs
- focused on threats to the detriment of understanding vulnerabilities
- insistent on letting the good guys define the problem, not the bad guys
- insistent on letting the existing security infrastructure and strategies define the problem, not the bad guys
- conducted by personnel who don't want to find problems—so they don't

5. The overall goal of an effective vulnerability assessment should be to predict what the adversaries might do. This is fundamentally a psychology problem, not a hardware, technology, assets, infrastructure, building design, management, or digital computer modeling problem. But you can't reliably predict what someone might do if you can't "get inside his head". Conventional, formalistic vulnerability assessment tools largely ignore the adversary's psychology, perspectives, and motivation. Moreover, formalistic tools are not (for the most part) tools that an adversary even uses, and thus are not effective at mimicking or predicting his behavior in an expedient and realistic manner.

6. An **Adversarial Vulnerability Assessment** goes beyond formalistic, unimaginative, semi-quantitative, linear methods to view the security problem from the perspective of the adversary. The emphasis is on using creative assessors who are psychologically pre-disposed to effectively spoofing hardware and organizations, who have hands-on ("hacker") experience defeating security, and who attempt (both by their intrinsic nature and with the aid of psychologists and others) to think, see, and feel what the adversaries think, see, and feel. Modern techniques for effective brainstorming and creativity are employed, based on many decades of research into how new ideas can be best generated. It is also essential to accurately understand the security organization's goals, attributes, personnel, culture, and climate.

7. The Argonne Vulnerability Assessment Team conducts **Adversarial Vulnerability Assessments** using a multi-disciplinary team approach. Hackers, technicians, physicists, engineers, computer scientists, artists, sociologists, and psychologists are employed to understand the fundamental issues behind any given security application, and to discover and demonstrate security vulnerabilities, as well as practical countermeasures. This approach has repeatedly resulted in the discovery of surprising, easy-to-exploit vulnerabilities totally overlooked by security managers, designers, manufacturers, and vendors, as well as other vulnerability assessors using more conventional techniques.

8. The lessons of our work is that there are almost always fairly simple and inexpensive countermeasures for eliminating, or at least partially mitigating, even the most serious vulnerabilities. The vulnerabilities have to be known and acknowledged, however, before such countermeasures can be implemented.

9. Some organizations do on-the-ground “realistic” exercises, and/or talk about the importance of creative vulnerability assessments, but the actual results often fall far short of a true adversarial vulnerability assessment.

-- Roger Johnston, Argonne National Laboratory, February 2010.

Journal of Physical Security 4(1), 1-9 (2010)

Formal Evaluation of a Majority Voting Concept to Improve the Dependability of Multiple Technology Sensors

Francesco Flammini

ANSALDO STS Italy
Via Argine 425, Naples, Italy
francesco.flammini@ieee.org

Abstract. Finding a good trade-off among the probability of detection (POD), the false alarm rate (FAR) and the reliability of detectors is a very important task in physical security system design. Existing solutions try to achieve this aim either by using the most advanced technologies or by combining basic sensors in logical OR/AND relations. However, these approaches are either not cost-effective or they do not allow for the necessary flexibility to obtain the right balance. In this paper I propose a majority voting scheme for multiple technology detectors which I evaluate using stochastic modelling techniques. This solution has the major advantages that it permits good overall dependability while using low-cost detectors, and also enables a precise fine tuning of POD and FAR parameters. To the best of my knowledge, no similar system has been studied in depth in the research literature. I provide a set of results which clearly show the advantages of the proposed approach.

Keywords: physical security, intrusion detection, stochastic modelling, quantitative evaluation, diversity redundancy

1. Introduction

The importance of dependability in physical security systems is increasing as threats escalate, especially in applications related to critical infrastructure protection. One of the most important topics in this research field is the automatic decision fusion to support the task of security operators. In case of diverse redundancy of sensors, a correlation of basic events generated by independent sensors could be used to improve the dependability of alarm generation (see e.g. reference [3]). The aim of this paper is to provide a formal demonstration of this concept in the specific case of a basic majority vote. In particular, I will refer to a straightforward example of volumetric intrusion detectors (also known as “radars”); however, the results are general enough to be used with any sensor combination provided that diverse technologies (and/or detection criteria) are used. Throughout the paper, I will adopt the reference dependability taxonomy (including the concepts of reliability, availability, trustworthiness, survivability, etc.) provided in reference [2].

The usefulness of an intrusion detection system critically depends on its capability to distinguish an alarm condition initiated by an actual unauthorized intruder from either a false alarm, or from an alarm failure caused by noise, atmospheric disturbance, animals, alterations in the placement and state of operability of protected area equipment, and change in actual versus the design range, among other things. For instance, ultrasonic intrusion detection systems are not only subject to false alarms caused by drafts and air movements, but can also be bothered by ultrasonic noises generated by, for example, bells and hissing. Moreover, they are also subject to alarm failures due to changes from nominal range occasioned by variations in the ultrasonic propagation medium.[7] Similarly, microwave intrusion detection systems produce false alarms in response to water movement in plastic pipes, energy received from beyond the protected area due to wall and window penetration, and unwanted reflections, among other things. However, the sources that adversely affect the performance of ultrasonic detection systems are in general different from those that

give rise to false alarms and failures of alarm for microwave detection systems, and conversely. Thus, while drafts, air movements, and ultrasonic noises adversely affect ultrasonic system performance, none of them poses a significant detection problem for microwave systems. And while water movement in plastic pipes, wall or window penetration, and reflections give rise to false alarms for microwave intrusion detection systems, such events are not obstacles to accurate detection for ultrasonic systems. Hence a variety of technologies have been used simultaneously to more reliably detect the presence of an intruder in region under surveillance. Microwave, ultrasonic, photoelectric and passive infrared [10] are some of the more common technologies in current use [8]. Each has certain unique advantages and disadvantages which makes it more or less desirable for a particular environment or application. None is fool-proof, and all are subject to the ever-annoying false alarm. Multiple technology intruder detection systems in AND-type correlation have proven to be substantially more reliable and less susceptible to false alarming than single technology systems, with "common cause" false alarms happening in very rare circumstances (if installed using the right criteria). However, besides the higher cost, it is rarely noticed that AND-type correlations have a negative impact on availability, detection probability and the possibility of spoofing. (It is enough to spoof one of the sensors.) In contrast, OR-type correlations have some advantages (e.g., POD) but also considerable disadvantages, including an unacceptably high rate of false alarms.

The solution proposed in this paper aims at finding a good compromise between those contrasting requirements by adopting a '2 out of 3' ('2oo3') majority voting concept. See Figure 1. It will be shown through the analytical evaluation of a formal stochastic model that this approach features several advantages with respect to alternate techniques, including the AND-type correlations widespread in multiple technology sensors. Results will be provided as quantitative parameters, i.e. non-functional dependability attributes. Among other things, significant advantages will be demonstrated for the POD, in the resistance to spoofing, and in the higher survivability, with only a modest disadvantage in cost and FAR compared to AND-type correlations. The results are general enough to be valid in any multiple technology sensor correlation, where the so called "diverse redundancy" is adopted (possibly also at the software levels). It should be noticed that the concept of 'majority voting' is also employed in safety-related fields for different purposes, including an increase in safety and availability.[5]

This paper is organized as follows: Section 2 provides some introductory definitions and theoretical results about AND-type, OR-type, and majority-voting event correlation. Section 3 introduces the reference model used for the analysis, the choice of parameters, and the evaluation results, which are discussed in detail. Section 4 summarizes the impact of the results and draws conclusions.

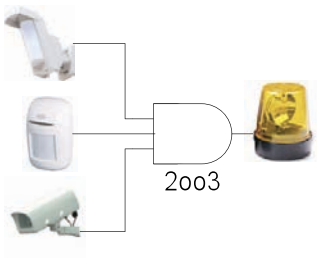


Figure 1. A schematic of the majority voting scheme for alarm correlation.

2. Basic definitions and description of the approach

The majority voting approach presented in this paper is based on the assumption that diverse technologies feature false alarms of differing natures, which is generally true

(as also stated in the previous section). More formally, the following two equations must hold for conditional probabilities[1]:

$$P(\text{false alarm from 1} \mid \text{false alarm from 2}) \approx P(\text{false alarm from 1})$$

$$P(\text{false alarm from 2} \mid \text{false alarm from 1}) \approx P(\text{false alarm from 2})$$

This allows obtaining some interesting theoretical results (see also [8]). If I define:

- P^1_F as the probability of false alarm of sensor 1
- P^2_F as the probability of false alarm of sensor 2

In case of diversity, I can assume that such probabilities for the two detection devices are (almost totally) independent from each other, therefore obtaining for the "AND" correlation the following result:

$$P^{1 \text{ AND } 2}{}_F \approx P^1_F \cdot P^2_F$$

In the realistic assumption that[2]:

- $P^1_F << 1$
- $P^2_F << 1$

Then I can state that:

$$P^{1 \text{ AND } 2}{}_F << P^1_F$$

$$P^{1 \text{ AND } 2}{}_F << P^2_F$$

In other words, the resulting FAR for the 'AND' correlation is substantially less than the FAR of the single sensors.

Similarly, it is possible to demonstrate that the probability of detection is negatively affected. In fact, if I define:

- P^1_D as the probability of detection of sensor 1
- P^2_D as the probability of detection of sensor 2

Then I can state (basing on the diversity assumption):

$$P^{1 \text{ AND } 2}{}_D \approx P^1_D \cdot P^2_D$$

Hence the result is that:

$$P^{1 \text{ AND } 2}{}_D < P^1_D$$

$$P^{1 \text{ AND } 2}{}_D < P^2_D$$

However, since it is realistic to assume[3]:

- $P^1_D <\approx 1$
- $P^2_D <\approx 1$

then the loss in POD is not as important as the gain in FAR reduction, so the trade-off is generally advantageous (as demonstrated by the results provided in the following section). The opposite holds true for the 'OR' correlation, which can be only advantageous when the priority is on event detection, and false alarms can be tolerated. This means that, generally speaking, AND-type and OR-type correlations feature contrasting specifications which do not allow for a fine tuning of the POD/FAR ratio or other dependability attributes (as it will be shown in the following).

[1] The '|' symbols stands for "given that", while the '≈' symbol means "almost equal".
[2] The '<<' symbols stands for "much minor than".
[3] The symbol '<≈' means "minor than but almost equal to" or rather "not much minor than".

Now, let me formally define the majority voting scheme proposed in this paper. A Boolean variable X_{2oo2} is said to be related to other 3 Boolean variables X_1, X_2 and X_3 through a '2 out of 3' correlation logic when the following formula holds[4]:

$$X_{2oo2} = (X_1 \wedge X_2) \vee (X_1 \wedge X_3) \vee (X_2 \wedge X_3)$$

This function can be specified using the so-called "truth table" shown in Table 1.

LOGIC VALUE 1	LOGIC VALUE 2	LOGIC VALUE 3	2OO3 LOGIC
FALSE	FALSE	FALSE	FALSE
FALSE	FALSE	TRUE	FALSE
FALSE	TRUE	FALSE	FALSE
FALSE	TRUE	TRUE	TRUE
TRUE	FALSE	FALSE	FALSE
TRUE	FALSE	TRUE	TRUE
TRUE	TRUE	FALSE	TRUE
TRUE	TRUE	TRUE	TRUE

Table 1. Description of the '2oo3' logic function.

In the case of sensors based on different detection technologies, the '2oo3' logic allows us to:

- Generate an alarm only when at least two of the three sensors agree on event detection, thus intuitively improving the detection reliability and decrease the false alarm rate of a single sensor.
- Increase the availability, mean useful life, and/or the survivability of the detector since it can continue working in a dual or even single technology configuration (with reduced performance) when, respectively, one or two sensors stop working. This allows for a fail-safe or fall-back mechanism until the failed sensor is replaced (assuming the electrical connections are designed not to feature a "stuck-at-alarm" on failed sensors).
- Reduce the likely success of tampering, blinding, or shielding attempts which could spoof single or (even more easily) dual technology sensors used in AND configurations (by far the most widespread).

Therefore, the '2oo3' logic can potentially improve the overall system dependability in terms of several relevant parameters, allowing us to achieve a set of non-functional (i.e. quantitative) specifications which would be impossible or very expensive to obtain using a single technology. This statement will be formally demonstrated in the following section using a model-based evaluation approach.

The implementation of the '2oo3' logic circuit is straightforward and introduces very little extra cost. An abstract scheme (and a comparison with more traditional designs) using an electrical representation is depicted in

Figure 2, where the symbols labelled with A, B and C represent 'switches' or 'circuit breakers' [1]. The actual design depends on other factors, including the type of contacts (e.g. voltage free or not, normally open/closed, etc.) and the latency of the alarm signals. More complex designs could also include the possibility of detecting and excluding a faulty sensor when the "disagreement rate" is above a certain threshold (i.e., it is generating too many false alarms).

Finally, please note that even though the independence assumption regarding false alarms is very important to ensure stochastic independence in event detection, in he next section, I will also evaluate the impact of slight dependencies on the occurrence of false alarms.

[4] ' $\wedge$ ' is the logic symbol of the 'AND' operator, while ' $\vee$ ' represents the 'OR' operator.

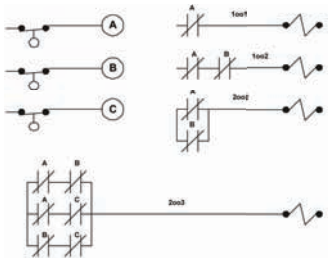


Figure 2. Electrical representation of voting schemes.

3. Modelling, evaluation and discussion of the results

In this section, I report the results of the quantitative evaluation of the proposed approach using a formal (or "analytical") stochastic modelling method based on Bayesian Networks (BN).[4] Bayesian Networks are a well known method for probabilistically modelling uncertainty in many scientific or engineering problems. With respect to other possible approaches, including the ones based on extensions of the Fault Tree formalism, BN allows us to express any kind of dependence among stochastic variables, to obtain more compact models, and to avoid the use of state-based modelling techniques when they are not strictly necessary (as in this case).

As for the sensor related data, I have checked some prior work on detection reliability evaluation, but none of them looked general enough to be considered as a reference source, since the results are highly dependant on the specific technologies, manufacturers, and applications (see e.g. reference [8]). Therefore, I have merged data coming form different papers and component data-sheets, and also from my testing experience only to get some "order of magnitude" estimates for POD, FAR and availability indices, which have been used as parameters to populate the BN models used for the analyses (as reported in Table 2); in other words, I have not used real data but I have used realistic pseudo-data. The conclusions which I will draw are valid regardless of the specific values of the parameters.

As for the support modelling and evaluation tool, I have used Netica by Norsys [9]. The Conditional Probability Table (CPT) for the '2oo3' connection has been directly derived from Table 1. I have chosen three example single technologies which vary in their overall dependability and cost, from an 'entry-level' (technology 3) to a 'top-level' (technology 1), passing through an "average-level" (technology 2). The AND-type (i.e. '2oo2') correlations have been evaluated both for 1-2 (best) and 2-3 (worst) combinations. The OR-type correlations (e.g. '1oo2' or '1oo3') have not been taken into account in the analysis because I have shown that their advantages are rather limited.

Figure 3 reports the results of the analysis regarding the FAR parameter in the complete independence assumption, while Figure 4 shows the effect of a slight correlation on the same parameter. The results clearly show that a little correlation (less than 20%) has negligible effects on the results. The results show that the lowest FAR is obtainable using a '2oo2' design (AND-type correlation); however a significant improvement (by a factor ranging from 2 to 16) over single technologies can be achieved by the '2oo3' design.

Figure 5 reports the results of POD evaluation. Here the best result (99.7%) is achieved by the '2oo3' design (with a significant advantage of over 2 points compared to the best '2oo2'), which slightly improves the POD of the best single technology, even using additional technologies which are not as good as the best one.

Figure 6 presents the results of the steady-state availability evaluation, which gives a measure of how much the system is "survivable", that is, able to remain operational (even in a degraded state, i.e. with reduced performance) without requiring a

maintenance intervention. In this case, the winner is '2oo3' with an availability of about '4 nines'[5], which is better than any single technology. Please note that any '2oo2' design significantly worsens this parameter, halving the availability value with respect to single sensors.

Figure 7 shows the results of "spoof rate" evaluation, the assumption here being that an intruder is able to spoof with a certain probability one or more technologies. The conservative assumption is that the best technology is also the hardest to spoof—which could be untrue. Nevertheless, the results show that, as intuition suggests, the '2oo2' design significantly worsens the resistance of detectors to spoofing by a factor ranging from approximately 1.5 to 3, which is difficult to achieve in practice. Instead, the '2oo3' approach reduces the success rate of spoofing attempts with respect to the best single technology (3.3% instead of 5%).

Finally, Table 2 summarizes the results obtained by the analyses, and compares them with original data for single technologies. The best results for each column (cost, availability, spoofing success rate, POD, and FAR) are highlighted in bold style, while the cells associated with the '2oo3' design are shaded in light grey. Regarding the cost, I have neglected the (small) overhead due to the correlation circuits.

It is clear that the '2oo3' design wins over the other technologies for all the parameters except cost and FAR, and is the only approach which always ensures better results with respect to the single technologies. In contrast, the '2oo2' approach provides inferior results with the exception of FAR, which can be significantly better with respect to any other design. In conclusion, considering the small cost increase of '2oo3' designs with respect to '2oo2' ones, the results clearly show that the '2oo3' approach allows advantageous trade-offs between dependability parameters required for detectors (or any other event-sensing devices). This makes the '2oo3' designs attractive for a wide range of physical security applications.

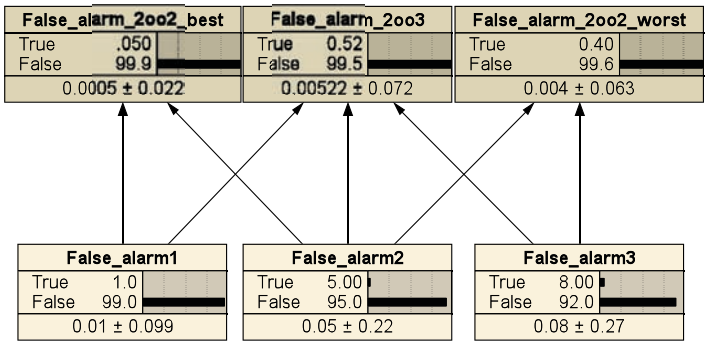


Figure 3. FAR evaluation of majority voting.

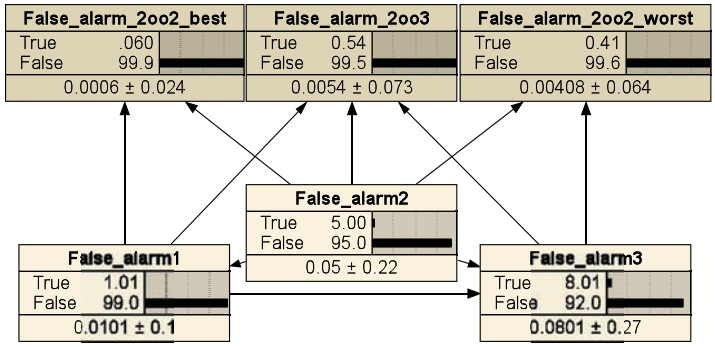


Figure 4. Effect of a slight correlation (10÷20%) on the false alarm rate.

[5] The expression '4 nines' means 0.9999 (or 99.99%).

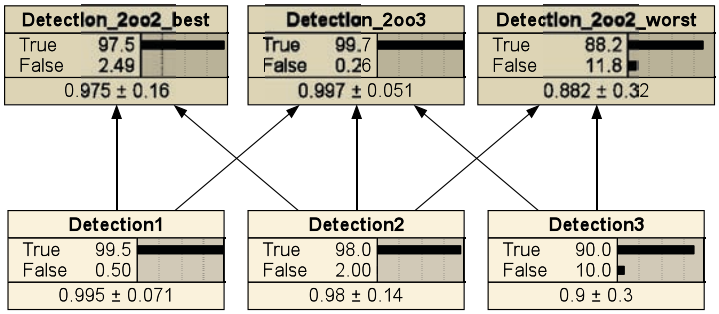


Figure 5. POD evaluation of majority voting.

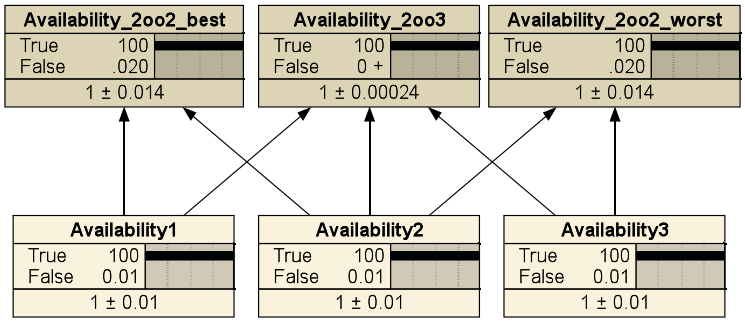


Figure 6. Availability evaluation.

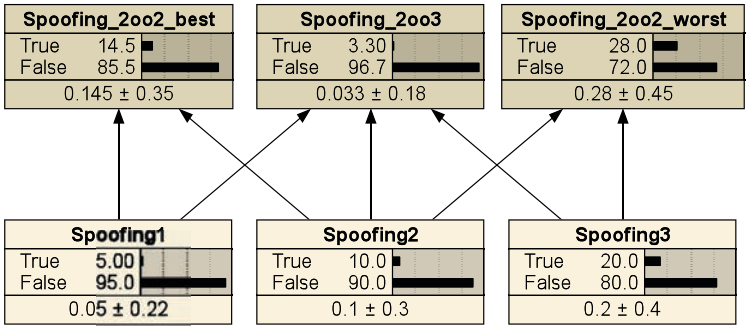


Figure 7. Spoofing success rate evaluation.

TECHNOLOGY	COST [€] BETTER ↓	AVAILABILITY [%] BETTER ↑	SPOOF [%] BETTER ↓	POD [%] BETTER ↑	FAR [%] BETTER ↓
SINGLE (BEST)	500	99.990	5	99.5	1
SINGLE (AVERAGE)	200	99.990	10	98	5
SINGLE (WORST)	**100**	99.990	20	90	8
DUAL (2OO2, BEST)	700	99.020	14.5	97.5	**0.05**
DUAL (2OO2, WORST)	300	99.020	28	88.2	0.4
TRIPLE (2OO3)	800	**99.999**	**3.30**	**99.7**	0.52

Table 2. Summary of results and comparison of technologies.

4. Conclusions

The most important goals in the design of physical security systems are to maximize the detection probability, and to minimize the occurrence of false alarms, in order to achieve optimal performance. In this paper, I have demonstrated using an analytical approach how a cost-effective solution can be achieved by exploiting diverse

redundancy in sensor technology and alarm correlation for majority voting. Majority voting allows us to improve the probability of detection of even the most advanced single sensor technology, as well as the overall detection availability, at the cost of slightly more false alarms only with respect to dual technology (i.e., AND-type correlation); furthermore, majority voting also improves robustness to spoofing attempts.

The correlation studied in this paper can be implemented using simple programmable logic devices, software programs controlling computer digital I/O cards, or any COTS (Commercial Off The Shelf) integrated circuits meeting the correlation logic needs (3-input OR gate and 3 two-input AND gate). An effective solution can be obtained by holding the input values of the sensors for a few seconds (e.g., using timed flip-flops) in order to allow for the necessary detection latencies from the diverse technologies. In some cases, triple technology sensors in a single enclosure can be already available as COTS. In these cases the output of the single sensors can be accessed singularly and correlated in a '2oo3' configuration, as explained in this paper, instead of using the less effective AND/OR logic.

Other possible majority voting schemes (e.g., '3oo4', '4oo5', etc.), sometimes used in mission/safety-critical systems, are likely to introduce a far higher complexity in system design, but they could fit the needs of specific applications and can be evaluated using the same approach presented in this paper.

I have motivated the approach basing on cost-effectiveness principles, since a linear reliability growth usually implies an exponential cost growth. However, some modern detection technologies (e.g., audio-video analytics) are not yet very reliable, regardless of the manufacturer experience and testing effort. One idea is to combine more diverse artificial intelligence algorithms (e.g., object tracking, neural networks, etc.) and a majority voting scheme for event detection in order to get better results.

Finally, majority voting is not necessarily Boolean: a (possibly weighted) average of measured values can be considered in the case of continuous numerical values. Such an application is currently under analysis for networks of smart wireless sensors.

References

1. Adamsky, B.: Design critical control or emergency shut down systems for safety and reliability. White Paper. http://www.ips.invensys.com/en/knowledge/Documents/white-papers/IPS_GL_UP_SS_WP_12-08_DesignCriticalControl.pdf (last access January 6th 2010)
2. Avizienis, A., Laprie, J.C., Randel B.: Fundamental Concepts of Dependability. LAAS Report n. 01-145, 2001
3. Bocchetti, G., Flammini, F., Pappalardo, A., Pragliola, C.: Dependable integrated surveillance systems for the physical security of metro railways. In: Proc. 3rd ACM/IEEE International Conference on Distributed Smart Cameras (ICDSC 2009), 30 August - 2 September, 2009, Como (Italy): pp. 1-7
4. Charniak, E.: Bayesian Networks without Tears. In: AI Magazine, 12(4), 1991: pp. 50-63
5. Flammini, F., Marrone, S., Mazzocca, N., Vittorini, V.: Evaluating the Hazardous Failure Rate of majority voting computer architectures by means of Bayesian Network models. In: Risk, Reliability and Societal Safety - Aven & Vinnem (eds), Proc. ESREL'07, Stavanger, Norway, June 25-27, 2007: pp. 1715-1721
6. Garcia, M.L., The Design and Evaluation of Physical Protection Systems, Butterworth-Heinemann, 2001
7. Li, Y. P., Yang, J., Li, X.D., Tian, J.: Ultrasonic Intruder Detection System for Home Security. In: LNCS Vol. 344/2006: pp. 1108-1115
8. Martin, P.T., Feng, Y., Wang, X.: Detector Technology Evaluation. http://www.mountain-plains.org/pubs/pdf/MPC03-154.pdf, 2003 (last access January 6th 2010)

9. Norsys Netica Web Site: http://www.norsys.com/netica.html (last access January 6th 2010)
10. Rogalski, A.: Infrared detectors: status and trends. In: Progress in Quantum Electronics, Vol. 27, Issues 2-3, 2003: pp. 59-210

Journal of Physical Security 4(1), 10-21 (2010)

The Strategic Citizen: A Physical Security Model for Strategic Critical Infrastructure Protection (CIP)

Shawn F. Peppers

ABSTRACT

The current physical security paradigm that engages an active shooter primarily depends upon law enforcement - which has response time limitations. From the time of the shooter's first shot until his incapacitation, 3 to 4 minutes have elapsed, with the shooter having shot a person every 15 seconds. The Strategic Citizen, derived from the Federal Flight Deck Officer (FFDO) Program, is a conceptual homeland security model for enhancing the physical security of Critical Infrastructure and Key Resources (CIKR) against armed assault.

INTRODUCTION

America's physical security posture for Critical Infrastructure Protection (CIP) suggests it is insufficiently prepared to prevent the consequences of deliberate armed aggression. The current physical security paradigm that engages an active shooter primarily depends upon law enforcement - which has response time limitations. Analysis "based on 5-year data obtained from 24 school shootings in 18 States and 41 workplace shootings in 12 States, from the time of the shooter's first shot until his incapacitation, 3 to 4 minutes have elapsed, with the shooter having shot a person every 15 seconds."[1]

A physical security paradigm against an active shooter that averages one casualty every 15 seconds ought to be reconsidered - especially when terrorists have implemented similar tactics. The Strategic Citizen, derived from the Federal Flight Deck Officer (FFDO) Program, is a conceptual homeland security model for enhancing the physical security of Critical Infrastructure and Key Resources (CIKR) and reducing victim personal injury and property loss against armed assault.

For any security countermeasure to be effective, the threat has to be clear. Instead of navigating the nuances between the similarities and/or variations of an active shooter with a terrorist, a different threat construct is necessary. Two common characteristics of active shooters tend to be spontaneity of violence and proximity to targets. For the purpose of this article, the Strategic Citizen addresses the threat of spontaneous close combat; where an active shooter can take advantage of spontaneity

Shawn F. Peppers works for the Utah Department of Public Safety where he coordinates Critical Infrastructure Protection (CIP) activities. Also, Mr. Peppers is an adjunct instructor at Utah Valley University. The views expressed in this article are those of the author and do not reflect the official policy or position of the Utah Department of Public Safety or Utah Valley University.

and proximity amid infrastructure, and where such violence could maximize and/or amplify the aggressor(s) intent to destroy innocent life and damage property.

The Strategic Citizen, within a homeland security framework, is the civilian whose occupation is associated working directly with or in close proximity to CIKR (including schools). By virtue of this proximity, such a person is able to provide localized and/or immediate physical protection to threatened life and property. The citizen in such a role is "strategic" when an armed attack on CIKR could intensify victim injury and property loss; which in turn could have a strategic impact on the functioning of the economy (national, state and local level).[2] To paraphrase Marine Corps General Charles Krulak's concept of the Strategic Corporal, when operating in an asymmetric threat environment "the Strategic Citizen will be the most conspicuous symbol of homeland security policy and will potentially influence not only the immediate tactical situation, but the operational and strategic levels as well."[3] The 9/11 Commission identified four failures; one of them is imagination.[4]

The current homeland security approach seems to oscillate between prevention, response, and resiliency measures. In the article *Marrying Prevention and Resiliency: Balancing Approaches to an Uncertain Terrorist Threat,*[5] Brian A. Jackson suggests a hybrid approach. Attempting to predict and/or prevent future terrorist threats through intelligence sharing and analysis will remain an elusive goal. Commercial air travel being an example, "given public sensitivities and the practical difficulties of collecting and analyzing large amounts of information on every traveler, it is likely that a residual of irreducible threat uncertainty will always remain."[6] These same concerns could also apply to the homeland security enterprise as a whole.

Due to potential uncertainty, this threat ambiguity may become a "basis for the argument for focusing on resiliency rather than traditional prevention—if we don't try to prevent disruptions but instead invest in measures that help us "take the hit" wherever it comes from, then such uncertainties are much less important."[7] Jackson proposes that "rather than approach this as an either/or choice between prevention and resiliency, these two strategies can instead be viewed as ingredients for a hybrid preventive strategy: consequence prevention."[8] In a similar fashion, the Strategic Citizen seeks to prevent the consequences of spontaneous close combat, not necessarily preventing the aggression from taking place. Furthermore, the Strategic Citizen concept does not aim to substitute existing prevention based security programs, it intends to supplement them.

NEW CONCEPT - EXISTING PROGRAM

The archetype for the Strategic Citizen concept is the FFDO program, which became law in the Homeland Security Act of 2002.[9] This legislation required the Department of Homeland Security (DHS) to "establish a program to deputize volunteer pilots of air

carriers…to defend the flight decks of aircraft of such air carriers against acts of criminal violence or air piracy."[10] Arming volunteer pilots provided - an individual - the opportunity to prevent the consequences of criminal violence or air piracy.

As the Strategic Citizen is specific to infrastructure protection, a foundational understanding of what is considered Critical Infrastructure and Key Resources is helpful. Although they each have separate definitions, the Department of Homeland Security (DHS) seems to associate CIKR[11] as an integrated entity. The USA PATRIOT Act defines Critical Infrastructure as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (Sec. 1016(e))."[12] Whereas the Homeland Security Act of 2002 defines Key Resources as "publicly or privately controlled resources essential to the minimal operations of the economy and government (Sec. 2(9))."[13] For the purpose of this article, a Strategic Citizen model would use the current definitions of CI and KR, in conjunction with the 18 CIKR sectors identified in the National Infrastructure Protection Plan (NIPP)[14] as a working framework for applicability. Additionally, it is important to keep in mind that aggressors might not only want to destroy CIKR, but weaponize it (e.g. 9/11).

Being that the FFDO program is the model for the Strategic Citizen, baseline programmatic characteristics are critical. Arguably, the most important aspect of the FFDO program is the pilot's legal authority. There are two vital characteristics that are distinctive to the FFDO program; the first is that *"FFDOs are considered Federal law enforcement officers only for the limited purposes of carrying firearms and using force, including lethal force, to defend the flight deck of an aircraft from air piracy or criminal violence."*[15] Secondly, *"FFDOs are not granted or authorized to exercise other law enforcement powers such as the power to make arrests, or seek or execute warrants for arrest, or seizure of evidence, or to otherwise act as Federal law enforcement outside the jurisdiction of aircraft flight decks."*[16] The legal authority of the pilot is specific; FFDOs are not government "agents" in any traditional sense. These important legal stipulations are key distinctions that distinguish the FFDO from other physical security models.

Additionally, the pilot has been given legal protections. A "federal flight deck officer shall not be liable for damages in any action brought in a federal or state court arising out of acts or omissions of the officer defending the flight deck of an aircraft against acts of criminal violence or air piracy unless the officer is guilty of gross negligence and/or willful misconduct."[17]. To ensure accountability, any type of Strategic Citizen model must possess a similar legal framework as the FFDO program.

Eligibility is another crucial component of the FFDO program. Aside from specific airline related requirements, an applicant must be a volunteer (participation is not mandatory) and a U.S. citizen.[18] Participating volunteers "are not eligible for compensation from the Federal Government for services provided as a Federal Flight Deck Officer."[19] It is also a prerequisite that the applicant successfully complete assessments for psychological, medical or physical ability requirements.[20] These eligibility requirements and other programmatic characteristics help ensure that only capable and competent individuals are selected to become FFDOs.

Additionally, while the government provides the training and equipment (including firearm), volunteers are responsible for lodging and travel to the training facilities. These out of pocket expenses are about $200, not including travel.[21] Once volunteers have successfully negotiated the eligibility, selection and training process, they are deputized as Federal Flight Deck Officers for a period of five years.[22] FFDOs are also required to perform bi-annual training on their own time and at their own expense.[23] The volunteer nature of the FFDO program has other cost benefits as well.

Christopher Bellavita correctly points out that "if we are not attacked again within the next decade, it will be difficult to maintain the nation's homeland security apparatus. The national government's budget, let alone most states' and cities' budgets, will not sustain it. Homeland security as a national program will atrophy."[24] Furthermore, the target is not necessarily "the airplane, or the mall, or the subway. Bin Laden has made his goal clear. The target is our economy: "We bled Russia for ten years until it went bankrupt and was forced to withdraw in defeat…. We are continuing in the same policy to make America bleed profusely to the point of bankruptcy.""[25] Not only does our CIKR physical security model need to be effective, it needs to be affordable.

Using data provided by the Airline Pilots Security Alliance, it is estimated that a ten year annualized FFDO program would cost $29million per year and protect 97% of airline flights.[26] "As a comparison, the federal air marshal program costs $688[million] per year and protects only about 5% of airline flights."[27] Recognizing the value of volunteer citizens could reduce the financial costs of a statist approach to physical security.

The other potential cost, which is somewhat obscure at this point, is if a mass casualty armed attack (e.g. Mumbai) happened in the United States – what types of security measures would government consider in the aftermath? Would new security programs be introduced? Could we afford it? Would those new programs affect civil liberties? It is important to provide policy makers' different homeland security models to mull over periodically. If the day comes when homeland security legislation is

extremely urgent, this expanded dialogue performs a valuable service of generating informal pre-debate.

THREAT OWNERSHIP

As stated previously, spontaneous close combat articulates a more appropriate threat construct, which captures distinctive advantages common to armed aggressors – spontaneity and proximity. Furthermore, research recognized by the *National Criminal Justice Reference Service* (*NCJRS*)[28] illustrates response times and the subsequent limitations law enforcement has in swiftly preventing the consequences of active shooter incidents.

Essentially, the Strategic Citizen concept seeks to reduce victim personal injury and property loss from the time an armed aggressor strikes, to the time the aggressor is incapacitated. Data suggests that dependence on a traditional law enforcement centric physical security model, against an active shooter, results in one person shot every 15 seconds until the aggressor is incapacitated. The FFDO program is an existing DHS physical security model for CIP, whose characteristics could be applied to other CIKR sectors for potentially reducing victim personal injury and property loss against spontaneous close combat.

Data is scarce which compares the efficacy of active shooter victim self-protection (with a firearm) encounters, against active shooter law enforcement encounters. Research comparing personal injury and property loss data, between victim self-protection (with a firearm) in an active shooter scenario visa vie law enforcement would be beneficial. This is an area where further research is necessary.

However, data is available that indicates using a firearm is effective for self-protection. Research by Gary Kleck and Don B. Kates suggests that where a firearm was used in self-defense, risk for personal injury and property loss is reduced in comparison to other self-protective measures. “In general, self-protection measures of all types are effective, in the sense of reducing the risk of property loss in robberies and confrontational burglaries, compared to doing nothing or cooperating with the offender. The most effective form of self-protection is use of a gun.”[29] From an injury standpoint, research suggests “although many victims are hurt in personal contact crimes, few are injured after using self-protection measures, and thus there is little injury that could have been provoked by victim resistance.”[30] Furthermore, Jongyeon Tark and Gary Kleck infer that “resistance with a gun appears to be most effective in preventing serious injury, though this finding is not statistically significant due to the small number of reported gun cases.”[31] Again, this is an area that requires further research as it pertains to active shooter incidents. However, extrapolation from this research suggests that expanding the FFDO program to other CIKR sectors, could provide an opportunity to

reduce victim personal injury and property loss in relation to active shooter incidents in the absence of a law enforcement presence.

As part of addressing the arming of pilots, a Government Accountability Office report[32] discussed the advantages and disadvantages of arming the crew for enhancing airline security. In the report, the disadvantages of Less-Than-Lethal alternatives are their inability to decisively incapacitate an aggressor. In an active shooter scenario, the effective incapacitation of an aggressor is a key component for reducing victim personal injury and property loss. Although the FFDO operating environment may differ from other CIKR sectors, the characteristics of the FFDO program could provide other CIKR physical security programs an existing framework to build upon. Interestingly, the current threat environment is persuading those beyond aviation to consider an armed physical security model as well.

Merchant mariner Richard Phillips was the Captain of the Maersk Alabama when his ship was attacked by Somali pirates and he was taken hostage. Five days later, military intervention successfully rescued Captain Phillips.[33] Testifying before Congress to address piracy, Captain Phillips suggested that arming the crew could be one component of a holistic maritime security strategy. In his testimony, Captain Phillips stated "that arming the crew, as part of an overall strategy, could provide an effective deterrent under certain circumstances and I believe that a measured capability in this respect should be part of the overall debate about how to defend ourselves against criminals on the sea."[34] Subsequently, the Maersk Alabama was attacked a second time by pirates. On this occasion, however, an embarked security team was able to repel the attack using acoustic devices and small arms fire.[35]

Although not statistically significant, utilizing basic observation and deductive reasoning implies the Maersk Alabama is an interesting case. The same ship was attacked twice by pirates; in the first attack victims were unarmed, in the second attack the victims were armed. Where firearms were absent, part of the crew was taken hostage. In the attack where firearms were present, the attack was repelled; thereby reducing the risk of victim personal injury and property loss. Others are also educating themselves on potential benefits of embedded armed physical security.

Concerned with an asymmetric threat environment, the Harrold Independent School District in Texas has decided to allow their teachers to be armed; a policy which the Governor supports.[36] "In order for teachers and staff to carry a pistol, they must have a Texas license to carry a concealed handgun; must be authorized to carry by the district; must receive training in crisis management and hostile situations and have to use ammunition that is designed to minimize the risk of ricochet in school halls. Superintendent David Thweatt said the small community is a 30-minute drive from the

sheriff's office, leaving students and teachers without protection."[37] This policy indicates that arming teachers provides an opportunity to reduce victim injury and property loss against armed aggression in the absence of a law enforcement presence. With active shooter incidents such as Columbine, Beslan, Virginia Tech etc., educators are starting to revisit and readjust their physical security posture.

Terrorists - albeit aggressors - are adapting and exploiting America's physical security weaknesses. In an incremental and independent manner, the threat of spontaneous close combat has encouraged elements of both the public and private sector to gravitate toward an FFDO type of physical security model. Additionally, the current government centric CIKR physical security model could also be difficult to improve. Privacy concerns, diversity of threats, and budgetary constrains represent public safety challenges for all levels of government. In light of the adapting threats, a more flexible physical security model should be considered.

DECENTRALIZE PHYSICAL SECURITY

In the book, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*[38] the logic for a Strategic Citizen model is further explained. Authors Ori Brafman and Rod A. Beckstrom, from an organizational standpoint, compare the effectiveness of centralized organizations against ones that are decentralized. The spider and the starfish – the former considered centralized and the latter decentralized - appear similar where both have many legs for support and function, but are different in terms of survivability. As Brafman and Beckstrom indicate, if a spider were sliced in half it would die. However, if a starfish were sliced in half the result is two functioning starfish.

In the context of the Global War on Terrorism, organizations such as Al Qaeda behave in a decentralized manner and attempt to function like a starfish. However, on 9/11 the centralized physical security model could not prevent the consequences of terrorists seizing commercial aircraft. The creation of the FFDO program is a tacit recognition that a decentralized physical security program was essential for preventing the consequences of terrorists attempting to pirate commercial aircraft.

Luis P. Villarreal provides a "Natural Security" corollary; consider the relationship the immune system has with the body. The immune system does not "depend on a central authority, such as our brain, to initiate a response."[39] In fact, "our immune systems do this automatically, against old or new threats, with no central authority."[40] In the context of homeland security, our current physical security model for CIKR lacks an immune system. At present, our CIKR physical security resources addressing spontaneous close combat are primarily dependent upon and dispatched by a governmental brain.

The Strategic Citizen concept is similar, in principle, to other volunteer based public safety initiatives as well. As an example, the American Red Cross provides training and encourages volunteers to learn First Aid, CPR and AED training so that an individual has the "confidence to respond in an emergency situation with skills that can save a life."[41] For instance, if someone were in need of CPR and immediate medical assistance, it would be unreasonable to suggest that an immediate observer should wait for authorized medical responders in order to provide chest compressions. Additionally, it would seem somewhat strange if fire departments did not encourage individuals to operate fire extinguishers for preventing the consequences of spontaneous fire. These public safety initiatives are effective because they operate in a decentralized and independent manner. The same public safety logic should also apply to physical security approaches.

Brafman and Beckstrom conclude that a hybrid organization is ideal – where elements of both centralization and decentralization are present. The FFDO, indeed, is a hybrid physical security model. The FFDO program is centralized from an administrative standpoint while being decentralized from a security standpoint. The FFDO program's authorization, accountability and training are provided by a centralized organization (e.g. DHS) – much like the Red Cross administers first aid training. Once trained, FFDO's become dispersed, providing embedded physical security in a random and decentralized manner; where elements of both the spider and the starfish exist.

FURTHER CONSIDERATIONS

Consequently, further considerations for implementing a Strategic Citizen concept are required. Although the FFDO is an already existing DHS program, I have no expectations for a Strategic Citizen concept to be implemented anytime soon - due to what some may consider its controversial nature. Moreover, I encourage a vigorous debate regarding the merits of this concept. Below are some areas that require further deliberation and certainly more research.

- Weapon Safety

  It is likely the same arguments made - for and against - arming pilots will reemerge for a Strategic Citizen model.[42] An open and honest conversation of security models addressing the threat of spontaneous close combat is important. With that said, in 2008 there was an accidental discharge by an FFDO aboard an aircraft; no one was injured. However, the DHS Inspector General (IG) concluded the "locking holsters used by the Federal Flight Deck Officer (FFDO) program increases the likelihood of an accidental discharge of a weapon in an aircraft cockpit."[43] Furthermore, the DHS IG recommended "TSA should discontinue the

use of the locking holster and consider other methods for FFDO to secure their weapons."[44]

Weapon safety must be a top priority. However, within the context of spontaneous close combat, it is crucial to swiftly incapacitate an armed aggressor that is threatening life and property. Clearly, more research would be needed for the type of authorized weapon and handling requirements as it relates to a Strategic Citizen's specific CIKR operating environment.

- Fratricide

  Certainly, the possibility of friendly fire is a concern for any armed self-defense situation against an active shooter. Law enforcement refers to a similar concern known as deconfliction. In undercover investigations, the possibility exists for investigators to work within close proximity to other undercover agents unknowingly. Within this sometimes hazy operational environment, "agencies may interfere with each other's cases, causing investigative efforts to be disrupted or, worse, officers to be unintentionally hurt or killed."[45]

  To mitigate this risk, a deconfliction system[46] has been developed for the purpose of increasing officer safety while operating in an asymmetric threat environment. Although the approach to officer safety through a deconfliction mechanism may not be a precise solution for the Strategic Citizen model in addressing the potential of friendly fire, it could however, provide a foundational framework from which to build. More research and analysis regarding this subject is necessary.

- Legislation

  Due to the complicated legal issues associated with a Strategic Citizen model, legislation will likely be required to allow armed volunteer's to provide CIKR physical security. Legislation may also be needed on the federal level if certain infrastructures span across State lines. As stated earlier, if something does happen and policy makers need an immediate solution, there may be little time for spirited debate. An assortment of solutions must be readily available when circumstances demand options.

- Sector Applicability

  As previously mentioned, the current CIKR definitions could indicate sectors where a Strategic Citizen model might apply. Furthermore, each CIKR sector is not going to have the same operating environment as that of an FFDO. Defensive training will need to be sector specific - much like the FFDO – and will need to

address the dynamics of armed interactions as it pertains to spontaneous close combat. Further research is required to analyze how a Strategic Citizen model would operate as it pertains to the respective CIKR sector environments.

It should also be stated that a Strategic Citizen model is not indented to replace in anyway a concealed carry permit or law enforcement. The former will still be necessary for self/home defense; the Strategic Citizen model is specific to CIKR physical security. As for the latter, to paraphrase and reiterate FFDO program guidelines, a Strategic Citizen "would not be granted or authorized to exercise other law enforcement powers such as the power to make arrests, or seek or execute warrants for arrest, or seizure of evidence, or to otherwise act as law enforcement outside their respective and legally defined CIKR jurisdiction."[47]

CONCLUSION

The current homeland security CIKR physical security paradigm for an active shooter is insufficient in rapidly preventing the consequences of spontaneous close combat. When research suggests a person is shot every 15 seconds in an active shooter scenario, the current CIKR physical security paradigm should be revisited. A Strategic Citizen model, based on characteristics from the FFDO program, provides an opportunity to reduce victim injury and property loss against spontaneous close combat in the absence of law enforcement. It is an unreasonable expectation for government to provide immediate CIKR physical protection when an armed aggressor strikes; especially if there are multiple and/or simultaneous attacks. The creation of the FFDO program is at least an implied acknowledgement of government limitations.

In an asymmetric and uncertain threat environment, where Americans demand freedom, increased security and fiscal discipline – responsible volunteer citizens may be required to provide decentralized CIKR physical security against the threat of spontaneous close combat.

---

[1] U.S. Department of Justice, National Criminal Justice Reference Service (NCJRS). http://www.ncjrs.gov/App/Publications/abstract.aspx?ID=245861; "Patrol Response Challenge," *Law and Order* 56, no.6 (June 2008).
[2] General Charles Krulak, "The Strategic Corporal: Leadership in the Three Block War," *Marines Magazine*, January 1999. http://www.au.af.mil/au/awc/awcgate/usmc/strategic_corporal.htm
[3] Ibid.
[4] The 9/11 Commission Report. *Final Report of the National Commission on Terrorist Attacks upon the United States*, New York: W.W. Norton, p.339; Christopher Bellavita, "What is Preventing Homeland Security?," *Homeland Security Affairs* 1, no. 1 (Summer 2005) http://www.hsaj.org/?article=1.1.3
[5] Brian Jackson, "Marrying Prevention and Resiliency: Balancing Approaches to an Uncertain Terrorist Threat," *RAND*, 2008, http://www.rand.org/pubs/occasional_papers/2008/RAND_OP236.pdf
[6] Ibid., p.10
[7] Ibid.
[8] Ibid.

[9] Library of Congress. Thomas. Homeland Security Act 2002, Title XIV. http://thomas.loc.gov/cgi-bin/query/F?c107:1:./temp/~c107uCmrMQ:e528114:
[10] Ibid.
[11] Department of Homeland Security. *National Infrastructure Protection Plan 2009 (NIPP).* http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf
[12] John Moteff and Paul Parfomak, *, Critical Infrastructure and Key Assets: Definition and Identification*, CRS Report for Congress, RL 32631 (October 2004), p. 7. http://digital.library.unt.edu/govdocs/crs/data/2004/meta-crs-5954.tkl; Library of Congress THOMAS, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*, http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3162.ENR:
[13] Ibid., p.7; Library of Congress THOMAS, *Homeland Security Act of 2002*, http://thomas.loc.gov/cgi-bin/query/z?c107:h.r.5005.enr:
[14] Department of Homeland Security, *National Infrastructure Protection Plan (NIPP)* http://www.dhs.gov/files/programs/editorial_0827.shtm
[15] Department of Homeland Security, Transportation Security Administration. *Federal Flight Deck Officer Important Information*. http://www.tsa.gov/lawenforcement/programs/ffdo_information.shtm
[16] Ibid.
[17] Ibid.
[18] Department of Homeland Security, Transportation Security Administration. *Federal Flight Deck Officer Eligibility Criteria*. http://www.tsa.gov/lawenforcement/programs/ffdo_eligibility.shtm
[19] Department of Homeland Security, Transportation Security Administration. *Federal Flight Deck Officers*. http://www.tsa.gov/lawenforcement/programs/ffdo.shtm
[20] Department of Homeland Security, Transportation Security Administration. *Federal Flight Deck Officers Selection and Training*. http://www.tsa.gov/lawenforcement/programs/ffdo_training.shtm
[21] Ibid.
[22] See, *Federal Flight Deck Officer Important Information*
[23] See, *Federal Flight Deck Officers Selection and Training*
[24] Christopher Bellavita, "Changing Homeland Security: Shape Patterns, Not Programs," *Homeland Security Affairs* 2, no. 3 (2006), p.6. http://www.hsaj.org/?article=2.3.5
[25]See, "What is Preventing Homeland Security?," p.5.
[26] Airline Pilots Security Alliance. *Standardized Federal Flight Deck Officer (FFDO) Program Costs*. http://www.secure-skies.org/armedpilotcosts.php
[27] Ibid.
[28] See, *Patrol Response Challenge*; National Criminal Justice Reference Service *(*NCJRS*)*
[29] Gary Kleck and Don B. Kates. *Armed: New Perspectives on Gun Control*. Amherst:Prometheus Books, 2001. p. 294.
[30] Ibid.
[31] Jongyeon Tark and Gary Kleck, "Resisting Crime: The Effects of Victim Action on the Outcomes of Crimes," *Criminology* 42, no. 4 (2004), p. 902.
[32] U.S. Government Accountability Office. *Information Concerning the Arming of Commercial Pilots, GAO 02-822R*. 28 June 2002. http://www.gao.gov/new.items/d02822r.pdf
[33] Andrea Stone, "Capt. Phillips calls for arming ship officers," *USATODAY.com*, April 30, 2009, http://www.usatoday.com/news/washington/2009-04-30-captain-phillips_N.htm.
[34] Richard Phillips, *Statement of Captain Richard Phillips, Master, Maersk Alabama, to the Senate Committee on Foreign Relations* (United States Senate, 2009), http://foreign.senate.gov/testimony/2009/PhillipsTestimony090430p.pdf.
[35] 2nd Class Nathan Schaeffer, "M/V Maersk Alabama Repels Suspected Pirate Attack," *U.S. Naval Forces Central Command, U.S. Fifth Fleet*, November 18, 2009, http://www.cusnc.navy.mil/articles/2009/195.html.
[36] Angela K. Brown, "Teachers armed for school," *The Washington Times*, August 27, 2008, http://www.washingtontimes.com/news/2008/aug/27/teachers-armed-for-school/.
[37] "North Texas school district will let teachers carry guns," *The Houston Chronicle*, August 15, 2008, http://www.chron.com/disp/story.mpl/front/5945430.html; Harrold Independent School District,

Safety Program/Risk Management Emergency Plans.
http://www.tasb.org/policy/pol/private/244901/pol.cfm?DisplayPage=CKC%28LOCAL%29.pdf&QueryText=FIREARMS

[38] Ori Brafman, and Rod A.Beckstrom. *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*. New York: Penguin Group, 2006

[39] Luis P. Villarreal. 2008. "From Bacteria to Belief: Immunity and Security." In *Natural Security: A Darwinian Approach to a Dangerous World,* ed. Raphael D. Sagarin and Terence Taylor, 44. Berkley: University of California Press.

[40] Ibid.

[41] Prepare for Emergencies with American Red Cross First Aid, CPR and Automated External Defibrillator (AED) Courses. *American Red Cross*. http://www.redcross.org/static/file_cont5294_lang0_1934.pdf

[42] See, *Information Concerning the Arming of Commercial Pilots,*

[43] Department of Homeland Security, Office of Inspector General, Semiannual Report to Congress (April 1, 2008 – September 30, 2009), p.28.
http://www.dhs.gov/xoig/assets/semiannlrpts/OIG_SAR_Apr08_Sep08.pdf

[44] Ibid., p.29.

[45] Regional Information Sharing Systems, RISSafe™, Officer Safety Event Deconfliction System.
http://www.riss.net/rissafe.aspx

[46] Ibid.

[47] See, *Federal Flight Deck Officer Important Information*

What's with All This Peer-Review Stuff Anyway?*

Jon S. Warner**

Vulnerability Assessment Team
Argonne National Laboratory

Introduction

The *Journal of Physical Security* was ostensibly started to deal with a perceived lack of peer-reviewed journals related to the field of physical security. In fact, concerns have been expressed that the field of physical security is scarcely a field at all.[1]

A typical, well-developed field might include the following:[1] multiple peer-reviewed journals devoted to the subject, rigor and critical thinking, metrics, fundamental principles, models and theories, effective standards and guidelines, R&D conferences, professional societies, certifications, its own academic department (or at least numerous academic experts), widespread granting of degrees in the field from 4-year research universities, mechanisms for easily spotting "snake oil" products & services, and the practice of professionals organizing to police themselves, provide quality control, and determine best practices. Physical Security seems to come up short in a number of these areas.

Many of these attributes are difficult to quantify. This paper seeks to focus on one area that is quantifiable: the number of peer-reviewed journals dedicated to the field of *Physical Security*. In addition, I want to examine the number of overall periodicals (peer-reviewed and non-peer-reviewed) dedicated to physical security, as well as the number of papers published each year about physical security. These are potentially useful analyses because one can often infer how healthy or active a given field is by its publishing activity. For example, there are 2,754 periodicals dedicated to the (very healthy and active) field of physics.[2]

Type of Journals

This paper concentrates on trade journal versus peer-reviewed journals. Trade journals typically focus on practice-related topics. A paper appropriate for a trade journal is usually based more on practical experience than rigorous studies or research. Models, theories, or rigorous experimental research results will usually not be included. A trade journal typically targets a specific market in

* Editor's note: This paper was not peer-reviewed.
** Associate Editor, Journal of Physical Security

an industry or trade. Such journals are often considered to be news magazines and may contain industry specific advertisements and/or job ads.

A peer-reviewed journal, a.k.a "referred journal", in contrast, contains peer-reviewed papers. A peer-reviewed paper is one that has been vetted by the peer review process. In this process, the paper is typically sent to independent experts for review and consideration. A peer-reviewed paper might cover experimental results, and/or a rigorous study, analyses, research efforts, theory, models, or one of many other scholarly endeavors.

Why Peer Review?

Any field advances when there is a collaborative effort of sharing research, ideas, or other scholarly work in an open forum. This forum fosters discussion and helps shape the future of the field. In the world of academics, the most common and accessible forum available is the peer-reviewed journal. The "peer-review" process is essentially a pre-publication vetting process.

The reviewer is one of the key players in this vetting process. The reviewer is considered to be a subject matter expert by the editorial staff of the journal. A reviewer looks at the paper with a fresh eye, looking for mistakes or omissions and also determines if the paper is novel and substantial enough to warrant publication. The peer-review process is considered essential to the quality of an academic paper. From the peer review process, the community gains a high quality paper and the author gets a peer-reviewed publication. In some fields, the metric for being considered an expert is based upon the number (and/or importance) of peer-reviewed papers one has published. "Publish or perish" is a familiar mantra in many academic circles.

In academia (especially in science and engineering), researchers frequently present their work in the form of a peer-reviewed paper. Discussion usually follows. Bugs, problems, flaws, and weaknesses are hashed out and the field benefits from the discussion/disagreements and from an improved paper. It is the power of the peer review process that helps facilitate this process. Without open lines of communication, every person in a given field would be "reinventing the wheel" on an individual basis. In such a situation, the field would not progress very effectively, if at all. Trade journals alone are not enough to foster the type of information sharing and careful review that is necessary to enable a field to progress in a positive, rigorous, and healthy manner.

The Peer-Review Process

The peer review process begins when the editorial staff of a journal receives a paper or manuscript. The editor sends a copy of the work to a small number of external experts for review (typically two to three reviewers per paper). The reviewers usually work independently and typically do not know who the other reviewers are. The reviewers' main job is to evaluate the paper on its own merits and remain emotionally unattached during the review.

The reviewers' identities are typically kept secret from the authors of the paper. This makes it easier for the reviewers to offer objective criticism. Some peer-reviewed journals even try to keep the author's identity anonymous to the reviewers, though this is uncommon. The editor is usually the only person who knows the names of all the involved players. The editor is the chief decision maker in the process, whereas the reviewers act in an advisory capacity.

After the reviewers are finished, they each supply the editor with their critique, noting suggestions for improvement, weaknesses, or any other issues. Often, the reviewers have a list of specific issues or problems they would like to have addressed. The reviewer also supplies 1 of 4 general responses: 1) publish as is, 2) accept the paper for publication if the author improves the paper, 3) reject the paper but encourage resubmission after a rewrite, or 4) outright rejection.

After receiving all the reviewers' feedback, the editor might accept or outright reject the paper as it is. If the reviewers disagree about publishing, the editor might solicit another reviewer to act as a tiebreaker. More often, however, the editor compiles a list of concerns or questions brought up during the feedback process and ask that the author address the criticisms.

After receiving the critique, the author might address a given issue by modifying the paper, drafting a rebuttal, or some combination thereof. If the author were so inclined, he or she may pull the paper from further publication consideration at any point in the process.

When the editor receives a response from the author, the editor might then decide to publish the paper (or not) depending on the persuasiveness of the response. Alternatively, the editor may share the author's response with (and solicit a response from) each reviewer who raised a specific concern. Once the editor is satisfied the quality of the paper meets an accepted standard for the discipline, the paper is on it's way to publication.

After a paper has completed these steps, it is considered "peer-reviewed." The paper, having been accepted for publication, is now viewed as having merit and academic standing.

Anecdotal evidence about the lack of peer-reviewed physical security journals was the impetus for the *Journal of Physical Security*. This paper attempts to

provide an analysis of peer-reviewed papers and journals covering the field of Physical Security.

Peer Reviewed Physical Security Papers

The first point we will address is: are papers covering physical security being published in significant numbers? If not, then the argument could be made that there is no need for additional physical security journals.

Google Scholar

Google Scholar[3] includes a search of every book, article, journal, etc. in the Google database. Google Scholar has many of the inherent disadvantages of other types of Google searches, e.g., the Google database is huge. Searching {1989 Toyota pickup gas mileage}, for example, returns 559,000 hits. This is overwhelming. When looking for something specific, one can click through the results until an exact match is found.

Quantitative searches are a much more difficult problem. A search for {physical security articles} would be a good example. This search in Google Scholar returned 2,190,000 hits. There are some advanced search options, but in the context of this paper, these options seemed limited.

A refinement of the original search to {physical security articles – computer – cyber} returned 1,870,000 hits. (These searches seem to result in a lot of round numbers!) By eliminating matches that contained “computer” and “cyber” we can narrow the scope of the search.

Searching for {physical security articles – computer – cyber + ”peer reviewed”} returned 14,900 hits for the years 1990-2009. This works out to 784 papers per year. Putting quotes around “peer reviewed” tells the search engine to look for only these words in that specific order.

The most telling refinement comes from the search {“physical security*”* – computer – cyber + ”peer reviewed”}, which returns 170 hits over the 1990-2009 time period. This works out to about 9 papers a year. The same search without the “peer reviewed” portion returns 17,100 hits, or 900/year. I then tried filtering out social science articles: the search was run again with “-social” included in the search string. This reduced the result to 4,910 papers, or about about 258/year.

These results indicate that peer-reviewed physical security papers are indeed being published in significant, though not large numbers.

Argonne National Laboratory Library Article Search

To further investigate physical security publications, I turned to the ISI Web of Knowledge.[4] The Argonne National Laboratory library services department was very helpful in this endeavor.

The Web of Science/Knowledge is a science and social citation index consisting of several databases with information collected from thousands of scholarly journals, books, book series, reports, conferences, and more. The databases contain the: Science Citation Index Expanded; Social Sciences Citation Index; Arts & Humanities Citation Index; Conference Proceedings Citation Index - Science; Conference Proceedings Citation Index - Social Sciences & Humanities; Index Chemicus; and the Current Chemical Reactions. In short, this resource represents a broad range of papers published in the technical and social sciences.

A topic search of {security} resulted in 34,484 articles for 2005-2009. Almost 51% of these security papers were related to computer security. Narrowing the search to the words {physical} and {security} resulted in 2,923 articles, or 730 papers/year on average.

Approximately 8.5% of the security papers published contain the words "physical" and "security" within the text. The exact phrase {"physical security"} further refined the search down to 718 papers over the same four-year period. This works out to 179 papers a year, or 2% of all the security papers published in these journals. A quick scan of the underlying journals indicates that many of these papers were indeed peer-reviewed.

The ISI Web of Science/Knowledge results reinforce what we found earlier in the Google Scholar search. Papers about physical security are being written and published, though not in overwhelming numbers.

Peer Reviewed Physical Security Journals

The next question I tried to answer was whether physical security papers have a small number of periodicals dedicated to them, or are they scattered over the spectrum of periodicals that cover the field of security in general?

Bacon's Magazine Directory-2009

The first resource that I examined to address this question was the 2009 Bacon's Magazine Directory.[5] Bacon's lists 18,500 trade, professional, and

consumer periodicals in the United States and Canada. Below are some selected fields and the number of periodicals related to those fields:

Banking and Finance (557)
Arts and Entertainment (368)
Beverages (128)
Gifts, Antiques, and Collectables (73)
Fruits, Nuts, and Vegetables' (39)
Waste Management (38)
Rock and Cement Products (33)
Philanthropy (31)
Religious Administration (30)
Security (27)
Field Crops (25)
Plastics and Rubber (22)
Mortuaries and Cemeteries (17)
Tobacco (14)
Cleaning and Laundry (13)
Farm Chemicals and Fertilizers (9)

The periodicals listed in Bacon's are primarily trade journals that report on new products, plus offer staff-written articles, trade literature, by-lined articles, letters, etc. Although these journals may host physical security related articles, they really aren't peer-reviewed scholarly journals. In the area of security, there are 27 journals reported by Bacon's. Not one of these is dedicated to physical security. The Bacon's results seem to identify few (or no) physical security journals.

Genamics[6]

The Genamics[7] JournalSeek website (http://journalseek.net) is the largest free journal information database available on the Internet, containing 95,320 titles. It lists 144 periodicals with "security" in the title. They break down as follows:

Computer, network, IT, or information security: 42 (29.2%)
Counter-terrorism/homeland security: 5 (3.5%)
Geopolitics, peace and conflict studies, intelligence, national defense: 39 (27.1%)
Security Management: 4 (2.8%)
Social Security: 13 (9.0%)
Security Products Trade Journals: 7 (4.9%)
Nuclear Security, Safeguards, & Nonproliferation: 2 (1.4%)
Human Rights: 1 (0.7%)
Criminology & Police: 3 (2.1%)
Other, including Transportation, Library, Bank, Health Care, Hotel Security; and Security Law: 18 (12.5%)

Of these 144 periodicals, not one is devoted solely or primarily to physical security (except arguably 2 of the trade journals devoted to security sales and marketing), though 16 of the 144 periodicals contain articles or papers about physical security fairly often. (7 of these 16 periodicals are peer reviewed, with 2 of the 7 primarily about nuclear safeguards and nonproliferation, not physical security *per se*).

As with the Bacon's results, we can again conclude that there is a dearth of physical security periodicals (including peer-reviewed journals), and that any papers about physical security are scattered over the spectrum of existing security periodicals.

Ulrich's Periodical Directory

This resource is the 500lb gorilla of periodical databases. The Ulrich's worldwide serials directory[2] covers "300,000 serials from 90,000 publishers spanning 950 subject areas and 200 languages." The University of Chicago provided the Ulrich's periodical directory service used during this research.

Ulrich's reports that worldwide there are 16,835 periodicals relating to Law; 10,076 covering Sports; 8,924 involving Transportation; 8,880 on Engineering; 2,754 on Physics; and 437 journals on Security.

The breakdown by number of periodicals per topical area is interesting:

Folklore (661)
History of Asia (649)
Alternative Medicine (469)
Glass and Pottery (441)
***Security* (437)**
Physics of Heat (140)
Birth Control (175)
Leather and Fur (194)
Urology and *Nephrology* (392)
Postal Affairs (156)

Of the 437 security periodicals, 33 (7.5%) are peer-reviewed. Over half (58%) of the 33 peer-reviewed journals are categorized as Computer Security (19). A total of 10 (~30%) are classified as Criminology and Law Enforcement. Two of the periodicals (6%) cover Cryptography (another 3 Cryptography journals share classification with Computer Security), one journal is devoted to Transportation Security (from France), and one covers Library and Archival Security (United States).

Demographically, the United Kingdom is responsible for 48% of the 33 peer-reviewed security journals, with the United States coming in second (33%), followed by the Netherlands (6%). Switzerland, Germany, Japan, and France are tied with one peer-reviewed security journal apiece.

Of the original 437 security-related periodicals reported by Ulrich's service, none are solely dedicated to physical security. To put this into perspective, there are 204 journals devoted to *Astrology,* and 7 (3%) of these are peer-reviewed! There are also 9 journals about *Cold Fusion,* and 3 (33%) of these are peer-reviewed.

Ulrich's Periodical Directory probably does not include every periodical available. For instance, they omitted the *Journal of Physical Security*. Certainly though, the results can be taken to be representative of the overall pool of existing periodicals. This data confirms the previous two conclusions: There are few, if any, peer-reviewed journals dedicated to physical security and the existing physical security papers tend to be spread out over many different periodicals.

Discussion

There seems to be a general consensus that physical security is an important field. It's broad in scope, covering the protection of important assets such as people, airplanes, buildings, money, weapons, pharmaceuticals, chemicals, documents, equipment, food and drink products, merchandise, etc. This includes protection from theft, tampering, espionage, terrorism, sabotage, destruction, vandalism or unauthorized access. This diversity of scope makes physical security an extremely complex and rich field to work in.

One would expect extensive pockets of physical security research being conducted in academia, as well as in government and at private companies. The depth and scope of physical security research, it would seem, ought to be vast, involving a highly multi-disciplinary collaboration by security practitioners, security managers, engineers, social scientists, computer scientists, psychologists, chemists, physicists, mathematicians, etc. In order to share information, recognize failures and successes, and exchange ideas across the entire field, some form of effective communication is required. One of the most important communication channels available to other fields is the peer-reviewed journal.

Although, this is a very rudimentary study, the results clearly indicate that there are few peer-reviewed journals dedicated to the field of physical security. Papers about physical security are scattered throughout the (not very large) universe of existing periodicals, but perhaps not in the numbers we might expect for a field of this importance.

One troubling aspect of this conclusion is that perhaps this is a symptom of a much larger problem. Perhaps, as suggested above, the field of physical security isn't much of a field at all.

What can be done? More physical security papers need to be written and submitted to peer-reviewed journals. Although the peer-review process is time consuming, it helps to ensure the quality of the work being presented. One can think of the peer review process as a vulnerability assessment of the authors' paper. The paper will be much stronger after the process.

Acknowledgements

I'm grateful to Gary N. Davidoff and Todd J. Morris of the Argonne National Laboratory research library for their assistance during the course of this work, and Roger Johnston for providing the Genamics results and offering suggestions about the paper.

References

[1] R.G. Johnston, " How to Conduct an Adversarial Vulnerability Assessment", Invited Talk for the National Security Institute's IMPACT06 Security Conference, Falls Church, VA, April 3-5, 2006, (Los Alamos National Laboratory Report LAUR-06-1737).

[2] Ulrich's Periodical Directory, "Ulrich's Web.com" 2009. http://www.ulrichsweb.com/ulrichsweb/ (accessed December 10, 2009)

[3] Google, "Google Scholar Beta." 2009. http://scholar.google.com/schhp?hl=en&tab=ws (accessed December 10, 2009)

[4] Thomas Reuters, "ISI Web of Knowledge." 2009. http:// isiknowledge.com/ (accessed December 10, 2009)

[5] Cision, "Newspaper/Magazine Directory" 2009. http://us.cision.com/product.asp?key={ABFD28FA-2794-4611-BF03-1B01CEBC3C80} (accessed December 10, 2009).

[6] The following is a private communication from Roger Johnston, Vulnerability Assessment Team, Argonne National Laboratory.

[7] Genamics, "JournalSeek" 2009. http://journalseek.net/ (accessed December 10, 2009).

Journal of Physical Security 4(1), 31-35 (2010)

Viewpoint Paper

Museum Security and the Thomas Crown Affair*

Eric C. Michaud

Vulnerability Assessment Team
Argonne National Laboratory

Over the years, I've daydreamed about stealing a Vermeer, a Picasso, or Rembrandt. It tickles me, as much as watching the reboot of *The Thomas Crown Affair*.[1] Why is it, do you suppose, so much fun (despite the obvious immorality) to think about stealing a world renowned piece off the wall of a major metropolitan museum? Is it the romantic thoughts of getting away with it, walking past infrared detectors, and pressure sensors *ala* Indiana Jones with the sack of sand to remove the idol without triggering the security system? Is it the idea of snatching items with such fantastic prices, where the romance of possessing an item of such value is less intoxicating than selling it to a private collector for it to never be seen again? I suspect others share my daydreams as they watch theater or hear of a brazen daylight heist at museums around the world, or from private collections.

Though when reality sets in, the mind of the security professional kicks in. How could one do it, why would one do it, what should you do once it's done? The main issue a thief confronts when acquiring unique goods is how to process or fence them. They become very difficult to sell because they are one-of-a-kind, easy to identify, and could lead to the people involved with the theft.

The whole issue of museum security takes up an ironic twist when one considers the secretive British street artist "Banksy.[2] Banksy has made a name for himself by brazenly putting up interesting pieces of art in broad daylight (though many critics don't consider his work to be art) on building walls, rooftops, or even museums. I bring him up for a interesting take on what may become a trend in museum security. In March of 2005, Banksy snuck a piece of his called "Vandalized Oil Painting" into the Brooklyn Museum's Great Historical Painting Wing, plus 3 other pieces into major museums in New York. Within several days, 2 paintings had been torn down, but 2 stayed up much longer. In his

* Editor's Note: This viewpoint paper was not peer reviewed.

home country of the UK, a unauthorized piece he created and placed in the British Museum known as "Early Man Goes to Market" received different treatment when placed inside the walls. It was adopted into the permanent collection! I like his story because it's so counter-intuitive. Who would have thought that modern museum security might involve preventing people not just from stealing art, but from sneaking "unauthorized" art into museums? What is next, tampering with the archive records in order to make it look like the piece in question has always been there?

To learn more about museum security, I interviewed multiple experts in the field. It turns out that the glamorous lifestyle of Thomas Crown is not particularly relevant. In fact, usually nobody can point to a Mr. Big of the underworld coordinating thefts, though some organized crime families have been known to use stolen art as black market chips to trade. The common consensus among experts in the field of art theft is that, instead of most high-value pieces being stolen by outsiders with a blue print in hand and rappelling from a ceiling skylight (exciting as this Hollywood image is), in reality, 80 percent of art thefts involve insiders or accomplices that execute the crime over a period of time while working or volunteering in the museum.[3] (This figure of 80% of thefts involving insiders is interesting, in that the general consensus is that in 80% of cargo thefts from trucks, the driver is involved in some manner.)

Indeed, according to FBI statistics, between 70 and 80 percent of all solved art theft cases involve insider participation of some kind, yet according to Tom Cremers of the Musuem Security Network, "[Having] been involved in risk assessments in over hundreds of museums over the past ten years, it is quite astonishing how rarely the risk of insider participation is discussed."

In regards to the insider threat, a museum is not much different from any corporation or other organization. There are directors, employees, interns, and cleaning staff (very often outsourced), security guards (again outsourced, typically with very high turnover rates[4]). Unlike corporations, most museums also have volunteer staff, docents, and authorized visiting scholars. All these people can potentially take advantage of their position, or to be exploited by a clever attacker on the outside or inside using social engineering.

After discussing where museum security is headed with several people involved in the field, the consensus seems to be that it is going to be completely digital at the behest of companies designing

new security products. By this I mean that nearly every security sensor and alarm is being designed so that it is compatible or adaptable to Cat 5/6 Ethernet cable. Museum security sensors are usually connected to the network infrastructure, which then gets tied back to a server monitoring the security sensors. This approach should make us feel uneasy. This is security that rides on top of technology that time and time again has proven to be highly vulnerable, and very often implemented by closed source vendors who do not release details of their code or hardware because of it being proprietary. Being proprietary is not consistent with having good security. Closed systems cannot be easily vetted by security experts for serious vulnerabilities, including stupid and easy-to-exploit ones.

What happens when the museum's security camera in the parking lot is connected via a network cable, and an attacker decides to plug his laptop onto that cable: all of a sudden he gets access to the whole network. What are the security consequences? Could this person take control of the security systems? Could he gain access to the museum's donor list (sometimes with anonymous donors) or private art appraisal values for various reasons and possibly hold the data ransom? Or just publish the information online through a site called wikileaks.org to make it public? Could tampering with computer data send a traveling exhibit to the wrong location? It seems likely that future attacks on museums may be cyber attacks, but it does not appear that museum security is being sufficiently proactive to the threat.

Another interesting question is the quality of the security provided for museum artifacts that are not currently on display, typically 85%-99% of a museum's total holdings. Are they being monitored as carefully as they should be?

Another crucial security issue for museums is that there is no international standard for reporting losses, and no public database for making the news media, art aficionados, and art dealers aware of thefts by listing missing or stolen pieces. The databases of museum thefts that do exist are disjointed and available only to a small number of museum or security professionals, who often have to pay a fee for access. If we have learned nothing from computer security and open source "Full Disclosure" policies it is that the risk of public embarrassment at being the victim of a security incident pales in comparison to doing the right thing to improve security. By publicizing what is missing or stolen, cooperative security can take place. Nothing of the sort occurs when security incidents are kept secret.

If you are interested in learning more about museum security, I have found these references to be helpful:

http://www.museum-security.org/saz.html

http://en.wikipedia.org/wiki/Fence_(criminal)

http://en.wikipedia.org/wiki/Elmyr_de_Hory

http://www.sourcesecurity.com/news/articles/co-3108-ga.3200.html

http://www.interpol.int/Public/WorkOfArt/Default.asp - Interpol Art Theft Database

http://www.fbi.gov/hq/cid/arttheft/nationalstolen.htm – FBI Art Theft Database

Confessions of a Master Jewel Thief, by Bill Mason with Lee Gruendfeld (Villard, 2005), ISBN 0-375-76071-7

http://www.artloss.com/ - Art Loss Register

http://www.asisonline.org/councils/documents/SuggestedPracticesforMuseumSecurity.pdf – Suggested Guidelines for Museum Security

http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/notable.html – Passage on Vladimir Levin on the first electronic bank heist

http://www.wikihow.com/Forge-Email

Acknowledgements

I am grateful to Roger Johnston for assisting with this paper.

References

1. "The Thomas Crown Affair (1968 film), http://en.wikipedia.org/wiki/The_Thomas_Crown_Affair_(1968_film); "The Thomas Crown Affair (1999 film), http://en.wikipedia.org/wiki/The_Thomas_Crown_Affair_(1999_film)

2. "Banksy: On Art of the State", http://www.artofthestate.co.uk/banksy/banksy.htm

3. Private communication from Tom Cremers of the Musuem Security Network mailing list.

4. EG Bitzer, "Strategies for Cutting Turnover", *Security* Management **50**(5**)**, 88-94 (2006), based on EG Bitzer and RG Johnston, "Turnkey Turnaround Solutions: Exploiting the Powerful Tools of I/O Psychology", Los Alamos National Laboratory Report LAUR-05-113 (2005).

Sticky Bomb Detection with Other Implications for Vehicle Security*

Roger G. Johnston, Jim Vetrone, and Jon S. Warner

Vulnerability Assessment Team
Argonne National Laboratory

Introduction

A "sticky bomb" is a type of improvised explosive device (IED) placed on a motor vehicle by (for example) a terrorist. The bomb is typically attached with adhesive ("duct") tape, or with magnets. This paper reports some preliminary results for a very rudimentary demonstration of two techniques for detecting the placement of a sticky bomb on a motor vehicle. There are other possible security applications for these techniques as well.

Method 1: Tire Pressure

The weight of a truck and its cargo load can theoretically be determined from measurements of the tire pressure.[1] We investigated whether small changes in a vehicle's weight—such as that caused by the addition of a sticky bomb—could be detected by monitoring the vehicle's tire pressure.

The pressure was measured using a Vernier 12-bit analog-to-digital converter to sample a MKS Baratron differential pressure transducer (model 223BD-1ABB, ~$600) with 1 Torr pressure range full scale. The effective differential pressure resolution was approximately 0.001 Torr. (For comparison, there are 760 Torr in a standard atmosphere, and 0.001 Torr ≈ 1/1000 of a mm of mercury ≈ 0.13 Pascal ≈ 19 millionths of a pound per square inch). Much more sensitive pressure transducers are available commercially.

Tire pressure measurements were made on a parked 2004 PT Cruiser automobile (because that is what we had available to experiment on). The engine was off during measurements.

---

* Editor's Note: This paper was not peer reviewed.

The Baratron pressure transducer remained external to the car and its tire. Figures 1 and 2 show the experimental setup. Tubing was used to attach one end of the Baratron to the tire's stem. A 'T' in the tubing allowed the other end of the Baratron to be connected to a shutoff valve. Initially, the valve was opened so that the pressure (provided by the tire) was equalized on each side of the Baratron. The shutoff valve was then closed. Next, weight was added or subtracted from the vehicle. Any change, positive or negative, in the differential pressure across the Baratron was measured with the Vernier analog-to-digital converter and recorded with a notebook computer as a function of time.

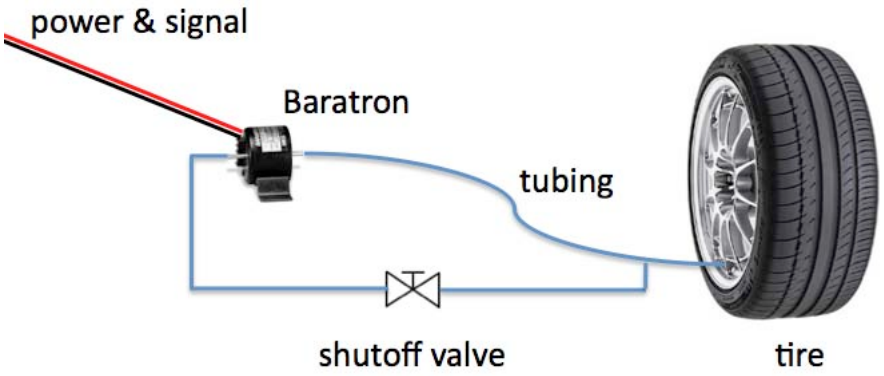


Figure 1 - Schematic of the experiment.

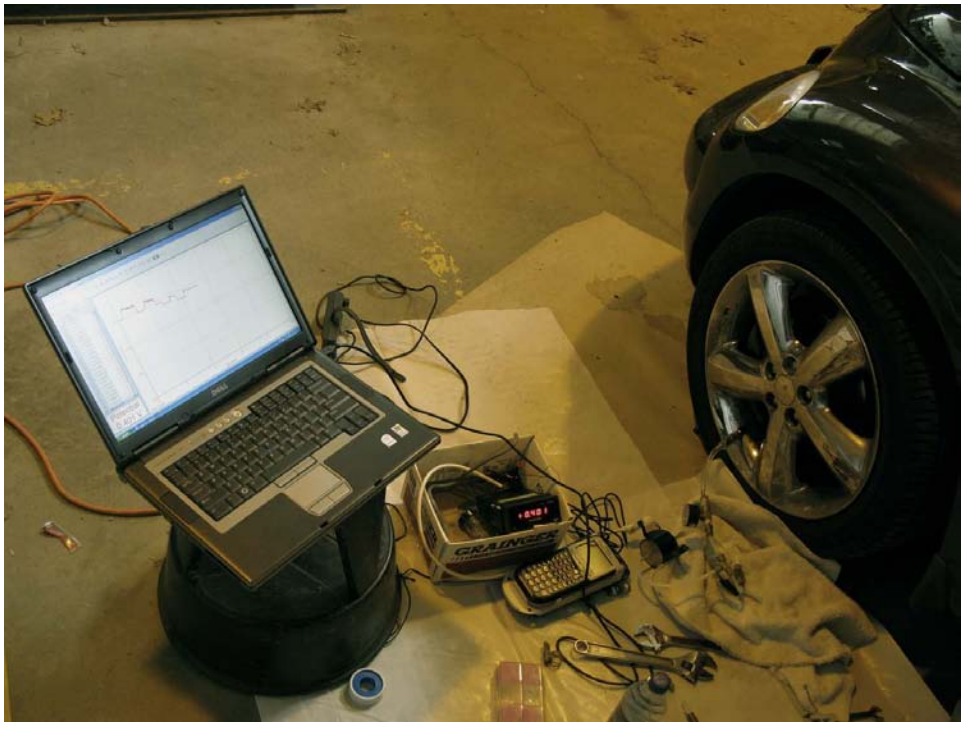


Figure 2 - The actual experiment.

Experimental results are shown in Figures 3-8. Figure 3 shows that the addition of a 10-pound weight to the car can be easily detected by the increase of air pressure in the front, driver's side tire.

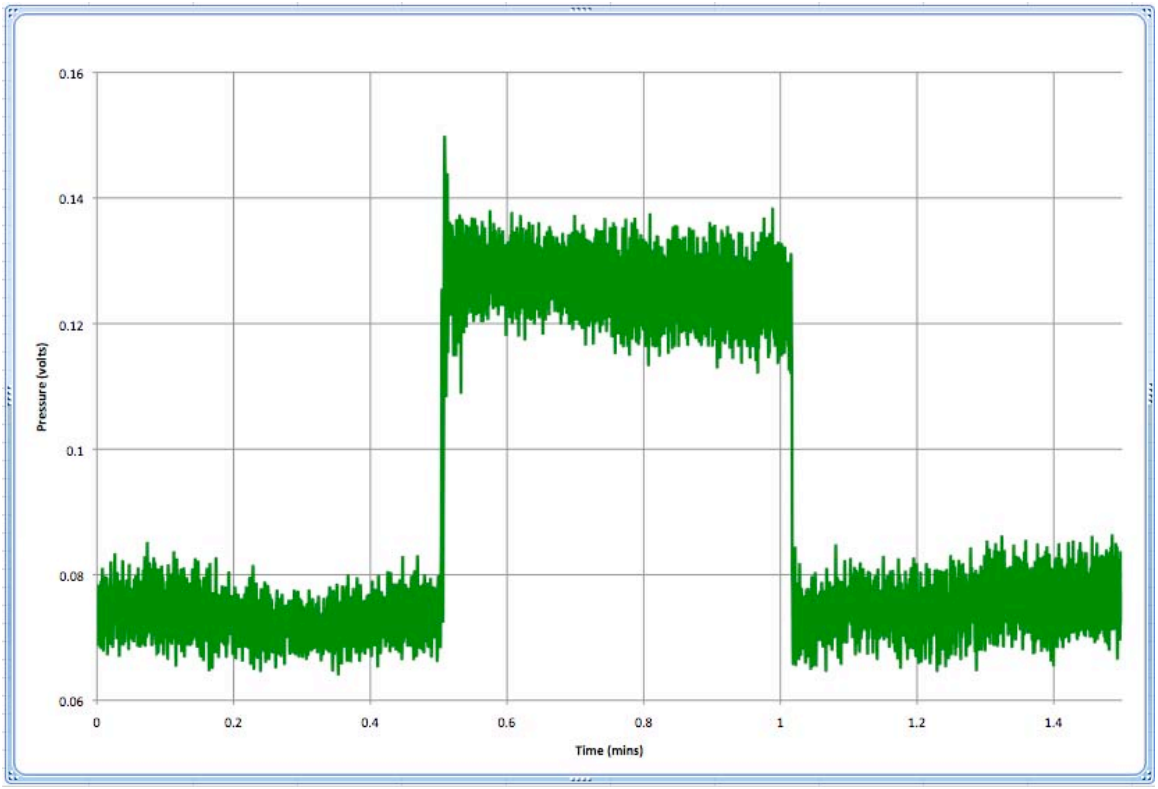


Figure 3 - 10 lb weight. Differential tire pressure as a function of time. While monitoring the pressure of the front, driver's side tire, a 10-pound weight was added to the driver's floor area at 0.5 minutes, then removed at 1 minute. (No driver was in the vehicle at the time.) A real sticky bomb would most likely be placed on the vehicle's exterior or the under carriage. The tire pressure increased when the weight was added, then returned to its original value when the weight was removed. A 0.010 volt change in the vertical axis corresponds approximately to a pressure change of 0.001 Torr.

Though we did not study the issue carefully, we believe the noise shown in figure 3 and subsequent graphs is a combination of electronic noise, analog-to-digital conversion noise, and background mechanical vibration/acoustical noise transmitted to the tire through the air and ground. Only the latter would cause true pressure oscillations in the tire. (The experiment was conducted in a relatively noisy environment about 2 km from a construction site.)

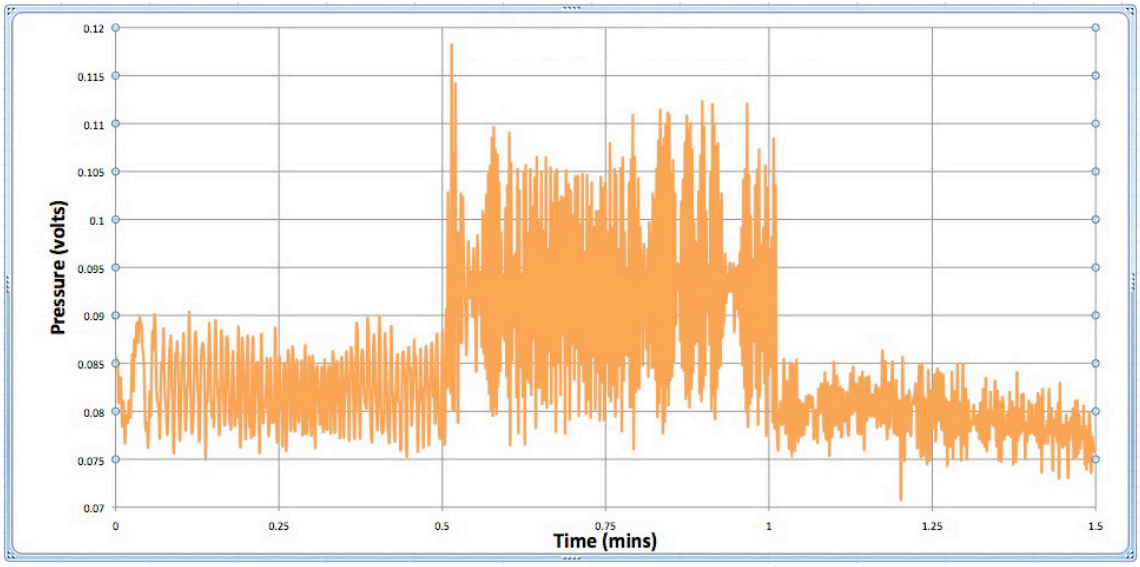


Figure 4 - Results for the same experiment in figure 3 except that the weight was 2 pounds, a value closer to the minimum effective mass of a sticky bomb used to attack a vehicle.

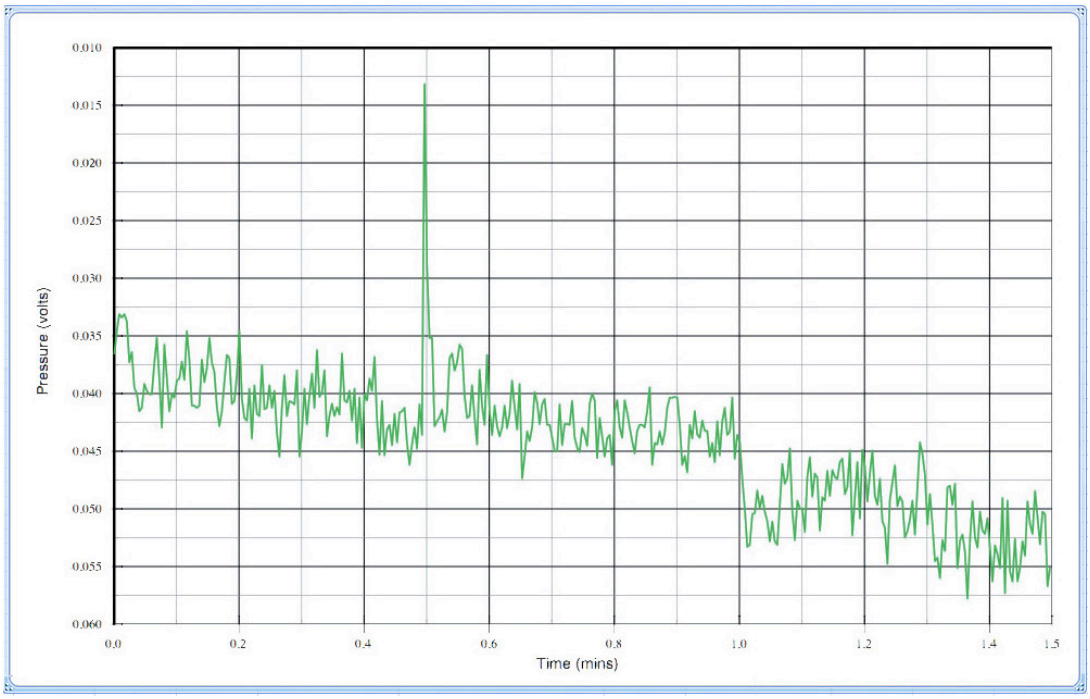


Figure 5 - The same experiment for 1 pound. The overall downward drift in the differential pressure may be due to some combination of a slow leak, temperature changes in the tire, and an incoming weather pressure front.

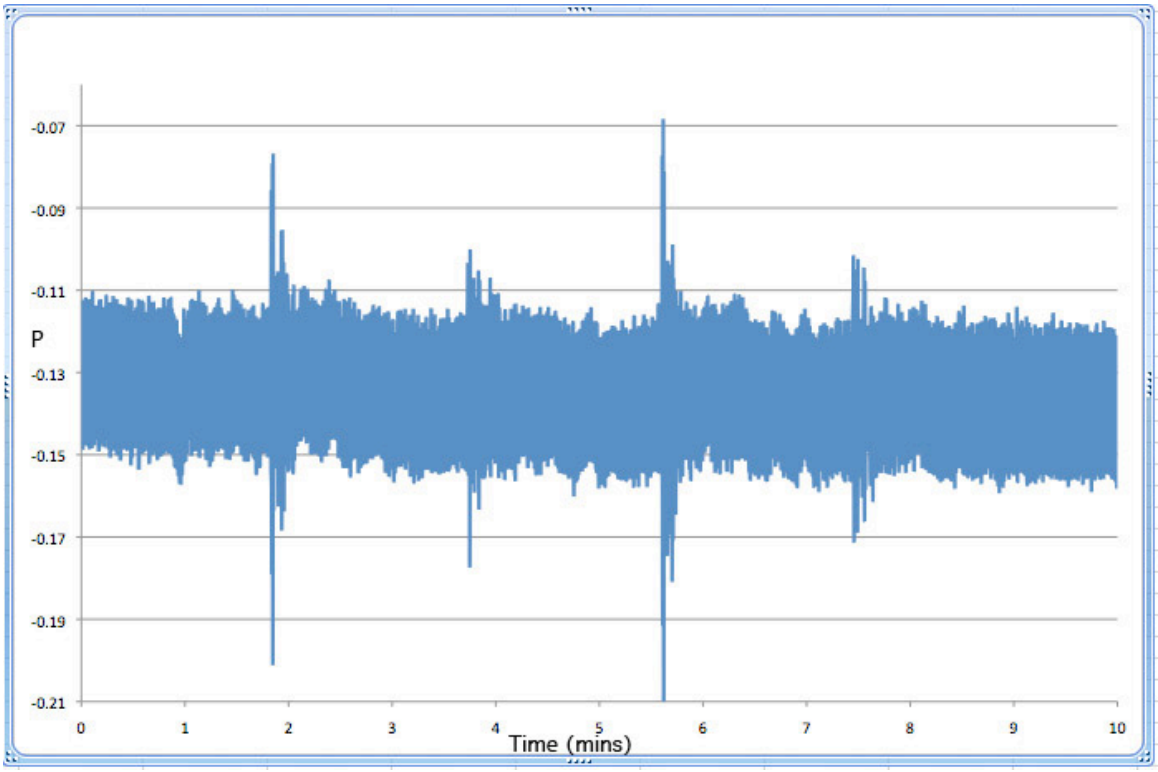


Figure 6 - The same experiment using a 4-ounce weight fairly gently placed on the driver's floor. The weight was added at approximately 2 minutes, removed at 4 minutes, replaced at 6 minutes, and removed at 8 minutes. While it is difficult to see the step functions caused by the extra weight amid the noise, pressure spikes clearly indicate when the weight has been added or removed. Wind or rain, however, might create similar spikes.

Discussion: Tire Pressure

Figures 3-6 indicate little difficulty in detecting the addition (or subtraction) of 1 or 2 pounds from the automobile. Figure 6 arguably suggests that as little as 4 ounces can be detected.

Improvements to this measurement technique should be possible by increasing the pressure sensitivity, reducing the high frequency noise in the pressure measurements, and moderating (or correcting for) the long-term drift. The latter, however, is not much of a problem since we are looking for only very short-term changes to the tire pressure.

Note that the change in tire pressure would be less for a vehicle that had more than 4 tires, such as a large truck.

Our results are for a parked vehicle. Making measurements on a moving vehicle would be more challenging, though perhaps a multi-axis accelerometer and measurement of the tire temperature could be used to correct (at least partially) for engine noise, road vibrations, and thermal changes. Wind and rain would no doubt also complicate the interpretation of the measurements. We suspect this technique would work at some level for a moving vehicle, but at a reduced sensitivity.

Placing the pressure transducer inside the tire—as is currently done with the much lower sensitivity tire pressure sensors used in modern cars to report low tire pressure—would probably be required for monitoring the tire pressure of a vehicle in motion.

There are other potential security applications for this technique beyond sticky bombs. Theft of a vehicle's contents, or smuggling unauthorized cargo onto a vehicle could be easily detected. It might be possible to detect the placement of a surreptitious Global Positioning System (GPS) or other illicit tracking device on a vehicle if the surreptitious package included a long-life battery, radio frequency transponder, and antenna.

Figure 7 and 8 also suggest that monitoring the tire pressure could be used to detect vehicle intrusion. Figure 7 shows what happens to the tire pressure when a person entered the back seat of a vehicle, then left 30 seconds later. Figure 8 demonstrates the intriguing idea that we can determine which door of the vehicle is opened by monitoring the pressure on just one tire.

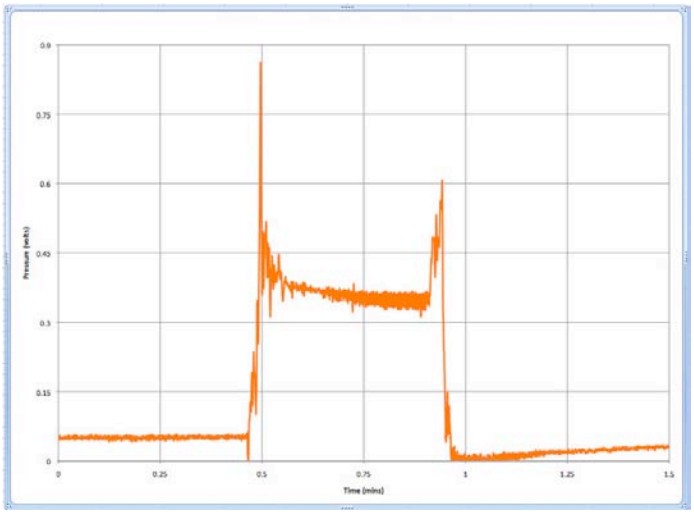


Figure 7 - Detecting a masher entering a parked car. A 145-pound man entered the back seat of the car at 0.5 minutes, then left at approximately 1 minute. The back door remained open throughout. Being in the back seat, his weight was distributed unevenly between the 4 tires, only one of which was being monitored for pressure changes (the front, driver's side tire).

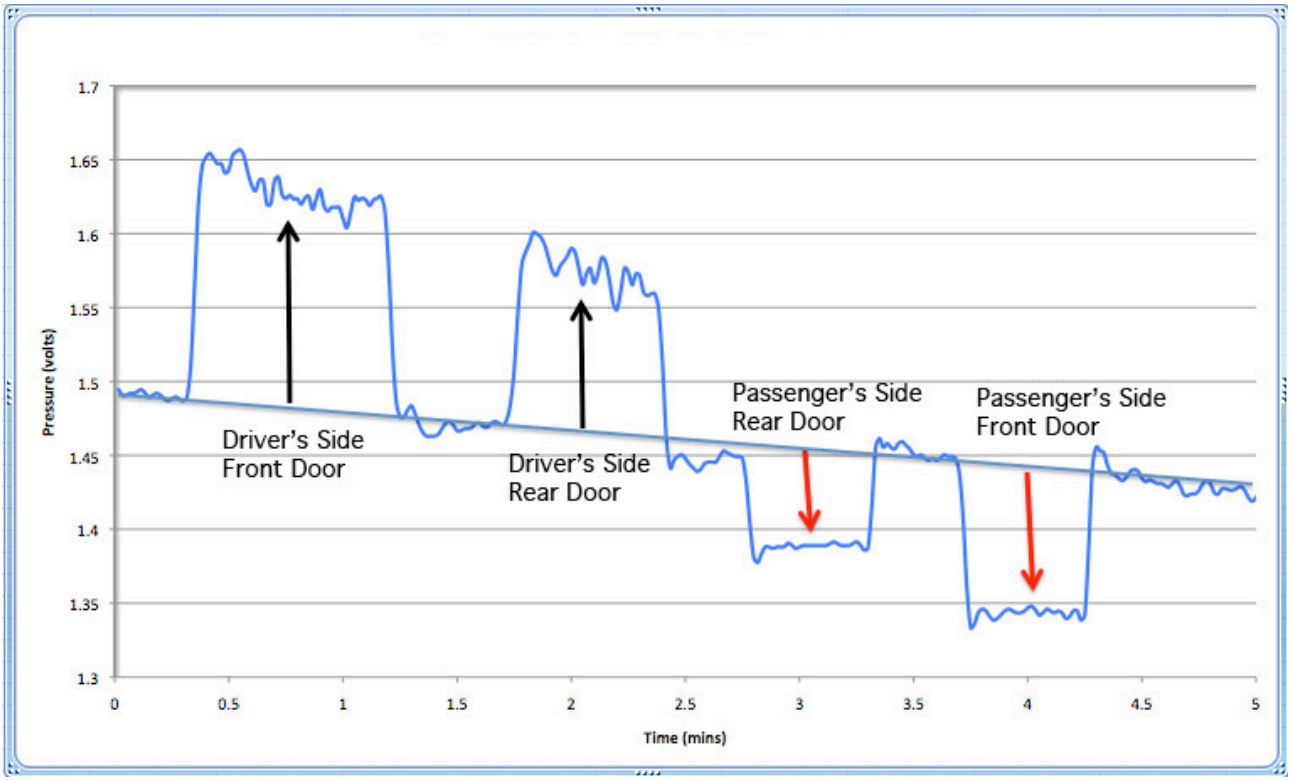


Figure 8 - By monitoring the pressure of the front, driver's side tire, it is possible to determine which of 4 doors are opened. Each of the 4 doors was opened for approximately 1 minute, then closed. The pressure *increases* when the driver's door was opened, because of the lever arm of the door. The pressure increase is less for the rear door on the driver's side because that door is not immediately located over the tire being monitored. Opening either passenger-side door causes the tire pressure to *decrease* because the car leans in the opposite direction due to the weight of the open door hanging out to the side of the vehicle. As in figure 5, the largely irrelevant overall downward drift in the differential pressure may be due to some combination of a slow leak, temperature changes in the tire, and an incoming weather pressure front.

Method 2: Magnetic Measurements

Instead of detecting the sudden weight change to a vehicle when a sticky bomb is attached, we investigated whether sticky bombs (or surreptitious tracking devices) that were attached with magnets could be detected by looking for sudden changes in magnetic field around the vehicle. While DC magnetic field lines can be significantly deviated directionally by ferrous metals, attenuation of the overall magnetic field strength is typically minor.

For this experiment, we compared the performance of two commercial magnetometers. The first was a handheld Walker Scientific Triaxial FluxGate Magnetometer with a 1 nanoTesla (nT) resolution along each of 3 axes. The other

magnetometer was a PNI V2XE 2-axis Digital Compass with an effective resolution of about 50 nT along each axis.[3] (By comparison, the amplitude of the Earth's magnetic field at Argonne, IL is approximately 45,000 nT at the surface.)

Readings from the Walker magnetometer were recorded manually from the liquid crystal display. PNI readings were recorded with an Apple notebook computer via a custom USB interface. Both magnetometers measure DC magnetic fields, but are not much affected by AC fields above a few hertz in frequency.

The cost of the Walker and PNI magnetometers in (retail) quantities of 1 are ~$2.5K and $75, respectively.

The automobile used for this experiment was a 1993 Subaru Legacy station wagon. We place the magnetometers on the driver's seat of the vehicle (see figure 9), even though this is not the optimal location for detecting sticky bombs applied to a car's exterior. A rare earth magnet was then placed at different locations near or on the vehicle's exterior, with the magnet's North pole oriented perpendicular to the vehicle's surface. (These locations, shown in figure 10, are not necessarily realistic for sticky bomb locations.)

The magnet we used for this demonstration was a 1" long, 1" diameter cylindrical rare earth magnet (~$1). Its holding strength was 60 pounds for a clean, optimal magnetic metal surface, but substantially less when attached to an automobile. A magnet this strong might be overkill for a sticky bomb weighing a few pounds applied to a parked vehicle, but could be appropriate if the terrorist wanted to be sure the sticky bomb remained on the vehicle as it traveled along bumpy roads. Results for weaker magnets would scale linearly with the strength of the magnet.

The results of our magnetic measurements are shown in table 1, and schematically in figure 10. The values shown are the amplitude of the change in magnetic field strength when the magnet was brought near or placed on the automobile. For the Walker magnetometer (being 3-axis), the change in amplitude was the quadrature, i.e., the square root of the squares of the changes in the magnetic field strength in the x, y, and z (vertical) directions. The 2-axis PNI magnetometer measured magnetic field strength only in the horizontal plane. Thus, the values shown for the PNI magnetometer in table 1 and figure 10 are the square root of the squares of the changes in magnetic field strength in the x and y directions only.

The results for the Walker magnetometer shown in table 1 and figure 10 are within about 20% of what we predicted theoretically for the magnet used in this demonstration by ignoring the presence of the metal in the car.

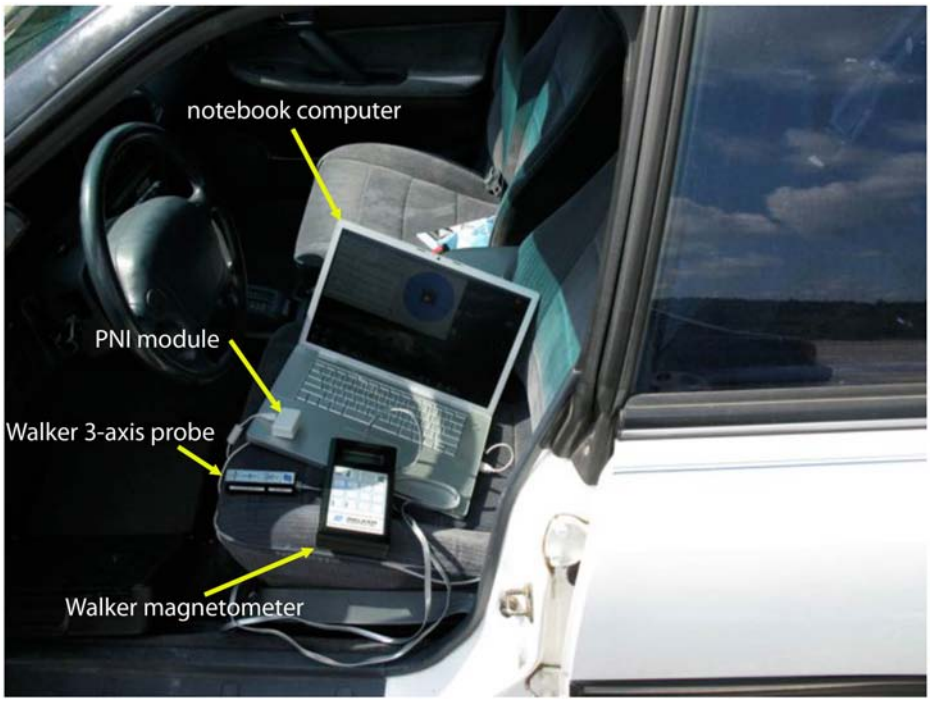


Figure 9 - The driver's seat location of the magnetometers and notebook computer used to record the PNI readings. The PNI module, which we built, consisted of the PNI magnetometer plus a USB interface circuit.

Table 1 - Experimental results for changes in the amplitude of the 3-dimensional (Walker) and 2-dimensional (PNI) magnetic field strength when the rare earth magnet was placed on or near the car. The approximate uncertainties for these measurements are ±3 nT for the Walker magnetometer and ±70 nT for the PNI magnetometer.

location	Walker (ΔnT)	PNI (ΔnT)
7 feet in front of the front license plate	361	0
left (passenger's side) front fender	289	251
front license plate	391	52
right (driver's side) front fender	3364	1577
rear, driver's side door	2472	909
right (driver's side) rear fender	1785	272
rear license plate	449	146
left (passenger's side) rear fender	283	251

Figure 10 - The results from table 1. The orange dots indicate the location of the magnet. The Walker readings are shown in green for each location, with the PNI readings in black parenthesis.

Differences in the readings for the Walker magnetometer vs. the PNI magnetometer are probably due to the PNI not measuring in the z (vertical) direction, the fact that the magnet and the PNI magnetometer were not in the same plane, the fact that the surface of the automobile where the magnet was attached was not always vertical, and our rather crude calibration and nulling (zeroing) techniques for the PNI magnetometer. (The Walker magnetometer displays results directly in nT and has a sophisticated built-in nulling algorithm. The PNI magnetometer gives results only in arbitrary units and lacks an amplitude nulling algorithm. This is because it is fundamentally a compass, interested only in magnetic angles.)

Discussion: Magnetic Measurements

Table 1 and figure 10 show that both the Walker and PNI magnetometers could easily detect placement of the magnet used in this demonstration. Based on these results, the Walker magnetometer should have little problem detecting a

magnet one-tenth as strong. With the PNI magnetometer, however, a weaker magnet might necessitate the use of 2 to 4 PNI magnetometers, placed in different locations around the vehicle so they would be closer to the magnet. A larger vehicle might also require multiple PNI magnetometers.

Conclusion

This was a rather crude demonstration. We were greatly constrained by the small amount of time and funding available for exploring either the tire pressure or magnetometer techniques. The preliminary results, however, would seem to suggest these two concepts warrant further investigation, either for sticky bomb detection or for other vehicle security applications.

References

1. See, for example, US Patent 6449582, "Vehicle Weight and Cargo Load Determination Using Tire Pressure", September 10, 2002

2. MKS, Type 223 Pressure Transducer, http://www.mksinst.com/docs/UR/223.pdf

3. PNI V2Xe 2-Axis Compass Module, http://www.tri-m.com/products/precisionnav/files/specs/v2xe_spec.pdf