What Alligators and Russian Dopers Can Teach Us About Security

Roger G. Johnston, Ph.D., CPP
Right Brain Sekurity (http://rbsekurity.com)

Two recent disturbing security incidents highlight the frequent lack of vulnerability assessments (VAs), or even a mindset that allows for the contemplation of security vulnerabilities. This almost always leads to serious security failures.

The first incident involves allegations of Russian tampering with urine samples used for testing athletes for banned performance-enhancing drugs. There are credible reports of extensive state-sponsored doping of Russian international athletes, hidden via tampering with urine testing samples. The cheating was reportedly implemented by tampering with so-called "tamper-proof" urine sample bottles. Don Catlin, the former head of the UCLA Olympic Analytical Laboratory has been quoted as saying, "I tried to break into those [urine sample] bottles years ago and couldn't do it. It's *shocking*."

In news reports, Catlin further recalls that when the manufacturer first showcased the urine sample bottles used for athlete drug testing to a roomful of doctors, "All of us were particularly pleased and excited by this bottle because it *looked* pretty bulletproof." The manufacturer is quoted as saying about the allegations of Russian spoofing of the "tamper-proof" sample bottles that, "We're all a bit speechless, to be honest...*No one can believe it*."

Shocked? No one can believe it? Really?!? The fact is that reliable tamper-detection is a largely unsolved problem. Low-tech attacks work quite well to spoof most (all?) tampering-indicating devices and containers. A simple attempt at finding the vulnerabilities would have demonstrated the sample bottles were not "tamper-proof".

The second recent, highly disturbing "security" incident that suggests the absence of effective vulnerability assessments was the horrific killing of a 2-year old child by an alligator at a Walt Disney resort in Orlando, Florida. Now alligators might be more conventionally considered a safety issue rather than a security issue, but security is fundamentally about trying to counter malicious actions by a nefarious adversary. Alligators would seem to fall into that category, in contrast to other forces of nature such as hurricanes, tornados, and earthquakes.

Risk Management must include not just understanding the threats, but also understanding the vulnerabilities. In the case of the Orlando incident, the alligator threat must certainly have been hard to overlook, even before the attack. According to the Associated Press, Florida has about 1 million alligators and officials receive 16,000 complaints about alligators each year. Last year, more than 7,500 nuisance alligators were relocated. Since 1973, 23 people have been killed by wild alligators.

The Walt Disney resort reportedly had no fences and no signs warning visitors about the alligators and how to behave safely around them. This is surely a serious vulnerability. Orlando is visited by large numbers of children and adults from all 50 states and many different countries where people may not be familiar with alligators and the risk they represent.

Hindsight is always 20-20 after a security incident, but it seems likely that even a rudimentary vulnerability assessment prior to the attack would have easily identified the lack of warning signs as a serious problem.

In my experience, there are a number of reasons why people and organizations may overlook vulnerabilities and effective vulnerability assessments (VAs). Sometimes, threats are confused with vulnerabilities. Often, various activities get confused with VAs. Examples include threat assessments, security surveys, compliance auditing, fault or event tree analysis, Design Basis Threat, the CARVER Method, reliability testing, **penetration testing**, **performance testing**, and "**Red Teaming**". While these things can certainly be useful, they are not comprehensive vulnerability assessments, and they are usually not highly effective at finding the security vulnerabilities that are likely to be exploited by adversaries. Another problem may be that, for many organizations, threats are much easier and more comfortable to contemplate and deal with than vulnerabilities.

So what exactly is a good vulnerability assessment? It is a holistic, imaginative exercise in thinking like the bad guys. It involves discovering and perhaps demonstrating vulnerabilities (weaknesses in the security) that might be exploited by the bad guys. It often also includes suggesting possible countermeasures to mitigate the vulnerabilities.

An effective VA is not constrained by wishful thinking, conflicts of interest, departmental politics, bureaucracy, lack of imagination, "shooting the messenger", cognitive dissonance, phony constraints, excessive formalism, or artificial boundaries between disciplines or hardware/software modules. It does not ignore the insider threat, focus only on frontal force-on-force attacks by outsiders, or consider only previous attacks. It does not let the

good guys or the current security posture and hardware define the vulnerabilities or the possible attacks. A good VA recognizes that all security is local, and that compliance and security are not the same thing.

The purpose of a VA is to improve your security. A VA is not a test you "pass". Indeed, you cannot test your security against attacks you haven't envisioned. Moreover, a VA is not a way of reassuring yourself everything is fine. It is not a software program you run, a model you "crank", an audit you conduct, or an exercise in finding "gaps" (though these things may be helpful).

The ideal outcome of a VA is not finding zero vulnerabilities—indicating the VA is worthless—but rather findings lots of vulnerabilities, which are always present in large numbers. This is true even after a good VA is completed and new countermeasures have been implemented.

A VA must be undertaken by creative, resourceful, independent people who genuinely want to find problems and suggest solutions. There must be no risk of retaliation for what they find and recommend. An effective VA is not undertaken by safety experts using safety models (though having the vulnerability assessors confer with safety people is a good idea). It is not a one-time thing, but rather an exercise that is done early, iteratively, and often.

Want to avoid shock, awe, and disbelief when it comes to your security? Then do legitimate vulnerability assessments!

[This essay was extracted from the *Journal of Physical Security* **9**(1), pp. 26-48 (2016).]