Viewpoint Paper

# Being Vulnerable to the Threat of Confusing Threats with Vulnerabilities*

Roger G. Johnston
Vulnerability Assessment Team
Nuclear Engineering Division
Argonne National Laboratory

The following ideas are common, but I think quite wrong and thus myths:

(1) A Threat without a mitigation is a Vulnerability.

(2) A Threat Assessment (TA) is a Vulnerability Assessment (VA).

(3) Threats are more important to understand than Vulnerabilities.

(4) Many of the most common tools used for "Vulnerability Assessments" (whether true VAs or actually TAs) are good at finding Vulnerabilities.

First some definitions. Most security professionals would probably more or less agree with the following definitions:

**Threat:** Who might attack against what assets, using what resources, with what goal in mind, when/where/why, and with what probability. There might also be included some general aspect of the nature of the attack (e.g., car bombing, theft of equipment, etc.), but not details about the attack or the security measures that must be defeated and the Vulnerabilities to be exploited.

**Threat Assessment (TA):** Attempting to predict the Threats. This may involve using intelligence data and information on past security incidents (at this building, facility, or infrastructure or ones like it.) To have proactive (not just reactive) security, however, a valid TA requires anticipating Threats that have not yet materialized.

*Editor's Note: This paper was not peer-reviewed. This work was performed under the auspices of the United States Department of Energy (DOE) under contract DE-AC02-06CH11357. The views expressed here are those of the author and should not necessarily be ascribed to Argonne National Laboratory or DOE. Jon Warner provided useful suggestions.

**Vulnerability:** a specific weakness in security (or a lack of security measures) that typically could be exploited by multiple adversaries having a range of motivations and interest in a lot of different assets.

**Vulnerability Assessment (VA):** Attempting to discover (and perhaps demonstrate) security Vulnerabilities that could be exploited by an adversary. A good VA also often suggests practical countermeasures or improvements in security to eliminate or mitigate the Vulnerability, or to aid in resiliency and recovery after an attack.

**Risk Management:** Attempting to minimize (security) hazards by deciding intelligently how to deploy, modify, or re-assign security resources. Involves the following inputs: TA results, VA results, assets to be protected, consequences of successful attacks, and the resources (time, funding, personnel) available to provide security.

**Attack:** An attempt by an adversary to cause harm to valuable assets, usually by trying to exploit one or more Vulnerabilities. The harm may include theft, sabotage, destruction, espionage, tampering, or adulteration.

Some examples of Threats and Vulnerabilities.

Threat: Adversaries might install malware in the computers in our Personnel Department so they can steal social security numbers for purposes of identity theft.
Vulnerability: The computers in the Personnel Department do not have up to date virus definitions for their anti-malware software.

Threat: Thieves could break into our facility and steal our equipment.
Vulnerability: The lock we are using on the building doors is easy to pick or bump.

Threat: Nefarious insiders might release confidential information to adversaries.
Vulnerability: Employees don't currently have a good understanding of what information is sensitive/confidential and what is not, so they can't do a good job of protecting it.

Threat: Disgruntled employees could sabotage our facility.
Vulnerability: The organization lacks effective Insider Threat countermeasures like background checks and disgruntlement mitigation (fair treatment of

employees, legitimate complaint resolution processes, employee assistance programs, no tolerance for bully bosses, etc.)

Threat: Extremists want to discredit our organization.
Vulnerability: It is easy for them to dump hazardous chemicals on our property or pour them down our drains, and then fraudulently report us to the authorities as polluters.

With these definitions, it should be clear that myth #1 above ("a Threat without a mitigation is a Vulnerability") makes no sense because (a) a Threat is not a Vulnerability, (b) security is a continuum and 100% elimination of a Vulnerability is rarely possible, (c) adversaries may not automatically recognize a Vulnerability so mitigating it may be irrelevant for that specific Threat, and (d) Vulnerabilities don't define Threats, i.e., terrorists don't exist because buildings and people can be blown up.

The commonly held myth #2 (TAs are VAs) is untrue because Threats are not the same thing as Vulnerabilities. Both TAs and VAs are needed, however, for good Risk Management, and they both depend on each other to some extent. Adversaries typically seek to exploit Vulnerabilities. Indeed, if there were no Vulnerabilities, the adversaries won't succeed. And if there were no Threats, any existing security Vulnerabilities would be irrelevant.

Note that Vulnerabilities don't map one-to-one onto Threats. Many different kinds of adversaries with very different agendas can potentially exploit the same Vulnerability for very different reasons. Thus a lock that is easy to pick permits attacks involving theft, espionage, or vandalism. Computers lacking up to date virus checkers can be exploited for lots of different nefarious purposes. Of course, Threats don't map one-to-one onto Vulnerabilities, either. An adversary can potentially pick and choose which Vulnerability or Vulnerabilities to exploit for any given goal.

In thinking about Myth #3 (Threats are more important than Vulnerabilities) we need to consider that a TA involves mostly speculating about people who are not in front of us, and who might not even exist, but who have complex motivations, goals, mindsets, and resources if they do exist. Vulnerabilities are more concrete and right in front of us (if we're clever and imaginative enough to see them). They are discovered by doing an analysis of actual infrastructure and its security—not speculating about people. Thus, getting Threats right is typically a lot harder than getting Vulnerabilities right. [Some people claim that

past security incidents can tell us all we need to know about Threats, but that is just being reactive, not proactive, and misses rare but very catastrophic attacks.]

I would go even further and argue that understanding Vulnerabilities is more powerful than understanding Threats—regardless of the relative difficulty of TAs vs. VAs. If you understand and take some reasonable effort to mitigate your security Vulnerabilities, you are probably in fairly good shape regardless of the Threats (which you are likely to get wrong anyway). On the other hand, if you understand the Threats but are ignorant of the Vulnerabilities, you are not likely to be very secure because the adversaries will have many different ways in.

Myth #4 (existing tools are effective at finding Vulnerabilities) is quite prevalent, especially for infrastructure security. This is perhaps because there are such a staggering number of Vulnerabilities in any large, complex system (especially compared to Threats) that dealing with the Vulnerabilities is daunting. Also, finding Vulnerabilities takes a lot of careful thinking, on the ground investigation, hands-on analysis, and imagination/creativity. Threat Assessments, in contrast, often (unfortunately) involve relatively easy and simple-minded use of check lists, security surveys, compliance audits, guidelines, software programs, boilerplates, compliance requirements, databases of past security incidents, and "cookie cutter" approaches. There is, of course, no reason why a TA can't or shouldn't involve profound, critical, original, and creative thinking about security issues, it's just that is so often does not.

I break down the so-called "Vulnerability Assessment" methods into 4 general categories:

1. Tools that can help find vulnerabilities but aren't typically very good at it because they do not encourage thinking creatively like the bad guys about actual, local vulnerabilities and/or they make invalid assumptions: Security Surveys, Compliance Audits, boilerplate Software Programs, Tree Analysis, "Red Team" exercises.

2. Tools that are good at finding Vulnerability Assessments: Adversarial Vulnerability Assessments (thinking about the security problem from the perspective of the bad guys, not the good guys and the existing security implementation), intrusion testing programs (for cyber security), critical security design reviews early in the design process for new security devices, systems, or programs.

3. Misnamed "Vulnerability Assessment" tools that are really techniques for helping to decide how to allocate security resources, i.e., more like overall Risk Management than VAs *per se*: CARVER Method, Delphi Method.

4. Tools that (despite the claims) are actually TA methods, not VA methods: Design Basis Threat, Compliance Audits, boilerplate Software Programs.

One litmus test to tell if somebody claiming to do a Vulnerability Assessment is really doing a Threat Assessment is if they have identified a relatively small number of "Threats/vulnerabilities" (which they typically put in a table with made up rankings or probabilities), and if mitigating them is a major undertaking. If they are really doing a VA, they will have identified and maybe demonstrated dozens or hundreds of very specific vulnerabilities, and many of the countermeasures for mitigating them will be cheap and relatively painless, e.g., install anti-virus software in the Personnel Department computers that automatically updates virus definitions.

Another sort of related problem commonly found in infrastructure security assessments is confusing features with vulnerabilities. Thus, a public road that travels close to the facility is often considered a Vulnerability. It is not, however; it is only an attribute. Only when coupled with an attack scenario (truck bomb, the road makes visual and electronic surveillance easier for espionage, assets can be thrown over the fence by insiders to the bad guy's parked truck, etc.) does a feature become a Vulnerability. The reason this is important is that different kinds of security countermeasures will typically be needed for different combinations of feature + attack. Without the context of attack scenarios, the only apparent countermeasure is to eliminate the feature; this may be expensive, impractical, and/or total overkill.

Finally, we should not get confused about the purpose of a TA or VA. Neither a Threat Assessment or a Vulnerability Assessment is something we test against, some kind of "certification", a standard, a metric for how good our security is, or a technique for finding out if our security mangers or frontline personnel are screwing up. The purpose of a VA is to improve security. The purpose of a TA is to help us decide (in conjunction with Risk Management) what and how much security we need. It doesn't make any sense to talk about "passing" a TA or VA. This certainly cannot mean all Threats have been recognized or neutralized, or that there are zero Vulnerabilities or even that all Vulnerabilities are known and mitigated. Such things are not possible, and not provably true even if they were possible.