Never miss important updates of this file: download the original pdf at http://www.ne.anl.gov/capabilities/vat/assess/

Philosophy on Vulnerability Assessments

Argonne Vulnerability Assessment Team
Roger G. Johnston, Ph.D., CPP
r o g e r j a ANL.GOV , 630-252-6168

1. There are a number of conventional tools for finding security vulnerabilities. These include security surveys, risk management, design basis threat, CARVER Method, Delphi Method, software vulnerability assessment tools, 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
- dominated by groupthink & bureaucrats
- plagued by “shoot the messenger” syndrome
- not validated by hands-on or real-world testing
- not done from the perspective of the adversaries
- obsessed with past security incidents, not future ones
- overly focused on technology, hardware, & physical assets
- overly binary in outlook (something is either secure or it is not)
- insistent on letting the good guys 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, 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. Moreover, they are not (for the most part) tools that an adversary even uses, and thus are not effective at mimicking 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.

ARGONNE NATIONAL LABORATORY, Nuclear Engineering Division, 9700 South Cass Ave., Argonne, IL 60439-4814

A U.S. Department of Energy laboratory managed by UChicago Argonne, LLC