

Talk for the 58th Annual ASIS Meeting
Philadelphia, PA, September 10-13, 2012



How to Think Like a Vulnerability Assessor

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

Vulnerability Assessment Team
Argonne National Laboratory

630-252-6168 rogerj@anl.gov



Vulnerability Assessment Team (VAT)



A multi-disciplinary team of physicists,
engineers, hackers, & social scientists.

The VAT has done detailed
vulnerability assessments on
over 1000 different security
devices, systems, & programs.

The greatest of faults, I should say,
is to be conscious of none.
-- Thomas Carlyle (1795-1881)

Sponsors

- DHS
- DoD
- DOS
- IAEA
- Euratom
- DOE/NNSA
- **private companies**
- intelligence agencies
- public interest organizations



Check us out on YouTube: keywords = argonne break into

Terminology

A tourist once stopped to admire a mule. He asked the mule's owner what the animal's name was. The farmer said, "I don't know, but we call him Bill."
-- Sen. Sam Erwin (1896-1985)

Threat: Who might attack, why, when, how, with what probability, and with what resources. (Includes information on goals and attack modes.)

Threat Assessment (TA): Attempting to identify threats.



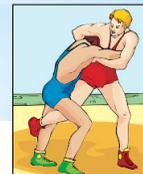
Terminology

Sometimes security implementations look fool proof. And by that I mean proof that fools exist.
-- Dan Philpott

Vulnerability: Flaw or weakness that could be exploited to cause undesirable consequences.

Vulnerability Assessment (VA): Discovering and demonstrating ways to defeat a security device, system, or program. Should include suggesting countermeasures and security improvements.

He that wrestles with us strengthens our skill. Our antagonist is our helper.
-- Edmund Burke (1729-1797)





Threat vs. Vulnerability



Threat: Adversaries might try to steal PII information (SSNs, credit card numbers, etc.) from our computer systems to commit crimes.

Vulnerability: We don't keep our anti-malware software up to date.

Threat: Adversaries could dump toxic chemicals on our property, then blame us to try to get us in trouble with environmental officials and the public.

Vulnerability: We don't have good access control or video monitoring of our grounds.



5

Why VAs Trump TAs (especially for catastrophic security incidents)

Threats	Vulnerabilities
reactive, focused on the past	proactive, focused on the future
speculative	right in front of you (if you're willing to see them)
hard to test	testable
not usually fixable	often easy to fix
often generic	specific to the ground level details
If you get the threats wrong but understand and (at least partially) fix the vulnerabilities, you may be ok.	If you get the vulnerabilities wrong (or ignore them), you are probably in trouble despite how well you understand the threats.



6

Security Risk Management - An Optimization Problem

Inputs:

- ✓ assets to protect*
- ✓ overall security goals*
- ✓ asset valuation/prioritization**
- ✓ consequences of successful attack(s)**
- ✓ threat assessment
- ✓ **vulnerability assessment***
- ✓ available resources & possible security measures**
- ✓ general security philosophy/strategy*
- ✓ various estimated/guessed probabilities



*often vague, incomplete, or missing
**often under-estimated

Outputs:

- What to protect and at what level
- How to deploy resources optimally



7

Purpose

The purpose of a VA is to improve security & minimize risk, not to:

- Pass a test
- **Test security**
- Generate metrics
- Justify the status quo
- **Praise or accuse anybody**
- Check against some standard
- Claim there are no vulnerabilities
- Engender warm & happy feelings
- Determine who gets salary increases
- **Rationalize the research & development**
- Apply a mindless, bureaucratic stamp of approval
- **Endorse a security product/program or Certify it as "good" or "ready to use"**



I cannot imagine any condition which would cause this ship to founder, nor conceive of any vital disaster happening to this vessel.
-- E.J. Smith, Captain of the Titanic



8

A VA is Not...

- auditing
- quality control
- reliability testing
- efficiency testing
- compliance testing
- acceptance testing
- ergonomics testing
- performance testing
- response time testing
- operational assessment
- environmental robustness testing



It only had one fault. It was kind of lousy.
-- James Thurber (1894-1961)

9

Techniques Often Confused with VAs

- feature analysis
- threat assessment
- Design Basis Threat
- CARVER Method (DoD)
- software assessment tools
- security survey (walking around with a checklist)
- security audit (are the rules known & being followed?)
- fault or event tree analysis (from safety engineering)
- Delphi Method (method for getting a decision from a panel of experts)



We made too many wrong mistakes.
-- Yogi Berra

10

Vulnerability Assessment (VA) Blunders

These assumptions are wrong:

- A vulnerability assessment should be done at the end.
- There are a small number of vulnerabilities.
- Most or all can be found & eliminated.
- A VA should ideally find zero vulnerabilities.
- Vulnerabilities are bad news.



Vulnerability Assessment (VA) Blunders

- Not using creative people with a hacker mentality who want to find problems and suggest solutions
- Conflicts of interest (economic & psychological)
- Shooting the messenger
- Sham rigor
- The fallacy of precision
- Fear of NORQ analysis

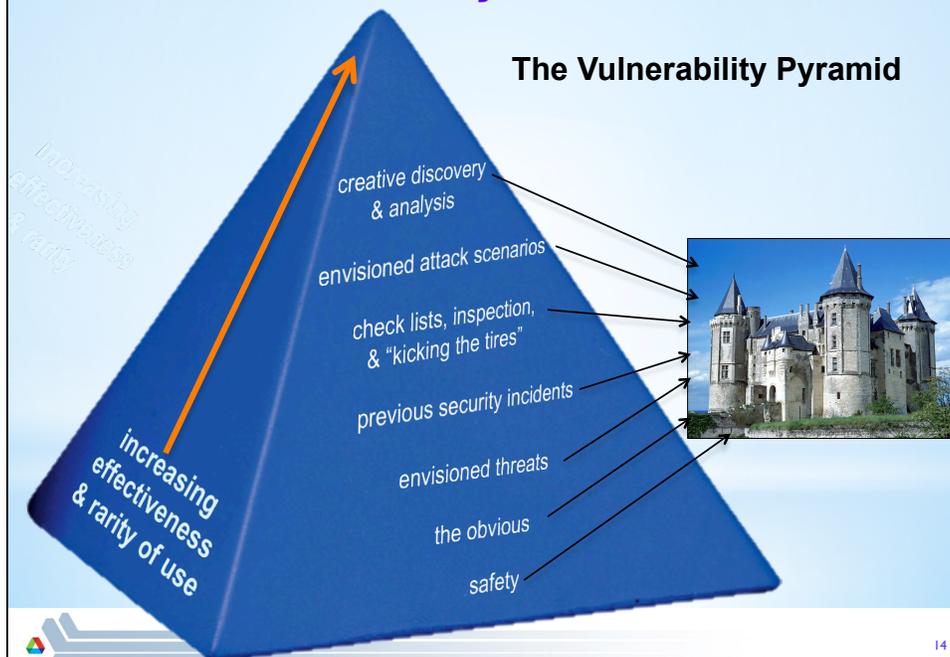
NORQ =
Non-Objective
Non-Reproducible
Non-Quantifiable

Vulnerability Assessment (VA) Blunders

- Focusing on high-tech attacks
- Letting attack methods define the vulnerabilities, not the other way around
- Arbitrarily constrained VAs (scope, time, effort, by modules or components)
- Limiting the VA to the lower part of the Vulnerability Pyramid



Where Vulnerability Ideas Come From



Safety & Security are 2 Relatively Unrelated Problems

Example: March 2012 Recall of 900,000
Safety 1st Push N' Snap Cabinet Locks

140 reports of babies/toddlers defeating
the locks, resulting in 3 poisonings



Security: All about nefarious adversaries.
Safety: No adversaries.



15

Working with Outside VAers

- Seek creative, hands-on assessors with a history of finding problems and suggesting solutions, and who are psychologically pre-disposed to doing so.
- At least be sure at the end you understand what subtle attacks & insider attacks look like!
- You don't have to mitigate all discovered vulnerabilities or accept all suggestions, but be sure you have good reasons (not just ego, arrogance, denial, laziness, or wishful thinking).



My definition of an expert in any field is a person who
knows enough about what's really going on to be scared.
-- P.J. Plauger

16

Assembling Your Own VA Team: Seek...

- ❑ hackers
- ❑ narcissists
- ❑ trouble makers
- ❑ hands-on types
- ❑ creative people
- ❑ loop-hole finders
- ❑ independent thinkers
- ❑ questioners of authority
- ❑ people curious about how things work



I don't want any yes-men around me. I want everyone to tell me the truth—even if it costs him his job.
-- Movie mogul Samuel Goldwyn (1879-1974)



17

Blunder: Thinking Engineers Understand Security

Engineers...

- ...work in solution space, not problem space
- ...make things work but aren't trained or mentally inclined to figure out how to make things break
- ...view Nature or economics as the adversary, not the bad guys
- ...think of technologies as failing randomly, not by deliberate, intelligent, malicious, opportunistic intent
- ...are not typically predisposed to think like bad guys
- ...focus on user friendliness—not making things difficult for the bad guys
- ...like to add lots of extra features that open up new attack vectors
- ...want products to be simple to maintain, repair, and diagnose—which usually makes them easy to attack



18

“White Box” vs. “Black Box” VA



White Box: Full details, specifications, and technical disclosures are given to the Vulnerability Assessors at the start.

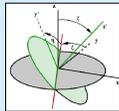


Black Box: The Vulnerability Assessors reverse engineering or discover all or most of the details on their own.

[Most time/cost effective & closest to reality.]
[Interesting & illuminating, but usually not realistic or time/cost effective.]



Adversarial Vulnerability Assessments



- Perform a mental coordinate transformation and pretend to be the bad guys (or VAers). (This is much harder than you might think.)

It is sometimes expedient to forget who we are. -- Publilius Syrus (~42 BC)



- Be much more creative than the adversaries. They need only stumble upon 1 vulnerability, the good guys have to worry about all of them.

It's really kinda cool to just be really creative and create something really cool. -- Britney Spears



Adversarial Vulnerability Assessments



- Don't let the good guys & the existing security infrastructure and tactics define the problem.

Evil will always triumph because good is dumb.
-- Rick Moranis, as Dark Helmet in *Spaceballs* (1987)



- Gleefully look for trouble, rather than seeking to reassure yourself that everything is fine.

On a laser printer cartridge: "Warning: Do not eat toner."

21

We need to be more like fault finders. They find problems because they want to find problems, and because they are skeptical:

- bad guys
- therapists
- movie critics
- computer hackers
- scientific peer reviewers
- mothers-in-law

I told my psychiatrist that everyone hates me. He said I was being ridiculous--everyone hasn't met me yet.
-- Rodney Dangerfield (1921-1997)



"Two mothers-in-law." -- Lord John Russell (1832-1900), on being asked what he would consider proper punishment for bigamy.

22

* AVA Steps

1. Fully understand the device, system, or program and how it is REALLY used. Talk to the low-level users and frontline personnel.
2. Play with it.
3. **Brainstorm--anything goes!**
(Effective brainstorming is the key!)
4. Play with it some more.



23

* AVA Steps

5. Edit & prioritize potential attacks.
6. Partially develop some attacks.
7. Determine feasibility of the attacks.
8. Devise countermeasures.
9. Perfect attacks.
10. Demonstrate attacks.
11. Rigorously test attacks.
12. Rigorously test countermeasures.



Delaying Judgment

Nothing can inhibit and stifle the creative process more—and on this there is unanimous agreement among all creative individuals and investigators of creativity—than critical judgment applied to the emerging idea at the beginning stages of the creative process. ... More ideas have been prematurely rejected by a stringent evaluative attitude than would be warranted by any inherent weakness or absurdity in them. The longer one can linger with the idea with judgment held in abeyance, the better the chances all its details and ramifications [can emerge].

-- Eugene Raudsepp, *Managing Creative Scientists and Engineers* (1963).

Keep the possibility phase completely separate from the practicality phase!

We all know your idea is crazy. The question is, is it crazy enough?
-- Niels Bohr (1885-1962)

25

The Creative VA Process

- Individuals must be given ownership of their original idea & should be personally recognized for their creativity.
- The ideal group environment:
 - + diverse
 - + high energy
 - + people tired
 - + urgent but not stressful
 - + free of authority figures
 - + humorous, joyful, & fun
 - + cohesive but not too cohesive
 - + competitive in a friendly & respectful way
 - + enthusiastic about individual differences & eccentricities
- Every idea, no matter how wacky or seemingly stupid, gets written down & treated as a gem, at least initially.



Sanity is a one trick pony--all you have is rational thought. But when you're good and loony, the sky's the limit!
-- The Tick

26

The Creative VA Process

Be skeptical! Pay close attention to explicit or unstated assumptions, and to security features that are widely praised or admired. These are often the source of serious vulnerabilities.

Concentrate on the 2nd and 3rd best attacks or countermeasures. You are likely overlooking something that would make them the best solutions.



If there is widespread agreement about the efficacy of an attack or countermeasure, re-examine. Something important was probably overlooked.

If everybody is thinking alike,
then nobody is thinking.
-- George S. Patton (1885-1945)



The Creative VA Process

Quantity breeds quality.

With all ideas: elaborate, expand, modify, subvert, exaggerate, & combine with other ideas. Pursue hunches & intuition.

The best ideas come late, and when you are not thinking about the problem.

Pursue what is interesting, controversial, contrarian, exciting, or silly.



Out of nowhere the idea will appear. It will come to you when you least expect it.
-- James Webb Young, *A Technique for Producing Ideas*

The best way to have a good idea is to have lots of ideas.
-- Linus Pauling (1901-1994)

The Creative VA Process

Develop and explore models, metaphors, & analogies.

Terminology constrains our thinking. Rename everything in your own (and/or silly) words, and think about them in light of the new terminology.

Consider different verbs for what the bad guys might want to accomplish: attack, steal, demolish, embarrass, tag, terminate, uncover, purify, whistleblow, poison, etc.



Ridicule existing security measures & strategies.

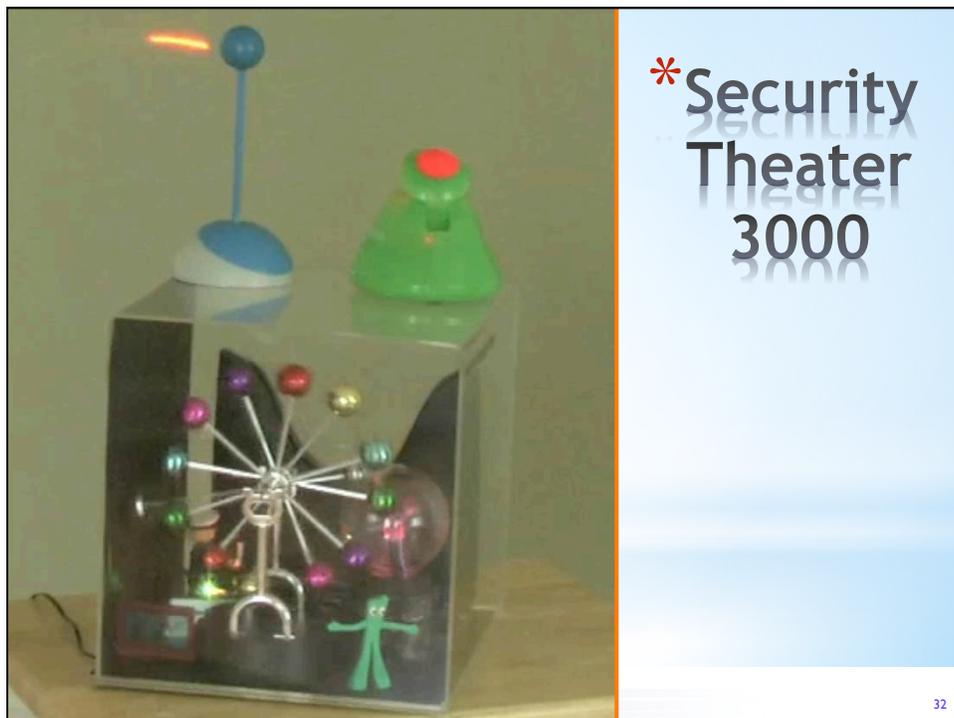
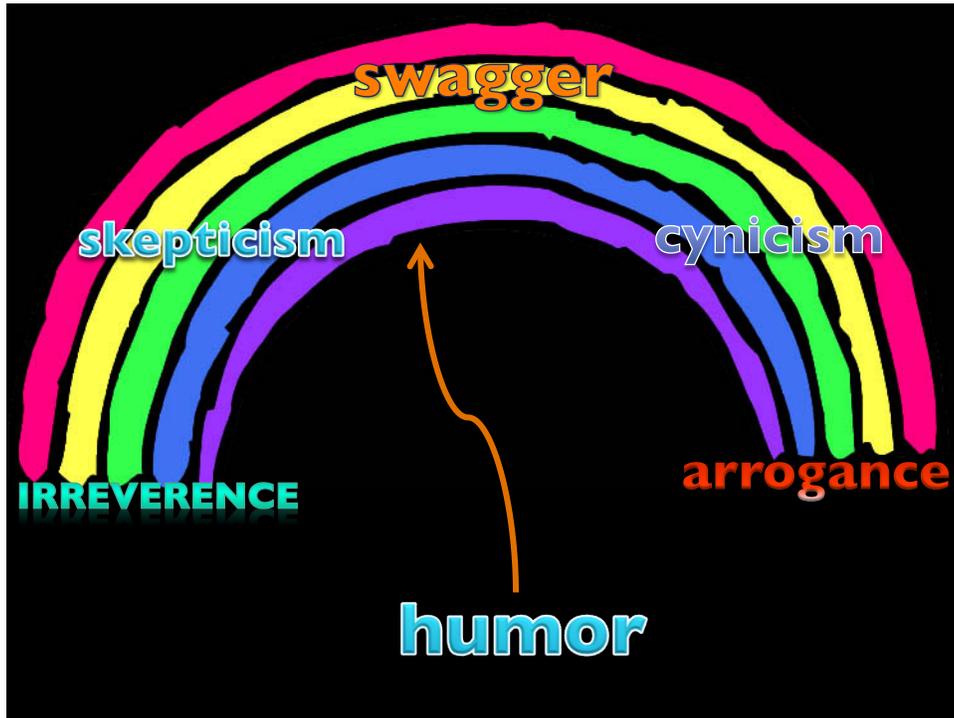
Avoid the fear of the NORQ!

*I never came upon any of my discoveries through the process of rational thinking.
-- Albert Einstein (1904-1973)*

29

Security Theater 3000
Video Goes Here

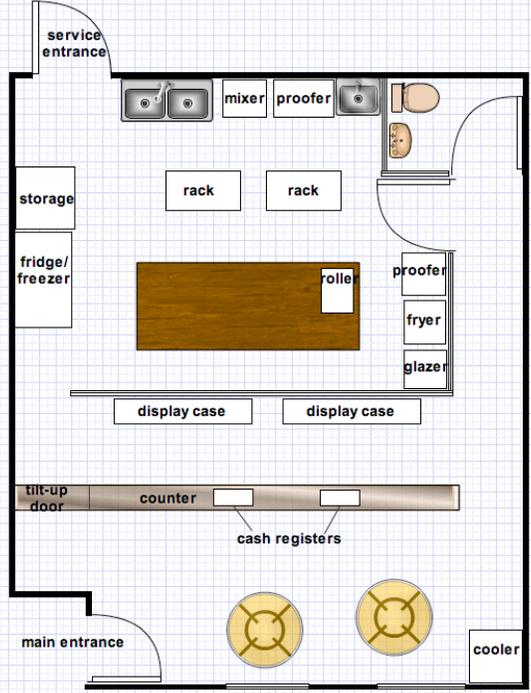




Slacker Donuts

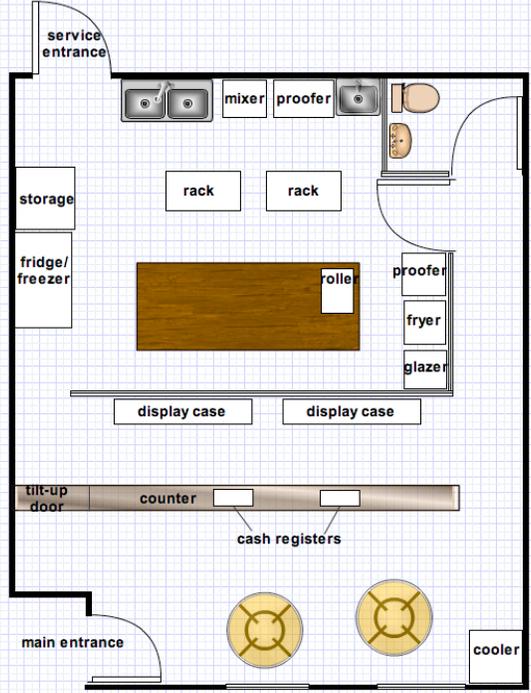


You want like...um...a donut, dude?™



Elements of the Slacker Donuts Security Program

- No checks
- There's a safe for cash but \$50 is immediately available to hand robbers
- Cash taken to local bank at 11 AM
- Not open 24/7 but bright illumination 24/7
- Periodic rounds by shared private security
- Good relations with local community, businesses, police, street people
- Shared slacker culture with employees and clientele
- Secret recipes known to only a few



In Summary

- * There are advantages to thinking like a Vulnerability Assessor when you think about your security.
- * Don't get confused about what a VA is or its role in overall Risk Management.
- * To go into "Vulnerability Assessor Mode", step outside yourself, be creative & irreverent+, and & try humor (which can be very mentally liberating).
- * You must want to find problems—or else find people who do.



35

*Special Thanks to:

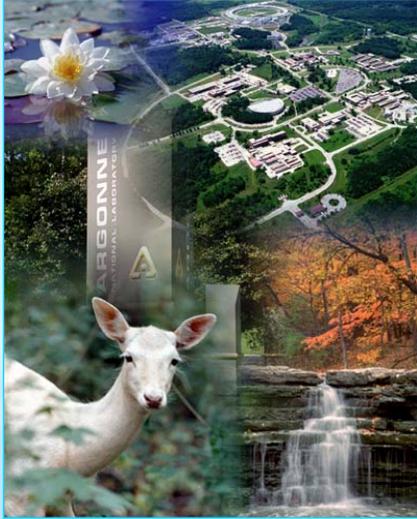
- * Christopher Folk (for helping to develop the Fear of NORQ model)
- * **Security Theater 3000 "Commercial"**
- * Mitch Farmer.....Investment Banker
- * Jim Regis.....Former Security Officer
- * Roy Lindley.....Arthritis Patient
- * Veronica Manfredi.....Wife (& Tech Support/Graphics)
- * Christopher Folk.....Husband
- * Marrison Faler.....Homemaker (& Tech Support)
- * Buddy the Dog.....As Himself
- * Greg Byslma.....Tech Support

I watch a lot of game shows and I've come to realize that the people with the answers come and go, but the man who asks the questions has a permanent job.
 -- Gracie Allen (1895? - 1964)



36

For More Information...



<http://www.youtube.com/watch?v=frBGGJqkz9E>

Additional information is available from:

rogerj@anl.gov
and

<http://www.ne.anl.gov/capabilities/vat>



If you look for truth, you may find comfort in the end; if you look for comfort you will get neither truth nor comfort...only soft soap and wishful thinking to begin, and in the end, despair.
-- C.S. Lewis (1898-1963)