Invited Talk for the National Security Institute's IMPACT06 Security Conference, Falls Church, VA, April 3-5, 2006

LAUR-06-1737

How to Conduct an Adversarial Vulnerability Assessment

Roger G. Johnston, Ph.D., CPP
Vulnerability Assessment Team
Los Alamos National Laboratory
505-667-7414 rogerj@lanl.gov
http://pearl1.lanl.gov/seals

Los Alamos NATIONAL LABORATORY

VAT

LANL Vulnerability Assessment Team

VAT

Physical Security
- consulting
- cargo security
- tamper detection
- training & curricula
- nuclear safeguards
- vulnerability assessments
- novel security approaches
- new tags & seals (patents)
- unique vuln. assessment lab

The VAT has done detailed vulnerability assessments on hundreds of different security devices, systems, & programs

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

critical review

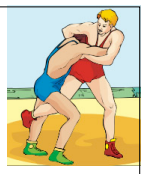
Fault Finders: They find problems because they want to find problems!

- bad guys
- hackers
- movie critics
- peer reviewers
- mothers-in-law

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

definition

VA vs AVA



vulnerability assessment (VA):
discovering and demonstrating ways to defeat a security device, system, or program. Should include suggesting counter-measures and security improvements.

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

adversarial vulnerability assessment (AVA):
doing a more effective VA from first principles by truly wanting to find security problems, by thinking like the bad guys, and by letting them (not the good guys) define the security issues.

b e n e f i t s

Other Reasons for Doing an AVA

- mental rehearsal
- fresh perspectives
- fun/relieves tedium
- increased alertness
- bluffing (don't underestimate)
- enhanced sense of professionalism
- educational/professional development for security staff
- can involve other members of the organization, thus increasing employees' security awareness
- can help justify additional resources for security

> Without deviation from the norm, progress is not possible.
> -- Frank Zappa (1940-1993)

n o t e a s y

Security is Difficult!

We need to recognize that security is difficult and there are no guarantees of success.

Especially because complacency, over-confidence, wishful thinking, and arrogance are not compatible with good security.

> If you're happy with your security, so are the bad guys.
> -- Anonymous

> Confidence is that feeling you sometimes have before you fully understand the situation.
> -- Anonymous

not easy

Why Security is Difficult

- The traditional performance measure for security is pathological: success is often defined as nothing happening.
- Cost/Benefit analysis is difficult.

- There are few meaningful standards, fundamental principles, metrics, models, or theories.
- Society & employees often do not like security.

> We spend all our time searching for security, and then we hate it when we get it.
> -- John Steinbeck (1902-1968)

not easy

Why Security is Difficult (con't)

- Security managers & personnel aren't always creative or proactive, but adversaries may be.
- Adversaries and their resources are usually unknown to security managers, yet the adversaries understand the security systems.
- Objectives are often remarkably vague.

> You've got to be very careful if you don't know where you are going, because you might not get there.
> -- Yogi Berra

n o t e a s y

Why Security is Difficult (con't)

- Effective security management is highly multi-disciplinary: engineering, computer science, psychology, sociology, management, economics, communication, & law.
- Adversaries can attack at one point, but security managers may need to protect extended assets.
- Adversaries need exploit only one or a small number of vulnerabilities, but security mangers must identify, prioritize, & manage many vulnerabilities, including unknown ones.

Evil is easy, and has infinite forms.
-- Blaise Pascal (1623-1662)

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

n o t e a s y

Why Security is Difficult (con't)

- Everything is a compromise & a tradeoff.
- Security functions are often tedious.
- Security personnel have trouble identifying security vulnerabilities because they don't want them to exist.

(It's hard to think like the bad guys if you devote your career to being a good guy.)

There is always more spirit in attack than in defense.
-- Titus Livius (59 BC)

phys sec

Why Security is Difficult (con't)

- Physical Security scarcely a "field" at all!
  - You can't (for the most part) get a degree in it.
  - Not widely attracting young people, females, the best & the brightest.
  - Few peer-review, scholarly journals or R&D conferences.
  - Lots of snake oil salesmen.
  - Shortage of models, fundamental principles, metrics, rigor, standards, guidelines, critical thinking, & creativity.
  - Overly macho and often dominated by bureaucrats, committees, groupthink, "old boys" networks, linear/concrete/wishful thinkers.

Is it ignorance or apathy? Hey, I don't know and I don't care. -- Jimmy Buffet

maxims

Security Maxims

1. **Infinity Maxim**: There are an unlimited number of vulnerabilities, most of which will never be discovered (by the good guys or bad guys).
2. **Arrogance Maxim**: The ease of defeating a security device, system, or program is inversely proportional to how confident/arrogant the designer, manufacturer, or user is about it.
3. **Ignorance-Is-Bliss Maxim**: The confidence that people have in security is inversely proportional to how much they know about it.

maxims

Security Maxims

4. **High-Tech Maxim**: The amount of careful, critical thinking that has gone into a given security device, system, or program is inversely proportional to the amount of high-technology used in it.

5. **Low-Tech Maxim**: Low-tech attacks are sufficient (even against high-tech security).

6. **Yipee Maxim**: There are effective, simple, & low-cost countermeasures to most vulnerabilities.

7. **Arg Maxim**: But your organization will be reluctant to implement them.

tools

Major Tools for Improving Security

- Security Survey (SS)
- Risk Management (RM)
- Design Basis Threat (DBT)
- Adversarial Vulnerability Assessment (AVA)

"Who are you and how did you get in here?"
'I'm a locksmith and I'm a locksmith.'
-- Leslie Nielsen as Lt. Frank Drebin, *Police Squad*

t
o
o
l
s

SSs, RM, DBT, & AVAs

- Not really the same thing because they produce different results.
- The task of identifying Threats & Vulnerabilities, done as part of RM or DBT, is typically not really an AVA.
- SSs, RM, DBT were major breakthroughs & are still useful… But they are not enough!

If they expect us to expect the unexpected, doesn't the unexpected become the expected?
-- Anonymous

S
S

Security Survey

- Basically a management walk around.
- Walk the spaces, looking for security problems.
- A checklist is often used.

We made too many wrong mistakes.
-- Yogi Berra

S
S

Limitations of Security Surveys

- Binary
- Close-ended
- Often unimaginative
- Not focused on adversaries
- Overly focused on the check list
- Does not encourage new countermeasures
- Expectation that problems will leap out at you

It's better to be looked over than overlooked.
-- Mae West, *Belle of the Nineties*, 1934

R
M

Risk Management

- Similar to Risk Management Techniques in other fields.
- Identify Assets, Threats & Vulnerabilities, Adversaries, Consequences, Safeguards & Countermeasures.
- Assign relative priorities and probabilities. (Generate lots of tables.)
- Field your resources appropriately.

We are never prepared for what we expect.
-- James Michener (1907-1997)

DBT

Design Basis Threat

- "Design Basis Threat" is similar to Risk Management.
- DBT means "design your security to deal with the current real-world threats, adversaries, & their resources".
- In practice, DBT tends to focus more on hardware and infrastructure than Risk Management does.

A hypothetical paradox: what would happen in a battle between an Enterprise security team, who always get killed soon after appearing, and a squad of Imperial Stormtroopers, who can't hit the broad side of a planet? -- Tom Galloway

RM & DBT

Limitations of RM & DBT

- There is rarely any guidance on how to determine the Threats & Vulnerabilities other than looking at past security incidents. But that is being reactive, not proactive. Not good enough post-9/11, in a rapidly changing world, or for dealing with rare catastrophic events.
- Too focused on physical assets instead of protecting people, morale, intellectual property, customers' interests, & external reputation.
- Still binary & close-ended

I skate to where the puck is going to be, not where it has been.
-- Wayne Gretzky

RM & DBT

More Limitations of RM & DBT

- Often done unimaginatively
- Typically dominated by groupthink & bureaucrats
- Not done from the perspective of the adversaries
- The attack probabilities are usually a fantasy
- Suffer from phony rigor, overconfidence in tables, and the "fallacy of precision"

3.14159265359

> There's no sense in being precise when you don't even know what you're talking about.
> -- John von Neumann (1903-1957)

RM & DBT

More Limitations of RM & DBT

- Tendency to let the good guys and existing security measures define the adversaries & attack modes
- Often used to justify the status quo--typically does not encourage new countermeasures
- Ignores simple/cheap countermeasures when the attack probabilities are judged (rightly or wrongly) to be low or zero

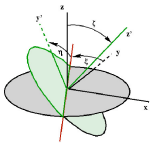
> It isn't that they can't see the solution.
> It is that they can't see the problem.
> -- G.K. Chesterton, *The Scandal of Father Brown* (1935)

A
V
A

Adversarial Vulnerability Assessment

- Perform a mental coordinate transformation and pretend to be the bad guys. (This is a lot harder to do than one might think.)

- Gleefully look for trouble, rather than seeking to reassure yourself that everything is fine.
- Unlike other techniques, don't let the good guys define the problem or its parameters.



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

c
o
m
p
a
r
e

Example: Open Window

security survey: issue orders to close & lock window!

risk management: ignore if not envisioned as part of a specific threat or attack from a likely adversary; otherwise, design procedure to close & lock window.

AVA: Oh boy, an open window! What mischief can this lead to?

You can observe a lot by just watching.
-- Yogi Berra

more info

Recommended References: Conventional Security Surveys & Risk Management

- WR Floyd, *Security Surveys* (1995).
- JF Broder, *Risk Analysis and the Security Survey* (1999).
- CA Roper, *Risk management for Security Professionals* (1999).
- ML Garcia, *The Design and Evaluation of Physical Protection Systems* (2001).

more info

Recommended References:
Social Engineering, Fakery, Wishful Thinking, & Deception

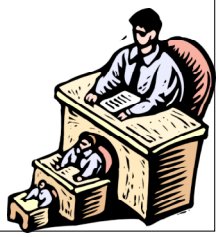
- K Hogan, *The Psychology of Persuasion* (1996).
- D Goleman, *Vital Lies Simple Truths: The Psychology of Self Deception* (1996).
- DL Smith, *Why We Lie: The Evolutionary Roots of Deception and the Unconscious Mind* (2004).
- KD Mitnick, WL Simon, & S Wozniak, *The Art of Deception: Controlling the Human Element of Security* (2002).
- T Hoving, *False Impressions* (1997).

more info

Recommended References:

For Dealing with the Government or a Large Organization

- D Dauten, *The Laughing Warriors: How to Enjoy Killing the Status Quo* (2003).
- RJ Sternberg (Editor), *Why Smart People Can Be So Stupid* (2002).
- RL Ackoff and S Rovin, *Beating the System: Using Creativity to Outsmart Bureaucracies* (2005).
- JQ Wilson, *Bureaucracy* (2000).



I hope you believe you understand what you think I said, but I'm not sure you realize that what you've heard is not what I meant.
-- Richard Nixon (1913-1994)

AVA steps

AVA Steps

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

Harry Solomon: Here's a job that I can do: "Police are seeking third gunman." Tomorrow, I'm gonna march over to the police station and show them that I'm the man they're looking for.
-- *Third Rock from the Sun*

AVA steps

AVA Steps

5. Edit & prioritize potential attacks.
6. Partially develop some attacks.
7. Determine feasibility of the attacks.
8. Devise countermeasures.

In theory there is no difference between theory and practice. In practice there is.
-- Yogi Berra

AVA steps

AVA Steps

9. Perfect attacks.
10. Demonstrate attacks.
11. Rigorously test attacks.
12. Rigorously test countermeasures.

After the meek inherit the Earth, I think we should just kick their butts and take it from them.
-- Jim Rosenburg

B
S
i
n
g

Effective Brainstorming is the Key!

You must be more creative and imaginative than your adversaries!

They only need to stumble upon one vulnerability, but you have to worry about all of them!

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

i
m
a
g
i
n
a
t
i
o
n

The Need for Creativity

Due to the rapid changes in the complexity of both technology and organizations over the past two decades, historical data has become less significant. Risk measurement and the identification of consequences require a combination of experience, skills, imagination, and creativity. This emphasis on subjective measurements is borne out in practice...

-- David McNamee, *Business Risk Management*, (1998), p. 43

The future ain't what it used to be. -- Yogi Berra

It's a poor sort of memory that only works backwards.
-- Lewis Carroll (1832-1898), *Alice in Wonderland*

B
S
i
n
g

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)

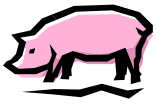
B
S
i
n
g

Realities of Creativity

Individuals are creative, not groups…

but the right group dynamics can energize, egg-on, & fertilize individuals…

and a group is usually necessary to fully explore attacks & countermeasures.



Could Hamlet have been written by committee, or the Mona Lisa painted by a club? Could the New Testament have been composed as a conference report? Creative ideas don't spring from groups. They spring from individuals.

-- Alfred Whitney Griswold (1885-1959)

B
S
i
n
g

Realities of Brainstorming

- Individuals must be given ownership of their original idea & should be personally recognized for their creativity.

- The group environment needs to be:
  + diverse
  + high-energy
  + urgent but not stressful
  + humorous, joyful, & fun
  + cohesive but not too cohesive
  + competitive in a friendly & respectful way
  + enthusiastic about individual differences & eccentricities

> There is evidence that brainstorming sometimes works better with nominal groups--pooled results from individual brainstormers--than with actual ones.
> -- Raymond S. Nickerson

- Every idea, no matter how wacky or stupid, gets written down & treated as a gem.

B
S
i
n
g

Realities of Brainstorming

Authority figures should not be involved, or at least should not act like authority figures.

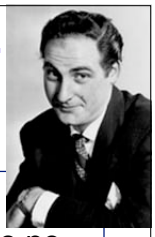
> A new idea is delicate. It can be killed by a sneer or a yawn; it can be stabbed to death by a joke or worried to death by a frown on the right person's brow.
> -- Charles Brower

A good model: comedy writing.

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

B
S
i
n
g

Brainstorming - Sid Caesar



When you came into the Writer's Room, you checked your ego at the door. In the room I was no big shot. There were no big shots. The big shot of the moment was the person who came up with the most recent funny situation, line, or bit. He or she could strut around while the other writers were seething and creatively scrambling for their next moment in the sun.

-- Sid Caesar and Eddy Friedfeld, *Caesar's Hours: My Life in Comedy, with Love and Laughter* (2003), p 123.

To stimulate creativity, one must develop the childlike inclination for play and the childlike desire for recognition.
-- Albert Einstein (1879-1955)

B
S
i
n
g

Brainstorming - Sid Caesar (con't)

"The energy in the Writer's Room was like a cyclotron--someone would come up with an idea and it would stimulate another idea and we would build on it…There was a healthy competition, like a bunch of pups in a big litter.

-- Sid Caesar and Eddy Friedfeld, *Caesar's Hours: My Life in Comedy, with Love and Laughter* (2003), pp 121-122.

You're only given a little spark of madness. You mustn't lose it.
-- Robin Williams

t
i
p
s

Security Brainstorming Tips

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)

t
i
p
s

Security Brainstorming Tips

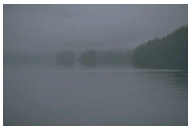
> The best way to have a good
> idea is to have lots of ideas.
> -- Linus Pauling (1901-1994)

Quantity breeds quality.

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

Keep a written record of ideas. Flip charts?

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



> 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*

t
i
p
s

Security Brainstorming Tips

Think about which rules could be broken to provide better security, or to execute better attacks.

Think backwards: How can we make security completely ineffective? How can our attacks fail miserably? How do we as the bad guys escape from the facility after completing our attack?

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

Solve the problem that isn't here yet.

> Now that the world is getting over the initial shock, and the war against terrorism has begun, what now for bridal retailers?
> -- Actual editorial in the trade magazine *Bridal Buyer*

t
i
p
s

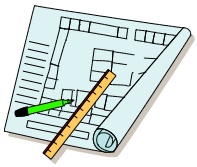
Security Brainstorming Tips

Mentally remove some security devices, measures, or personnel. Then consider the implications.

What if Albert Einstein, Chris Rock, or Frankenstein were in charge of security? What would they do differently?

What if Godzilla, your car mechanic, or the Boston Philharmonic Orchestra were the bad guys? How would they attack?

Draw lots of diagrams.



> If people don't want to come to the ballpark, how are you going to stop them? -- Yogi Berra

t
i
p
s

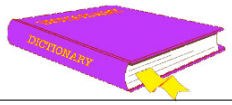
Security Brainstorming Tips

Develop and explore models, metaphors, & analogies.

"Ich bin ein Berliner." [I am a jelly donut.] -- John F. Kennedy (1917-1963)

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.



The problem with the French, is that they don't have a word for 'entrepreneur'. -- George W. Bush

t
i
p
s

Security Brainstorming Tips

Picture attacks from the ceiling and the floor. How would attacks work if everything was underwater, or if gravity stopped working?

Ridicule existing security measures & strategies.

Explore extremes: best & worst case scenarios for both the good guys and the bad guys.

Be wary of fault tree analysis! Most security failures are NOT the result of a sequence of stochastic failures at different points in the system.

There's a fine line between fishing and just standing on the shore like an idiot.
-- Steven Wright

tips

Security Brainstorming Tips

How will the bad guys *feel* during the attack? Try to imagine their satisfaction if they succeed.

How would the bad guys attack if they had infinite resources? Almost no resources?

What would the security look like if it had infinite resources? Almost no resources?

What questions would a 10-year old ask?
What questions would your mother-in-law ask?

I think the inventor of the piñata may have had some unresolved donkey issues.
-- Dan Johnson

people

AVA Personnel

Ideally, involve outsiders!

Vulnerabilities are often obvious to outsiders:

To see what is in front of one's nose needs a constant struggle.
-- George Orwell (1903-1950)

people

AVA Personnel (con't)

Also involve smart, hands-on, creative people inside your organization, including those who are not associated with security.

Seek: nonconformists, wise guys, trouble makers smart alecks, schemers, organizational critics, loophole finders, questioners of tradition and authority, outside-the-box thinkers, artists, hackers, tinkerers, problem solvers, & techno-nerds.

> Some people see things that are and ask, Why?
> Some people dream of things that never were and ask, Why not?
> Some people have to go to work and don't have time for all that.
> -- George Carlin

more info

Recommended References: Brainstorming & Creativity

- RJ Sternberg, *Handbook of Creativity* (1999).
- AG Robinson & S Stern, *Corporate Creativity: How Innovation and Improvement Actually Happen* (1998).
- A Hargadon, "Brainstorming Groups in Context", *Administrative Science Quarterly*, 12/1/1996.
- DC West, "The Definition and Measurement of Creativity", *Journal of Advertising Research*, 6/1/2004.
- R van Oech, *A Whack on the Side of the Head: How You Can be More Creative* (1998).
- II Mitroff, "Think Like a Sociopath, Act Like a Saint", *Journal of Business Strategy* 25, pp 42-53, October 2004.
- M Michalko, *Cracking Creativity: The Secrets of Creative Genius* (2001).

General Attributes of Effective AVAs

good AVA

1. No conflicts of interest or wishful thinking.

2. No "Shoot the Messenger" Syndrome. No retaliation or punishment against assessors, security personnel, or managers when vulnerabilities are found.

3. Use of independent, imaginative assessors who are psychologically predisposed to finding problems and suggesting solutions, and who (ideally) have a history of doing so.

> To show resentment at a reproach is to acknowledge that one may have deserved it.
> -- Tacitus (55-117 AD)

General Attributes of Effective AVAs

good AVA

4. No binary view of security.
5. Rejection of a finding of zero vulnerabilities.

6. Rejection of the idea of "passing" the VA, or of VAs as "certification".
7. Discovering vulnerabilities is viewed as good (not bad) news.

> When we were children, we used to think that when we were grown-up we would no longer be vulnerable. But to grow up is to accept vulnerability... To be alive is to be vulnerable.
> -- Madeleine L'Engle

General Attributes of Effective AVAs

good AVA

8. Done early, iteratively, and periodically.
9. Done holistically, not by component, sub-system, function, or layer. (Attacks often occur at interfaces.)
10. No unrealistic time or budget constraints on the AVA, or on what attacks or adversaries can be considered.
11. Done in context.

> He that will not apply new remedies must expect new evils; for time is the greatest innovator.
> -- Francis Bacon (1561-1626)

General Attributes of Effective AVAs

good AVA

12. No underestimation of the cleverness, knowledge, skills, dedication, or resources of adversaries.
13. The good guys don't get to define the problem, the bad guys do.
14. Simple, low-tech attacks are examined first.

> Do not touch anything unnecessarily. Beware of pretty girls in dance halls and parks who may be spies, as well as bicycles, revolvers, uniforms, arms, dead horses, and men lying on roads--they are not there accidentally.
> -- Soviet infantry manual from the 1930's

good AVA

General Attributes of Effective AVAs

15. Rohrbach's Maxim must be considered: No security system will ever be used properly (the way it was designed) all the time.

> Inanimate objects can be classified scientifically into three major categories; those that don't work, those that break down, and those that get lost.
> -- Russell Baker

16. Shannon's (Kerckhoffs') Maxim must be considered: The adversaries know and understand the security systems, strategies, and hardware being used.

> Everything secret degenerates … nothing is safe that does not show how it can bear discussion and publicity.
> -- attributed to Lord Acton (1834-1902)

good AVA

General Attributes of Effective AVAs

17. The following attacks are all considered:

- terrorism
- sabotage
- espionage
- fault analysis
- false alarming
- wait & pounce
- poke the system
- backdoor attacks
- counterfeiting
- impersonation
- social engineering
- tampering with security training
- insiders, outsiders, insiders + outsiders

> When choosing between two evils, I always pick the one I never tried before.
> -- Mae West (1893-1980)

Warning: Counterfeiting Attacks

Often overlooked: an adversary often needs only to mimic the superficial appearance and maybe the apparent performance of a security device. This is much easier than true counterfeiting.

Everything is what is is, and not another thing.
-- Bishop Joseph Butler (1692-1752)

Nothing is like it seems, but everything is exactly like it is.
-- Yogi Berra

Warning: Backdoor Attacks

Most security devices and systems can be compromised by having a few seconds of access to them at the factory, during shipment, or prior to installation.

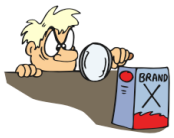
Every wall is a door.
-- Ralph Waldo Emerson (1803-1882)

We often get in quicker by the back door than by the front.
-- Napoleon Bonaparte (1769-1821)

Warning: Access Control & Biometric Devices

Question: Is that really your access control or biometric device, or is it a counterfeit or a tampered version? (…perhaps one that lets anybody in, with occasional random false rejects to look realistic.)

- Maintain a secure chain of custody, right from the factory!
- Check at random, unpredictable times with random, unpredictable people that the unauthorized are rejected!



I was the kid next door's imaginary friend.
-- Emo Philips

Warning: Access Control & Biometric Devices

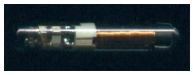
Guards supervising access control (AC) systems can usually be distracted.

They often don't know what an attack on the AC system looks like, so they are unlikely to detect one.

Security Guard: "Don't make me take off my sunglasses!" -- *Bringing Out the Dead* (1999)

Other Warnings

- RFIDs and contact memory buttons are cheap & easy to lift or counterfeit.



- Data encryption/authentication only provides security if the sending and receiving hardware is physically secure--which it almost never is.

- It's remarkably easy to spoof--not just jam--civilian GPS GPS receivers. (Almost nobody gets to use the more secure military GPS signals.) There are simple countermeasures, but these haven't been implemented.

Warning: GPS Vulnerabilities

- GPS cargo tracking is not secure.

- Many national networks (computer, utility, financial, & telecommunications) get their critical time synchronization signals from GPS. They are somewhat prepared for jamming, but not for spoofing, which is easy and could cause them to crash.

> You mean *now*?
> -- Yogi Berra when asked for the time of day

Warning: Biometrics

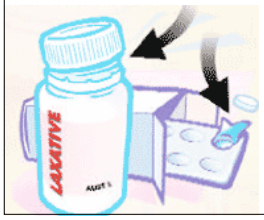
- Current Biometric Access Control Devices are easy to spoof by:
  - "counterfeiting" the biometric (easy)
    or
  - attacking the hardware (very easy)

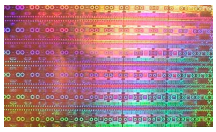
- Beware of bogus biometric performance specs:

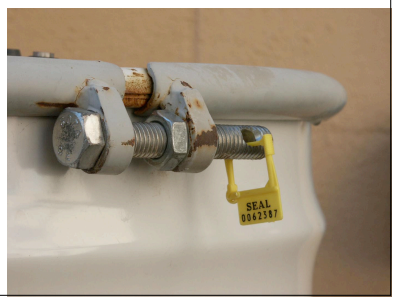
  For example, if N = the number of bits in the biometric signature, then 2^{-N} is **NOT**:
  - the probability of two people having the same signature
  - the Type 2 (false accept) error rate

Warning: Tags & Seals

- Tamper-Indicating Seals are easy to spoof. (Including high-tech electronic seals.)
- Consumer Tamper-Evident Packaging is easy for anyone to spoof.
- Anti-Counterfeiting Tags are easy to spoof.







Warning: Polygraphs

National Academy of Sciences $860,000 study:
"The Polygraph and Lie Detection" (October 2002)
http://www.nap.edu/books/0309084369/html/

Some Conclusions:

"Polygraph test accuracy may be degraded by countermeasures…"

"…overconfidence in the polygraph—a belief in its accuracy that goes beyond what is justified by the evidence—…presents a danger to national security…"

"Its accuracy in distinguishing actual or potential security violators from innocent test takers is insufficient to justify reliance on its use in employee security screening…"

good AVA

General Attributes of Effective AVAs

18. Keep in mind: A security device, system, or strategy will tend to be most vulnerable near the end of its life.

19. Don't forget about the physical security of computers, peripherals, and computer media!

> It does little good to have great computer security if wiring closets are easily accessible or individuals can readily walk into an office and sit down at a computer and gain access to systems and applications. Even though the skill level required to hack systems and write viruses is becoming widespread, the skill required to wield an ax, hammer, or fire hose and do thousands of dollars in damage is even more widely held. -- Michael Erbschloe, *Physical Security for IT* (2005)

Attributes of Effective AVAs (con't)

g o o d A V A

20. Avoid common fallacies, such as:

- All the threats & vulnerabilities will be discovered.
- When we are done, they will all be neutralized.
- We won't have to think about them until the next VA.
- Future VAs can be cursory once we do a good one.
- Some software package can do most of the work for us.
- Only security experts with many years of experience should participate.
- Whatever is commonly done in our industry is enough.
- Multiple layers of mediocre security = good security.
- Compliance = Good Security.
- High-Tech = High Security.
- Inventory & Security are the same thing. ≠

Warning: Multiple Layers of Security

- Multiple layers of bad security do not add up to good security.
- Tends to be a cop-out to avoid improving security.
- Leads to complacency.
- Some layers may not counter the insider threat. Example: fences.
- Some layers are not backups for others. Example: tamper-indicating seals & fences.

good AVA

General Attributes of Effective AVAs

21. Thinking about vulnerabilities & countermeasures does not end when the AVA is officially over!

22. Don't overlook or under-estimate the insider threat, especially from disgruntled employees.

> Honesty may be the best policy, but it's important to remember that apparently, by elimination, dishonesty is the second-best policy.
> -- George Carlin

not gruntled

Disgruntled Workers

Research shows that employee disgruntlement is associated with perceptions of unfairness & inequity, not necessarily objective conditions.

> We have met the enemy and he is us.
> -- Walt Kelly, the words of Pogo in Earth Day 1971 cartoon strip

Disgruntled employees are known to be a risk for workplace violence, espionage, theft, & sabotage.

> Actual courtroom testimony:
> Q: James shot Tommy Lee?
> A: Yes.
> Q: Then Tommy Lee pulled out his gun and shot James in the fracas?
> A: No, sir, just above it.

not gruntled

Workplace Violence (USA)

- ~ 1.7 million victims of workplace violence each year
- >800 workers killed each year due to workplace homicide

- Homicide is the number one cause of on-the-job deaths for females

Source: NIOSH

Always go to other people's funerals. Otherwise they might not come to yours. -- Yogi Berra

not gruntled

Disgruntlement Countermeasures

- Listen, acknowledge, validate, & empathize with employees.
- Allow employees to freely offer suggestions & concerns.
- Have legitimate complaint resolution processes. Too often these are non-existent, ineffective, adversarial, or fraudulent, especially in large or bureaucratic organizations. This is very dangerous (and bad for productivity).
- Be aware that employee perceptions about fairness are the only reality.

- Treat departing employees & retirees well.

Sincerity is everything. If you can fake that, you've got it made.
-- George Burns (1896-1996)

r e p o r t

The AVA Report

1. It must be clear that the AVA will produce more suggestions & countermeasures than are likely to be implemented. Security mangers (not the assessors) should ultimately decide which (if any) make sense to employ.

2. Findings are reported to the highest appropriate level without editing, inter-pretation, or censorship by middle managers.

> The problem is not that there are problems. The problem is expecting otherwise and thinking that having problems is a problem.
> -- Theodore Rubin

r e p o r t

The AVA Report

3. No confusion about the difference between AVAs and other kinds of testing (materials, environmental, ergonomic, field readiness, personnel, compliance).

4. The vulnerability assessors need to praise the good things because:
   - We want the good things to be recognized and to continue.
   - Security managers need to be willing to arrange for future VAs.
   - Discussing the good things will make security managers more willing to hear about potential problems.

> Honest criticism is hard to take, particularly from a relative, a friend, an acquaintance, or a stranger.
> -- Franklin B. Jones

The AVA Report

r
e
p
o
r
t

5. The report needs to include:

+ identity & experience of the assessors
+ any conflict of interest
+ any *a priori* constraints
+ time & resources used
+ samples, details, and/or demonstration of attacks
+ time, expertise, & resources required by an adversary to execute the attacks
+ possible countermeasures
+ a sanitized, statistical summary of the findings & identity of the assessors if the sponsor wishes to take public credit for the AVA.

> I don't care what is written about me as long as it isn't true.
> -- Katherine Hepburn (1907-2003)

How Flawed is Your Security Program? Take Our Test!

You're penalized 1 point for each of the following 45 attributes that generally apply to your security program. Total up your overall score.

Total points	Rating
0-2	a top-notch security program
3-6	significant room for improvement
7-14	not a healthy security program
15-22	Keystone Cops
23+	Maybe Moo Burger needs a new Assistant Manager?

45 Attributes of Flawed Security Programs

1. Widespread arrogance & overconfidence.
2. Security is viewed as binary. (This inhibits improvement.)
3. Insiders are not viewed as a threat.
4. Overly focused on paperwork, auditors, regulations, & formality.
5. Security & security managers are micro-managed by unqualified business executives.

Attributes of Flawed Security Programs (con't)

6. Security personnel are not encouraged to think on the job, or to ask questions and raise concerns.
7. Security personnel are reluctant to report problems or security incidents.
8. Security problems, vulnerabilities, & incidents are covered-up by security managers.
9. Serious vulnerabilities are assumed not to exist.

Attributes of Flawed Security Programs (con't)

10. Comments, suggestions, and criticisms concerning security are unwelcome from any quarter (internal or external) and result in retaliation, undue defensiveness, or automatic knee-jerk rejection of the input.

11. Creative, comprehensive, holistic vulnerability assessment are rare; security is rarely tested. "Vulnerability assessments" don't find significant vulnerabilities or result in substantial changes.

Attributes of Flawed Security Programs (con't)

12. "What if?" mental or walk-through exercises are rare, instead of being done daily or weekly.

13. Security personnel are granted few opportunities for education and professional advancement.

14. Security personnel receive little training and practice, including with observational skills, dealing with people, and how to spot social engineering tactics, misdirection, and sleight of hand.

Attributes of Flawed Security Programs (con't)

15. Security supervisors & managers are not well respected by subordinates.

16. Security managers rarely "walk the spaces" or chat informally with regular (non-security) employees.

17. Security personnel are not well respected by regular (non-security) employees, and/or tend to be rude, unprofessional, or inefficient in their dealings with regular employees and the public.

Attributes of Flawed Security Programs (con't)

18. The morale and self-esteem of security personnel is low. Appearance is poor.

19. Low-level security personnel are treated poorly.

20. Low-level security personnel are rarely recognized for good work.

21. Security training exercises are unrealistic & tedious.

22. Security personnel have few opportunities to demonstrate their prowess in contests/exercises.

Attributes of Flawed Security Programs (con't)

23. Security personnel feel no loyalty or connection to their employer, or to the employees and the organization they are protecting.

24. The organization lacks a fair and effective grievance or complaint resolution process for disgruntled employees (whether security or non-security personnel).

25. Confidential, professional counseling is not available for troubled employees (whether security personnel or otherwise).

Attributes of Flawed Security Programs (con't)

26. Security personnel are not briefed at the start of a shift, nor checked for fitness of duty.

27. Security personnel are not debriefed after their shift.

28. No pre-employment screening of employees; no periodic, thorough back-ground and reliability checks performed on security and other critical personnel.

Attributes of Flawed Security Programs (con't)

29. Unexplained or unexpected absences of security personnel are not investigated, nor are sudden outbreaks of widespread illness.
30. Sources of food and drink are not secure. Critical security personnel accept food & drink from colleagues, co-workers, and even the public.
31. Rosters, duty assignments, & schedules of authorized work are not well protected from tampering. Paper documents and verbal orders for security personnel are taken at face value.

Attributes of Flawed Security Programs (con't)

32. Security personnel do not know exactly how & when to summon help or sound an alarm.
33. There are no clear, widely understood and mentally rehearsed policies on the use of physical force.
34. Security personnel are vague on exactly what is expected of them.
35. The health and safety of security personnel is a low priority. Insurance and medical coverage is absent or poor.

Attributes of Flawed Security Programs (con't)

36. VIPs are allowed to bypass standard security procedures.

37. Security managers are automatically fired when there is a major security incident. Low-level security personnel are automatically disciplined or fired when there is a minor security incident.

38. Relations with the public, neighbors, & local authorities are poor, neglected, or ignored.

Attributes of Flawed Security Programs (con't)

39. Security awareness training for non-security personnel is boring, insipid, insulting, & threatening. It doesn't emphasize why security is important to them.

40. Security rules are put in place with little thought, few sanity checks, and little input from the people affected.

41. Hassling employees or the public is thought to automatically translate into good security.

Attributes of Flawed Security Programs (con't)

42. The security rules are only relevant for the good guys because the bad guys will ignore them.

43. Technology is viewed as a silver bullet for security.

44. New technology that employees would like to use is mindlessly banned for security reasons, rather than trying to intelligently accommodate it.

45. Changes in security are interpreted as an indication that security managers have been screwing up all this time.

> Those are my principles.
> If you don't like them, I have others.
> -- Groucho Marx (1890-1977)

How Flawed is Your Security Program? Take Our Test!

You're penalized 1 point for each of the following 45 attributes that generally apply to your security program. Total up your overall score.

Total points	Rating
0-2	a top-notch security program
3-6	significant room for improvement
7-14	not a healthy security program
15-22	Keystone Cops
23+	Maybe Moo Burger needs a new Assistant Manager?

more info

The LANL Vulnerability Assessment Team

Roger Johnston, Ph.D., CPP, Ron Martinez, Leon Lopez, Sonia Trujillo, Adam Pacheco, Anthony Garcia, Jon Warner, Ph.D., Alicia Herrera, Eddie Bitzer, M.A.

http://pearl1.lanl.gov/seals

We have a CD containing related papers & reports.

You can request a copy at rogerj@lanl.gov

Ring the bells that still can ring.
Forget your perfect offering.
There is a crack in everything.
That's how the light gets in.
-- The song "Anthem", by Leonard Cohen

more info

Other Issues Covered on the CD

Q: Can AVA techniques be used to improve safety, not just security?
A: "Adversarial" Safety Analysis

Q: How, to whom, and in what detail do you disclose security vulnerabilities that affect others?
A: Vulnerability Disclosure Index (0-100%)

Q: How can we reduce security guard turnover?
A: Tools from Industrial/Organizational Psychology

Q: How can cargo security be improved?
A: Better tamper-indicating seals, use protocols, and new cargo monitoring techniques

Q: How can we counter pharmaceutical counterfeiting w/o RFIDs (which don't provide security or involve consumers)?
A: Numeric tokens