Common Cargo Security Blunders and How to Avoid Them

Roger G. Johnston, Ph.D., CPP
Jon S. Warner, Ph.D.
Vulnerability Assessment Team
Argonne National Laboratory

630-252-6168 rogerj@anl.gov
http://www.ne.anl.gov/capabilities/vat

Argonne National Laboratory

3 sq miles, ~3200 employees, $630+ million annual budget
R&D and technical assistance for government & industry

Argonne NATIONAL LABORATORY

... for a brighter future

U.S. Department of Energy

UChicago ▸ Argonne LLC

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

Vulnerability Assessment Team (VAT)

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

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

The VAT has done vulnerability assessments on hundreds of physical security devices, systems, & programs.

Sponsors

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

Realities of Cargo Security Technology 1

Fix the non-technical stuff before you get all spun up about high technology. High tech will not solve your security problems.

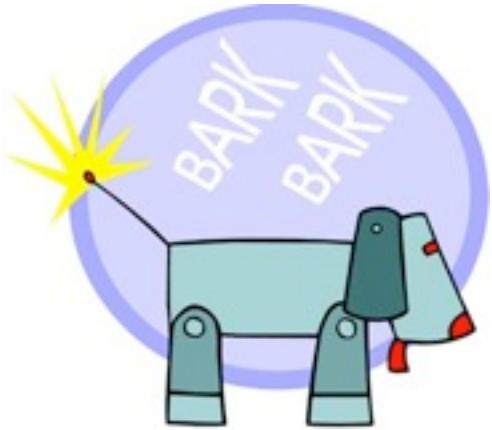
If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

-- Bruce Schneier

Realities of Cargo Security Technology 2

If you can't respond in real-time (immediately), you don't need real-time monitoring or a real-time alarm.

Most cargo real-time monitoring or hijack alarm devices are really about recovering the truck in a day or two (at best). It's not typically about recovering the goods.



Inspector Jacques Clouseau: The good cop/bad cop routine is working perfectly.
Ponton: You know, usually two different cops do that.
-- From the movie *The Pink Panther* (2006)

Realities of Cargo Security Technology 3

Employing a truck panic alarm or biometrics must be weighed against the fact that the truck driver is involved in ~80% of all cargo thefts!

The ultimate security is your understanding of reality.
-- H. Stanley Judd

Common Cargo Blunders 1

- Allowing private vehicles in loading dock areas
- Chaotic staging & loading dock areas
- Receiving & Shipping in the same area
- Not having separate, secure, enclosed storage areas for high-value cargo
- Truck drivers are allowed in the loading dock area

Common Cargo Blunders 2

- Not parking loaded trucks back to back overnight if the parking area lacks good security measures
- Not having perimeter security patrols at unpredictable times
- Not painting identification numbers on the top of trucks and transportainers so they can be spotted from the air or overpasses during emergencies

Common Cargo Blunders 3

- Trucks are not prohibited from stopping the first 150 miles from the departure point
- Predictable truck stops
- Not insisting on a dedicated shipment
- Loading millions of dollars of product into a single unescorted truck provided by the low-bid trucking company that doesn’t enforce its own security rules (if it has any).

Common Cargo Blunders 4

- Not making sure your trucking company follows its own security rules
- Not making sure your trucking company does background checks on its employees
- Less money spent on cargo security than other areas of security involving lower potential losses
- One-size-fits-all; no proportionality of security measures commensurate with the threat; concentrating on greatest cargo volume, not greatest threat

More Cargo Security Blunders

Locking or Sealing the Handle

Terminology

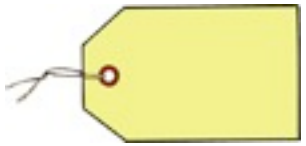
"Ich bin ein Berliner." [I am a jelly donut.]
-- John F. Kennedy (1917-1963]

lock: a device to delay, complicate, and/or discourage unauthorized entry.

(tamper-indicating) seal: a device or material that leaves behind evidence of unauthorized entry.

trap: a covert seal

tag: a unique identifier (e.g. license plate). There are 4 kinds, depending on whether counterfeiting and/or lifting is an issue.



Seal Realities

1. All seals need a unique identifier (like a “serial” number).
2. A seal is not a lock.
3. Use barrier seals with care!

There are three kinds of men. The one that learns by reading. The few who learn by observation. The rest of them have to pee on the electric fence for themselves.

-- Will Rogers (1879 - 1935)

Seal Realities

4. A seal must be inspected, either manually or with an automated reader, to learn anything about tampering or intrusion. The person doing this must know exactly what they are looking for.

5. Unlike locks & safes, defeating seals is more about fooling people & the use protocol than beating hardware.

6. A seal is no better than its use protocol.

A modest seal used intelligently can provide effective tamper detection.
A sophisticated seal used poorly will not.

It's better to be looked over than overlooked.
-- Mae West (1893-1980) in
Belle of the Nineties, 1934

(Seal Use Protocol)

A seal is no better than its formal and informal "use protocol"...

...how the seal is:

- manufactured
- procured
- shipped
- stored
- checked out
- installed
- inspected
- removed
- destroyed after use

- And how the seal data and reader are stored & protected and
- How the seal installers/inspectors are trained.

Seal Realities

7. There is no such thing as an undefeatable seal.

8. Misleading and confusing terminology is not helpful.

"I'm not a rocket surgeon."
-- Reality TV star &
tattoo artist Kat Von D

(Bad Seal Terminology)

The slovenliness of our language makes it easier for us to have foolish thoughts.
-- George Orwell (1903-1950)

- "tamper-proof" seal
- "tamper-resistant" seal
- security seal vs. indicative seal
- "high security" seal (e.g. ISO 17712)

It's not just about semantics.
It's about misconceptions & sloppy thinking.

When words lose their meaning, there is chaos in the land.
-- Confucius (551 BC – 479 BC)

Seal Realities

9. Effective tamper detection is a lot of work.

10. You must watch out for the wrong seal getting installed, or for the seal or door not being fully closed!

11. The seal must be checked for defects (manufacturing or backdoor attack) prior to installation.

12. Backdoor attacks can be implemented on unused seals in seconds at the factory or vendor, in transit, while sitting on loading docks, or prior to use.

13. A high-tech seal (especially with an automated reader) actually takes more work than a simple mechanical seal.

14. Just because the seal reader is happy does not mean the seal inspector should be happy.

Seal Realities

15. Both during seal installation & seal inspection: The door, hasp, locking mechanism, and container must be carefully inspected.

16. Don't write the seal serial number on the truck or railcar!

17. Truck drivers should not inspect the seal or carry the seal paperwork.

18. Don't use seals in sequential order.

19. Protect seals (and seal parts) both prior to use and after removal.

English Game Show Host: Watling Street, which now forms part of the A5, was built by which ancient civilization?
Contestant: Apes?

Seal Realities

20. Compare a seal side-by-side with an unused seal of the same kind, both before installation and during inspection. Check size, color, gloss, surface texture, font, & digit spacing/alignment.

21. The correct serial number is not enough. The seal must be carefully inspected. Watch out for the correct serial number, but the wrong kind of seal!

22. The way they are typically used, adhesive label seals are Security Theater.

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

Pressure Sensitive Adhesive Label Seals

- Lifting & Counterfeiting are easy.
- Lifting is usually the most likely attack.
- The difficulty of either attack is almost always greatly over-estimated by seal manufacturers, vendors, & users.

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

Installation

- It is essential to feel the surface to check that the adversary hasn't pre-treated it to reduce adhesion.

- The surface should not be cold, wet, or corroded.
- Pre-cleaning the surface with a solvent or detergent is strongly recommended.
- Full adhesion requires 48+ hours. A PSA seal is particularly easy to lift the first few minutes to hours. Heat can help. (Don't heat the solvent!)

Pressure Sensitive Adhesive Label Seals

- Match the adhesive to the surface. The best adhesive for bare metal may not be the best for painted metal, plastic, wood, cardboard, or glass.
- Ideally, the adhesive, substrate, & ink should be made of the same material, so they dissolve in the same solvents. (Possible but doesn't exist.)
- Carefully examine the surface area outside the perimeter of the label seal.
- Consider covering the label seal with a plastic protective sheet or clear protective spray.

Inspection

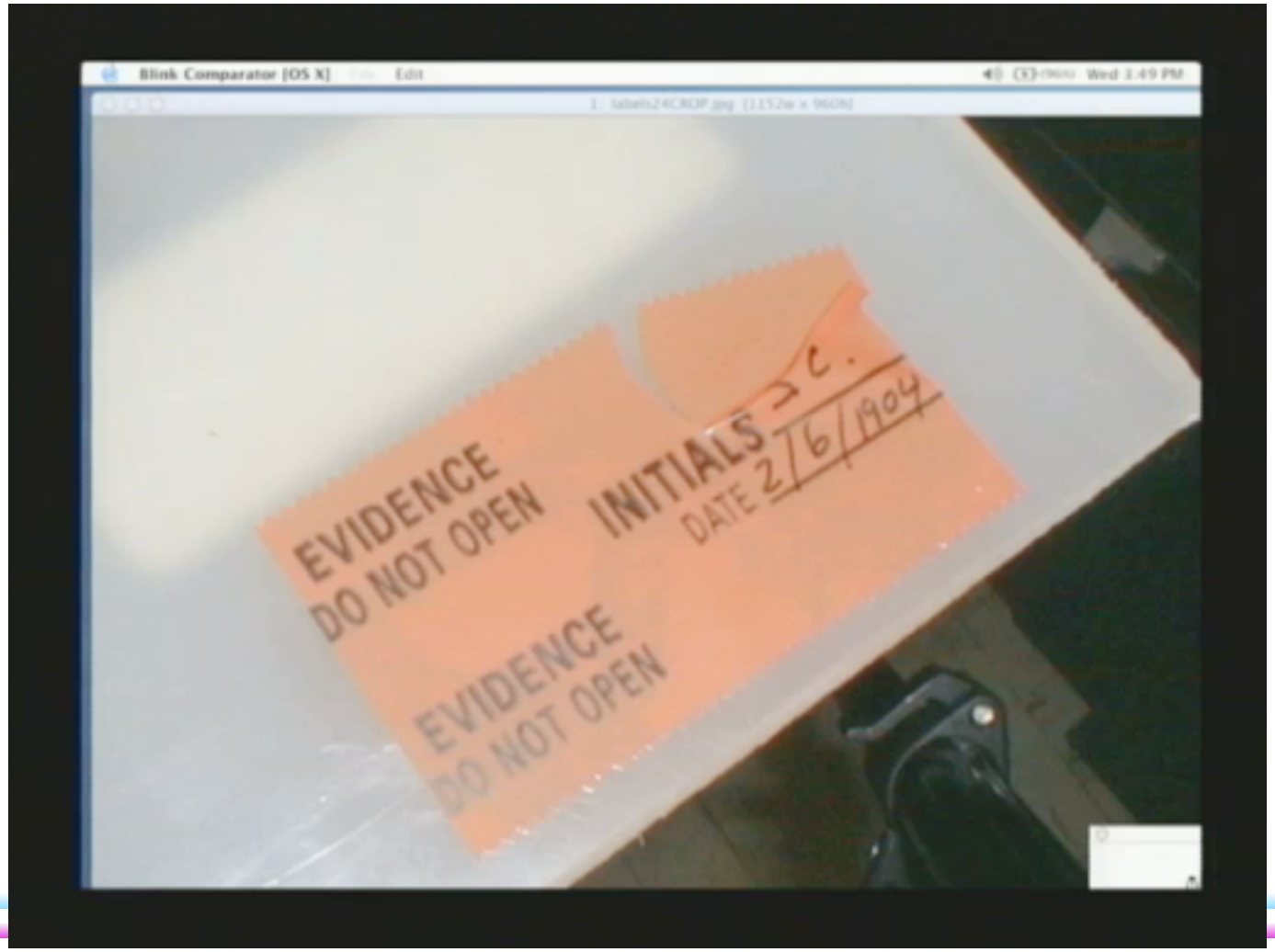
- Smell can be a powerful tool for detecting solvents, adhesives, paints, inks, epoxies, or other foreign material used in an attack.
  Or use a handheld chemical "sniffer" ($150-$9K).

- Always compare the seal side-by-side with an unused seal you have protected.
  Check size, color, gloss, font, & digit spacing/alignment.

- **The best test for tampering is to closely observe how the label seal behaves when it is removed.**

Pressure Sensitive Adhesive Label Seals

- A blink comparator is a very powerful tool for detecting tampering with PSA label seals.



Seal Realities

23. Seal manufacturers, vendors, and users will typically (greatly) over-estimate the difficulty of defeating their seals

24. Counterfeiting is usually not the most likely attack (except possibly for adversaries simultaneously attacking many seals). Vulnerabilities associated with re-using the original seal are more important.

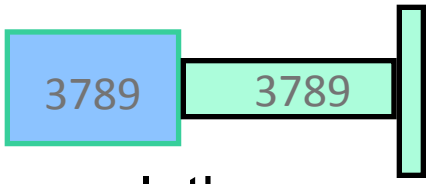
25. Counterfeiting is nevertheless often surprisingly easy.

26. It doesn't matter, however, because typically the adversary needs to mimic only the superficial appearance and (perhaps) the apparent performance of the seal. This is much easier than true counterfeiting!

> Sincerity is everything. If you can fake that, you've got it made.
> -- George Burns (1885-1996)

Seal Realities

27. (Ideally the same) serial number should appear on every independent part of a seal.



28. If serial numbers are stamped or embossed on a seal, they should be done deeply enough that they can't be easily buffed off.

29. Both the seal data (e.g., serial numbers) and the seal reader (if there is one) must be constantly protected.

30. Better seals are possible (but almost nobody is asking for them).

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

Blunder: Confusing Inventory & Security

Inventory

- Counting and locating stuff
- No nefarious adversary
- May detect innocent errors by insiders, but not surreptitious attacks by insiders or outsiders.

Security

- Meant to counter nefarious adversaries (insiders and outsiders)
- Watch out for mission creep: inventory systems that come to be viewed as security systems!

Inventory vs. Security Misconceptions

- An inventory system spots missing items, therefore it detects theft.

Wrong!

- I can just add security to my existing inventory system.

This almost never works well.

- Bad guys aren't interested in surreptitious thefts.

We disagree.

Examples of Confusing Inventory & Security

- rf transponders (RFIDs)
- contact memory buttons
- GPS

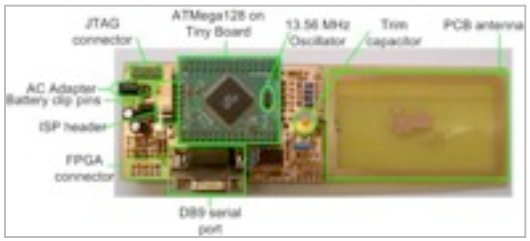
Usually easy to:
* lift
* counterfeit
* tamper with the reader
* spoof the reader from a distance

Very easy to spoof, not just block or jam!

A Sampling of RFID Hobbyist Attack Kits Available on the Internet

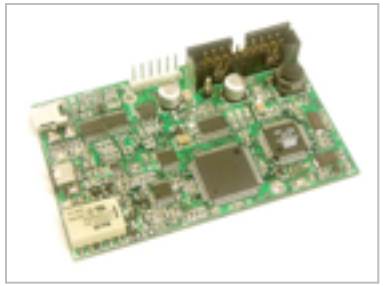
Commercial: $20 Car RFID Clone (Walmart)

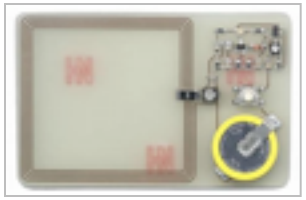
Commercial: Used for "faking RFID tags", "reader development."

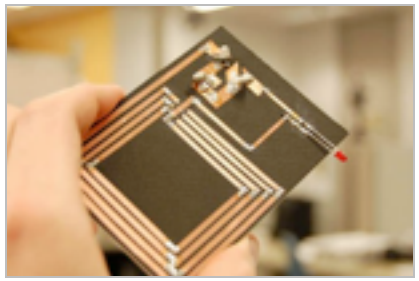


RFID Skimmers, Sniffers, Spoofers, and Cloners; oh my!

Documents, code, plans needed to build your own: free.



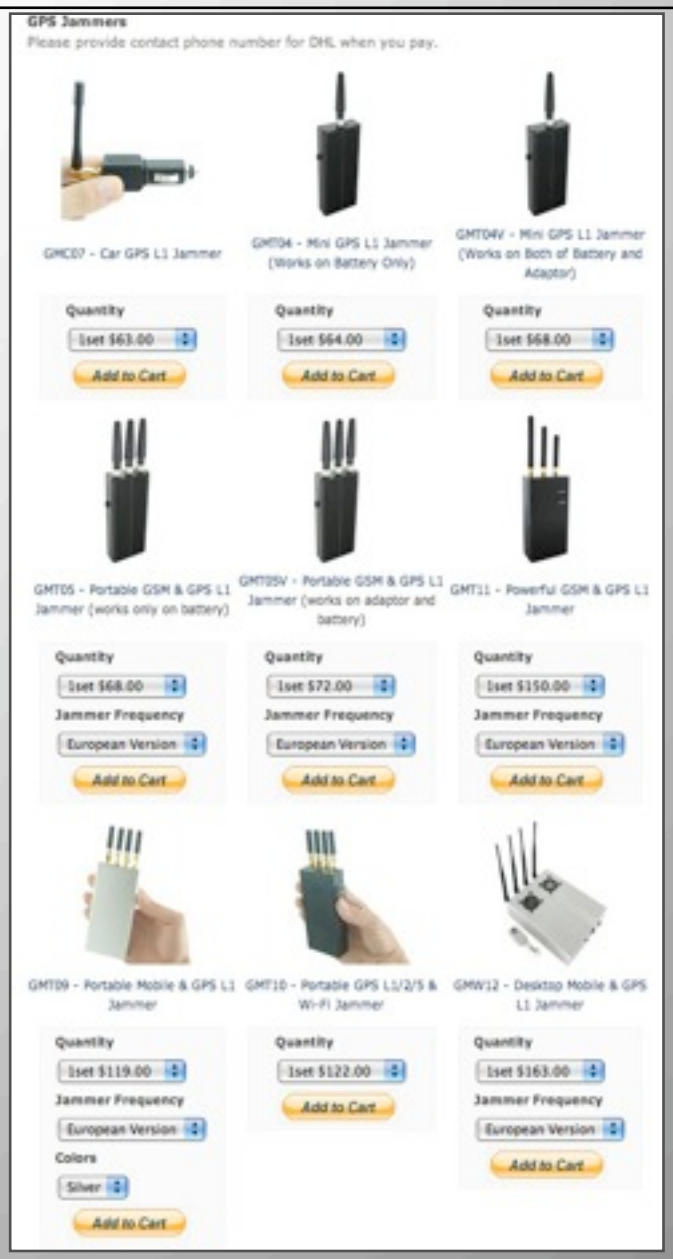




There is a huge danger to customers using this (RFID) technology, if they don't think about security.

-- Lukas Grunwald (creator of RFDump)

GPS (and Other) Jamming



Spoofing Civilian GPS Receivers

- Easy to do with widely available GPS satellite simulators.
- These can be purchased, rented, or stolen.
- Not export controlled.
- Many are surprisingly user friendly. Little expertise is needed in electronics, computers, or GPS to use them.

GPS Spoofing

GPS Spoofing

GPS Spoofing

Some Potential GPS Spoofing Attacks

- Crash national utility, financial, telecommunications & computer networks that rely on GPS for critical time synchronization
- Steal cargo or nuclear material being tracked by GPS
- Install false time stamps in security videos or financial transactions
- Send emergency response vehicles to the wrong location after an attack
- Interfere with military logistics (DoD uses civilian GPS for cargo)
- Interfere with battlefield soldiers using civilian GPS (against policy, but common practice anyway)
- Spoof GPS ankle bracelets used by courts and GPS data loggers used for counter-intelligence
- The creativity of the adversary is the only limitation

GPS Cargo Tracking / Geofencing

GPS Satellite

GPS
Signal

(vulnerable here)

Tracking Information Sent to HQ
(perhaps encrypted/authenticated)

GPS is great for navigation, but it does not provide high security.

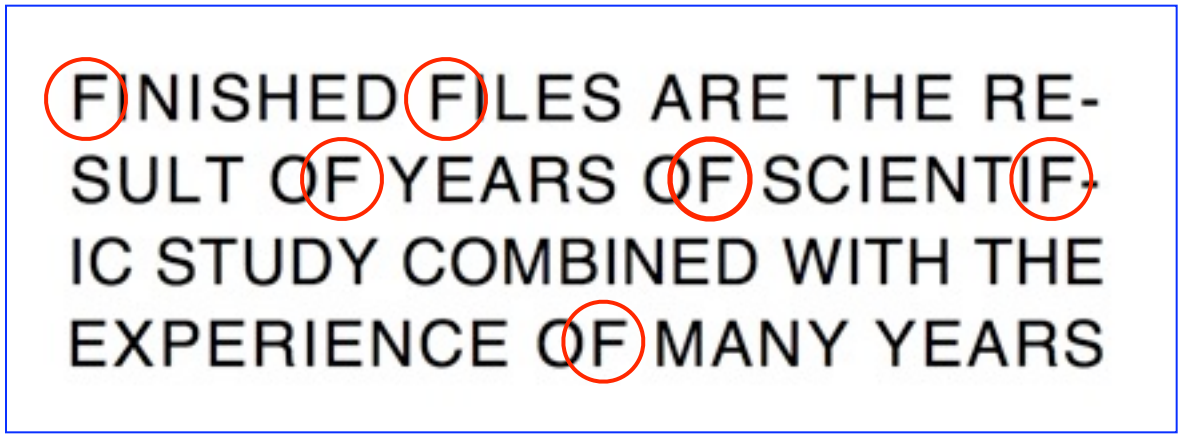
The Good News: Low-Cost Countermeasures

Look (in hardware or software) for artificial characteristics of GPS satellite simulator signals (or pre-recorded real GPS signals):

- Check the time intervals
- Monitor relative signal strength
- Monitor absolute signal strength
- Do a time comparison “Sanity Check”
- Perform a motion-based “Sanity Check”
- Monitor # of satellites & ID codes received
- Monitor signal strength of each received satellite

None of these countermeasures are currently in use.
They would require about ~$15 in parts (retail).

FINISHED FILES ARE THE RESULT OF YEARS OF SCIENTIFIC STUDY COMBINED WITH THE EXPERIENCE OF MANY YEARS


FINISHED FILES ARE THE RE-
SULT OF YEARS OF SCIENTIF-
IC STUDY COMBINED WITH THE
EXPERIENCE OF MANY YEARS

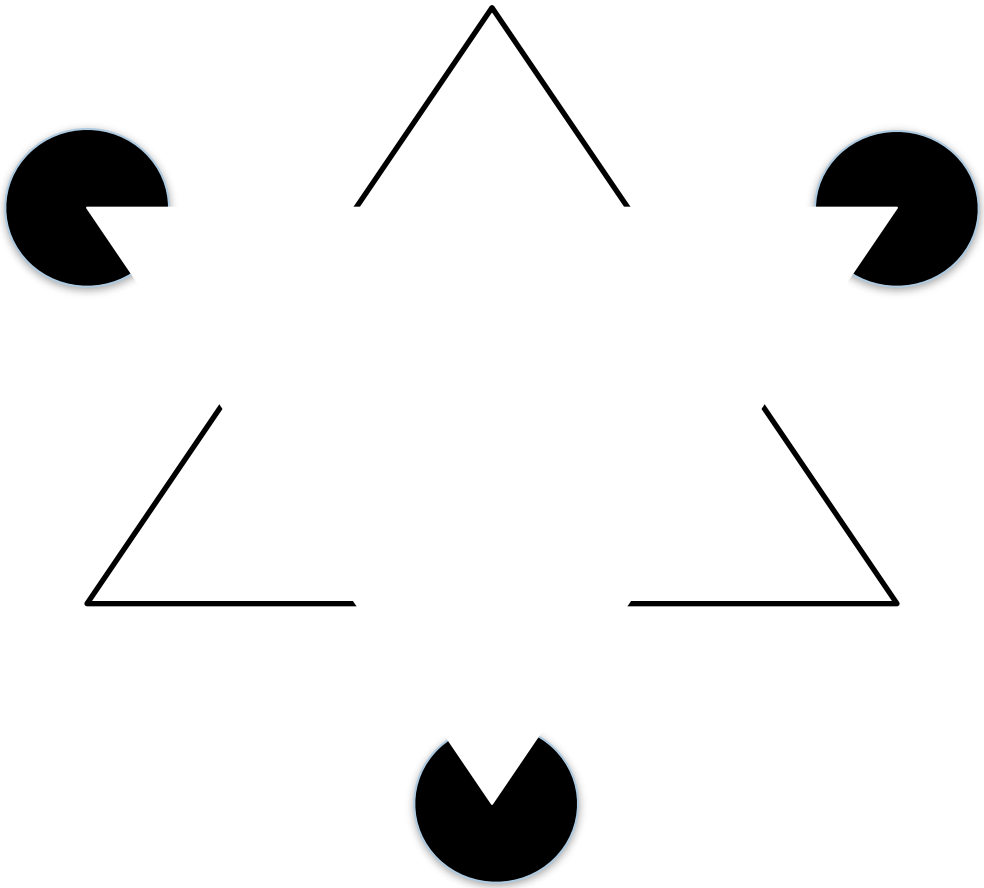
50 Years of Cognitive Psychology Research

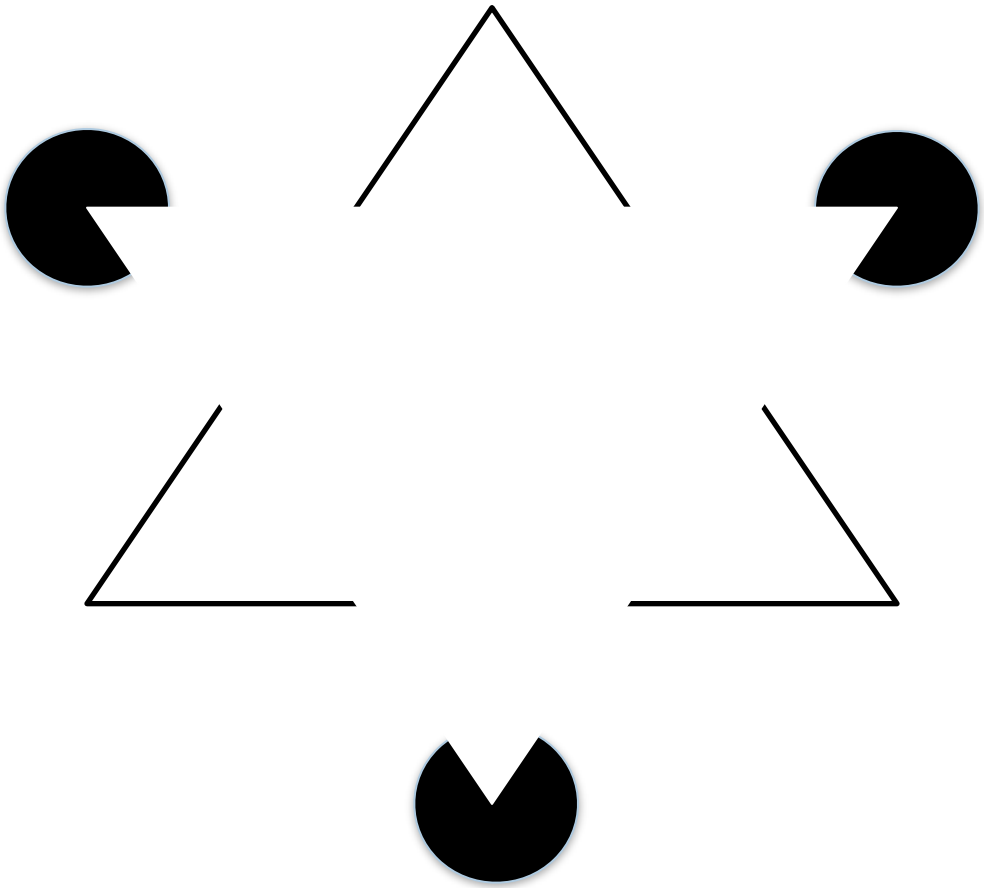
- People are remarkably poor observers.
- They don't realize how bad they are.
- "Perceptual Blindness" = "Inattentional Blindness": the phenomena of not being able to perceive things that are in plain sight, especially if you're focused on a particular visual task.

As a rule, we perceive what we expect to perceive. The unexpected is usually not perceived at all.

-- Peter Drucker (1909-2005)

Kanizsa Triangle





Perceptual Blindness

Blunder: Ignoring Perceptual Blindness

There are serious implications for security guards & safeguards inspectors, especially those who:

- ✓ provide nuclear safeguards
- ✓ check security badges
- ✓ watch video monitors
- ✓ make daily rounds
- ✓ inspect seals
- ✓ guard gates
- ✓ etc.

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

Possible Countermeasures for Perceptual Blindness?

If you don't find it often, you often don't find it. -- Jeremy M. Wolfe

- plan for it in the security plan
- educate security guards about it
- train on observational skills ???
- lots of rehearsing of "What if?"
- strange events during exercises
- demonstrations from magicians about distraction, misdirection, & sleight-of-hand

The eye sees only what the mind is prepared to comprehend.
-- Henri Bergson (1859-1941)

Blunder: Poor Security for Urine Drug Tests

It's easy to tamper with urine test kits.

Most urine testing programs (including for world class athletes & federal employees) have very poor security protocols.

Emphasis has been on dopers who avoid detection, but an innocent athlete or employee who's sample is spiked is equally troubling.

Serious implications for safety, law enforcement, public welfare, national security, fairness, litigation, careers, livelihood, reputations.

Journal of Drug Issues **39**, 1015-1028 (2009)

Selected VAT Security & Human Factors Publications

RG Johnston, “Countermeasures to Perceptual Blindness”, Proceedings of the INMM (2010).

EG Bitzer, PY Chen, and RG Johnston, “Security in Organizations: Expanding the Frontiers of Industrial-Organizational Psychology”, *International Review of Industrial and Organizational Psychology 24, 131-150 (2009).*

EG Bitzer, “An Exploratory Investigation of Organizational Security Climate in a Highly Regulated Environment”, Ph.D. Thesis, Colorado State University (2008).

EG Bitzer and A Hoffman, "Psychology in the Study of Physical Security", *Journal of Physical Security* 2, 1-18 (2007).

EG Bitzer, “Strategies for Cutting Turnover”, *Security Management* 50, 88-94 (2006).

EG Bitzer and RG Johnston, “Turnkey Turnaround Solutions: Exploiting the Powerful Tools of I/O Psychology”, Los Alamos National Laboratory Report LAUR-05-1130, (2005).

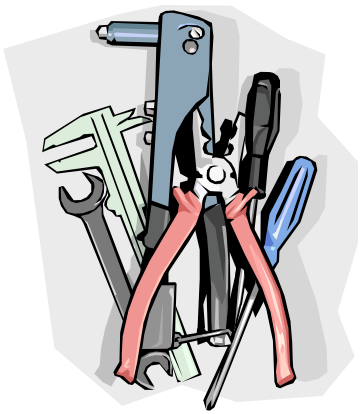
RG Johnston, JS Warner, ARE Garcia, et al., "Nuclear Safeguards and Security: We Can Do Better", Paper 1009, *Proceedings of the 10th International Conference on Environmental Remediation and Radioactive Waste Management*, September 4-8, 2005, Glasgow, Scotland.

RG Johnston, “Adversarial Safety Analysis: Borrowing the Methods of Security Vulnerability Assessments”, *Journal of Safety Research* 35, 245-248 (2004).

EG Bitzer and RG Johnston, "A Taxonomy for Security Assignments", *J Security Administration* 26, 1-11 (2003).

Access Control (AC), Including Biometrics

For most AC systems, it's easy to tamper with:



- power
- software
- hardware
- database
- microprocessor
- communications
- backdoor attacks
- keys or passwords
- door lock or turnstile

> I do not care to belong to a club that accepts people like me as members.
> -- Groucho Marx (1890-1977)

Most "security" devices have little built-in security or ability to detect intrusion/tampering.

Access Control (AC) Device Vulnerabilities

The importance of cradle-to-grave secure chain of custody:

As with most security devices, compromised after only 15-30 secs of access (at the factory or vendor, on the loading dock, in transit, in the receiving department, or after being installed).

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

Security of Security Products

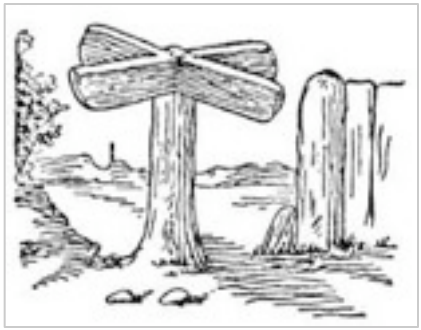
Access Control (AC)

Question: Is that really your AC 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

Access Control (AC) Blunders



- Bad door or turnstile design
- Not registering when the door is opened.
- Not tracking who exits
- No role-based access; Not changing access with promotions & personnel changes
- Not securing the equipment and personnel that make ID badges

"Badges? We don't need no stinkin' badges!"
-- From the movie *The Treasure of the Sierra Madre (1948)*
[The actual dialog was, "Badges? We ain't got no badges. We don't need no badges! I don't have to show you any stinkin' badges!"]

Biometrics Blunders

All the blunders of access control, plus:

- Not understanding how easy it is to counterfeit a biometric signature—though why bother?
- Downloading the entire database to satellite stations
- Not turning off the enroll function on satellite stations
- Believing the snake oil & bogus performance specs



I'm always amazed to hear of accident victims being identified by their dental records. If they don't know who you are, how do they know who your dentist is? -- Paul Merton

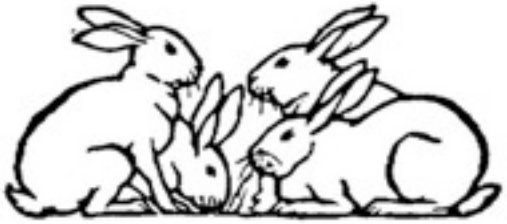
Warning: Multiple Layers of Security ("Security in Depth")

- Increases complexity
- Multiple layers of bad security do not equal good security.
- Often mindlessly applied: the layers are not automatically backups for each other, or may even interfere with each other
- Leads to complacency
- Tends to be a cop-out to avoid improving any 1 layer or thinking critically about security

Security is only as good as the weakest link. -- old adage

Vulnerability Assessment (VA) Myths

- You should do a VA at the end of development or planning
- There are a small number of vulnerabilities.
- Most or all can be found & eliminated.
- Vulnerabilities are bad news.
- A VA should ideally find zero vulnerabilities.
- Engineers understand security.



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)

Vulnerability Assessment (VA) Myths

- The most unimaginative, unquestioning security people in your organization should do the VA.
- The good guys get to define the problem.
- A VA is a formal, rigorous process.

- Software tools will find most of your vulnerabilities.
- These methods are effective at finding vulnerabilities: Security Surveys/Audits, Design Basis Threat, CARVER, Delphi Method, Threat Matrices, Fault Tree Analysis.
- It's more important to understand threats than vulnerabilities.

Blunder: Not Understanding What a VA is For

The purpose of a vulnerability assessment is to improve security, not to:

- Pass a test
- Generate metrics
- Justify the status quo
- Check against some standard
- Claim there are no vulnerabilities
- Rationalize the research & development
- Endorse a security product, or Certify it as “good” or “ready for use”
- Perform material, environmental, or quality tests
- Apply a mindless, bureaucratic stamp of approval
- Praise or accuse the developer, manufacturer, vendor, or user

Other Common Security Blunders

- Compliance-based security
- VIPs bypass security
- Letting anybody into the facility who acts like she knows what she is doing
- Not trying to bribe your employees, vendors, & contractors
- Overly complex, changing, variably interpreted, stupid security rules
- Rules that only the good guys follow

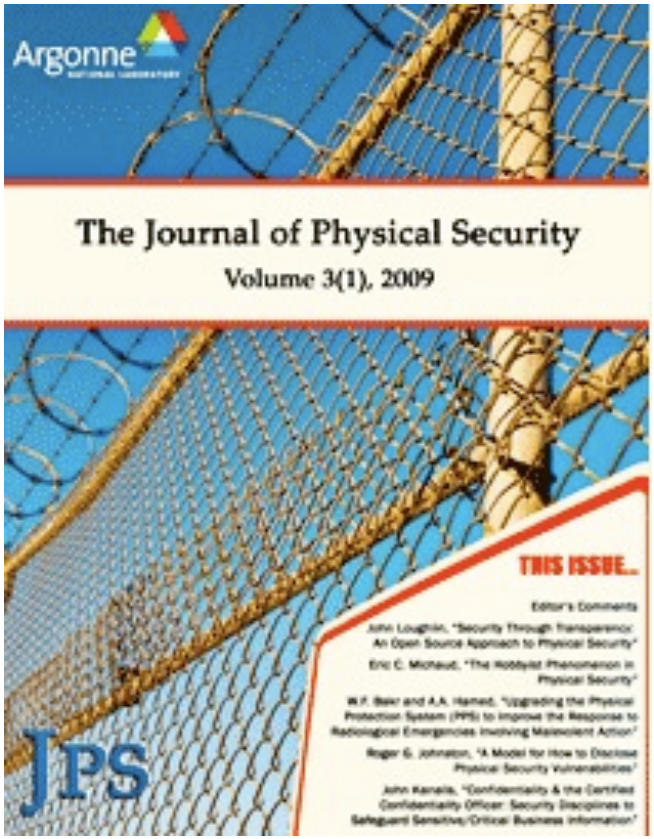
Other Common Security Blunders

- Too much emphasis on protecting physical assets instead of more important things
- Obsession with prevention, while ignoring mitigation, recovery, & resiliency
- Poor security camera resolution
- Not asking the security manufacturer or vendor how to defeat their product and about the countermeasures
- Locking or sealing a door with the hinges on the outside!

Everybody has a plan until they get hit in the face.
-- Various attributed to Sun Tzu (544?-496? BC)
and boxers Mike Tyson, Joe Louis, and Leon Spinks

For More Information...

Journal of Physical Security:
A free, online,
peer-reviewed R&D journal



http://jps.anl.gov

This presentation + much more related material is available from
rogerj@anl.gov
or
http://public.me.com/va_team
(password = shi-kah-gho)

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)