Invited talk for the 21st annual conference on Computers, Freedom, and Privacy, June 14-16, 2011, Washington, D.C.

Physical Security, Security Theater, and Snake Oil

Roger G. Johnston, Ph.D., CPP

Vulnerability Assessment Team
Argonne National Laboratory

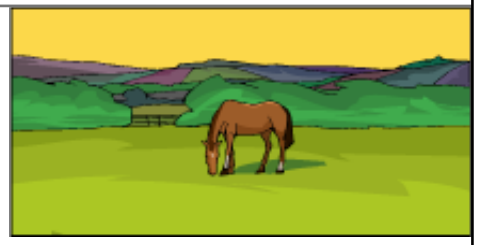
630-252-6168 rogerj@anl.gov
http://www.ne.anl.gov/capabilities/vat

The greatest of faults, I should say, is to be conscious of none.

-- Thomas Carlyle (1795-1881)

http://www.youtube.com/watch?v=frBBGJqkz9E

Physical Security: Scarcely a Field at All



- You can't (for the most part) get a degree in it from a major 4-year research university.
- Not widely attracting young people, the best & the brightest.
- Few peer-review, scholarly journals or R&D conferences.
- Lots of Snake Oil & Security Theater.
- Shortage of models, fundamental principles, metrics, rigor, R&D, standards, guidelines, critical thinking, & creativity.
- Often dominated by bureaucrats, committees, groupthink, linear/concrete/wishful thinkers, cognitive dissonance.

Radisson Welcomes
Emerging Infectious Diseases
-- Sign outside a Radisson Hotel

Problem: Lack of Research-Based Security Practice

The Journal of Physical Security

A free, online,
peer-reviewed R&D journal

http://jps.anl.gov

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)

Definition

Security Theater: sham or ceremonial security; Measures that ostensibly protect people or assets but that actually do little or nothing to counter adversaries.

Actual Courtroom Testimony:
Witness (a Physician): He was probably going to lose the leg, but at least maybe we could get lucky and save the toes.

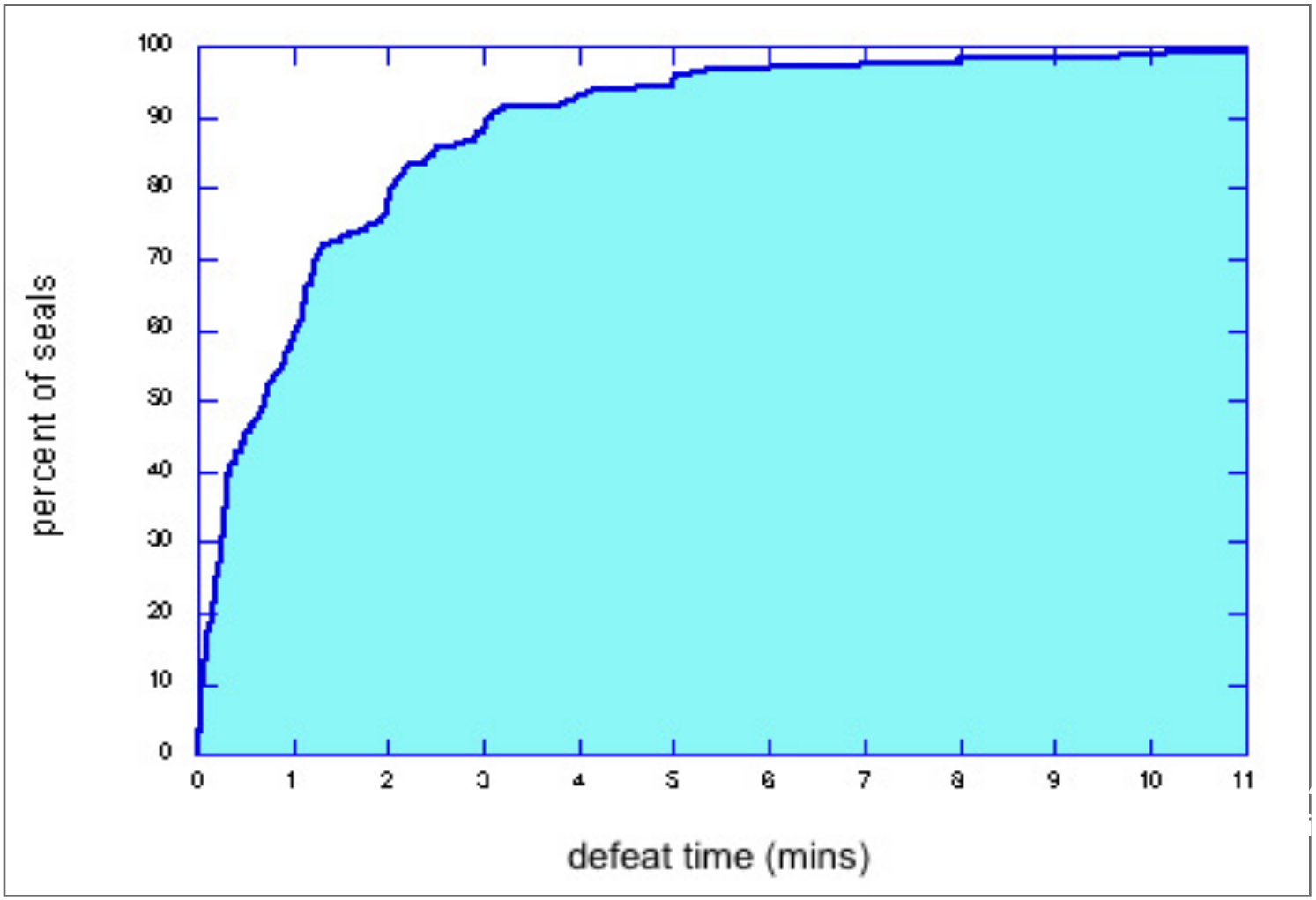
Security Theater

1. Best way to spot it is with an effective thorough VA.

2. Next best is to look for the characteristic attributes:

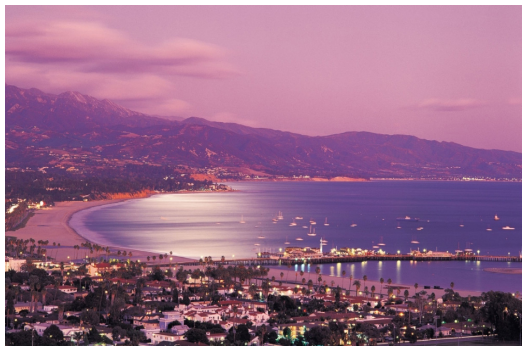
- Sense of urgency
- A very difficult security problem
- Involves fad and/or pet technology
- Questions, concerns, & dissent are not welcome or tolerated
- **The magic security device, measure, or program has lots of "feel good" aspects to it**
- Strong emotion, over confidence, arrogance, ego, and/or pride related to the security
- Conflicts of interest
- No well-defined adversary
- No well-defined use protocol
- No effective VAs; no devil's advocate
- The technical people involved are mostly engineers
- Intense desire to "save the world" leads to wishful thinking
- People who know little about security or the technology are in charge

Seals are easy to defeat: Percent of seals that can be defeated in less than a given amount of time by 1 person using only low-tech methods



Tamper-Evident Packaging Test

7th Security Seals Symposium
Santa Barbara, CA
February 28 - March 2, 2006



- 71 tamper detection experts participated.
- Various consumer food & drug products were tampered with.
- A college student (Sonia Trujillo) did the tampering using only low-tech attacks.

Results: Statistically the same as guessing!

If tamper detection experts can't reliably detect product tampering, what chance does the average consumer have?

On a bag of Fritos: "You could be a winner! No purchase necessary. Details inside."

Poor Security for Urine Drug Tests

It's easy to tamper with urine test kits.

Most urine testing programs (government, companies, athletes) have very poor security protocols.

Emphasis has been on false negatives, but false positives are equally troubling.

Serious implications for safety, courts, public welfare, national security, fairness, careers, livelihood, reputations, sports.

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

Polygraphs = Snake Oil

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…"

Electronic Voting Machines

Diebold Accu-Vote TS

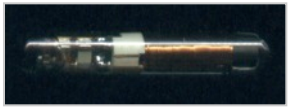
Sequoia Advantage AVC

Question on a job application form: Do you support the overthrow of the government by force, subversion, or violence? Answer from one applicant: Violence.

Blunder: Cheap Locks on Security Hardware

Examples of confusing Inventory & Security

- rf transponders (RFIDs)



- prox cards

- contact memory buttons

- GPS

- Nuclear MC&A

Usually easy to:

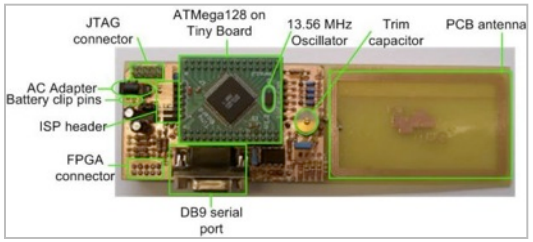
* lift
* counterfeit
* tamper with the reader
* spoof the reader from a distance

Very easy to spoof, not just jam!

A Sampling of RFID Hobbyist Attack Kits Available on the Internet

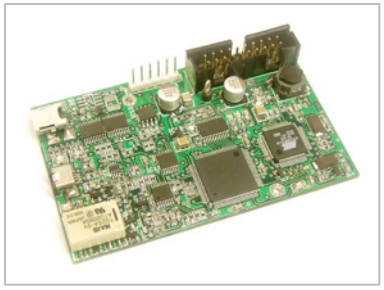
Commercial: $20 Car RFID Clone (Walmart)

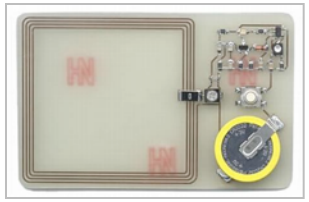
Commercial: Used for "faking RFID tags", "reader development."

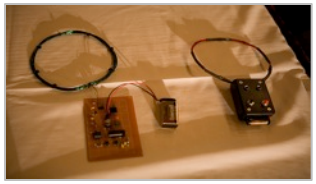


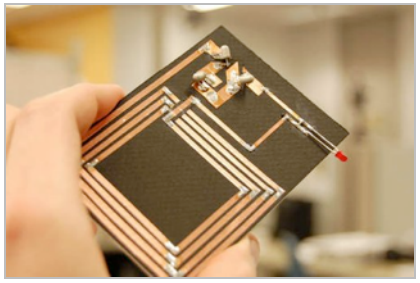
RFID Skimmers, Sniffers, Spoofers, and Cloners; oh my!

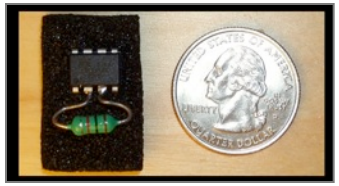
Documents, code, plans needed to build your own: free.

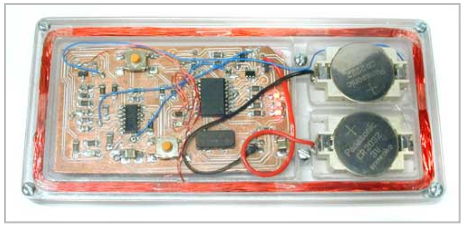


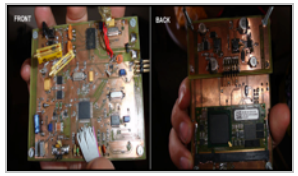










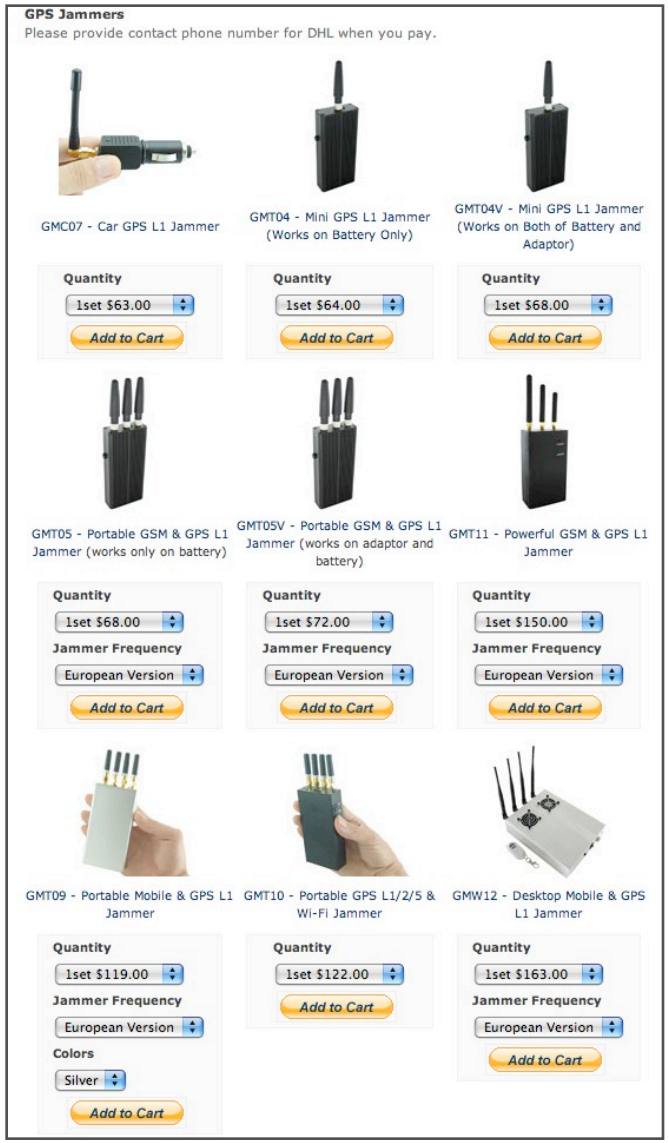


There is a huge danger to customers using this (RFID) technology, if they don't think about security.
-- Lukas Grunwald (creator of RFDump)

GPS: Not a Security Technology

- The private sector, foreigners, and 90+% of the federal government must use the civilian GPS satellite signals.
- These are unencrypted and unauthenticated.
- They were never meant for critical or security applications, yet GPS is being used that way!
- GPS signals can be: Blocked, Jammed, or Spoofed

GPS (and Other) Jamming



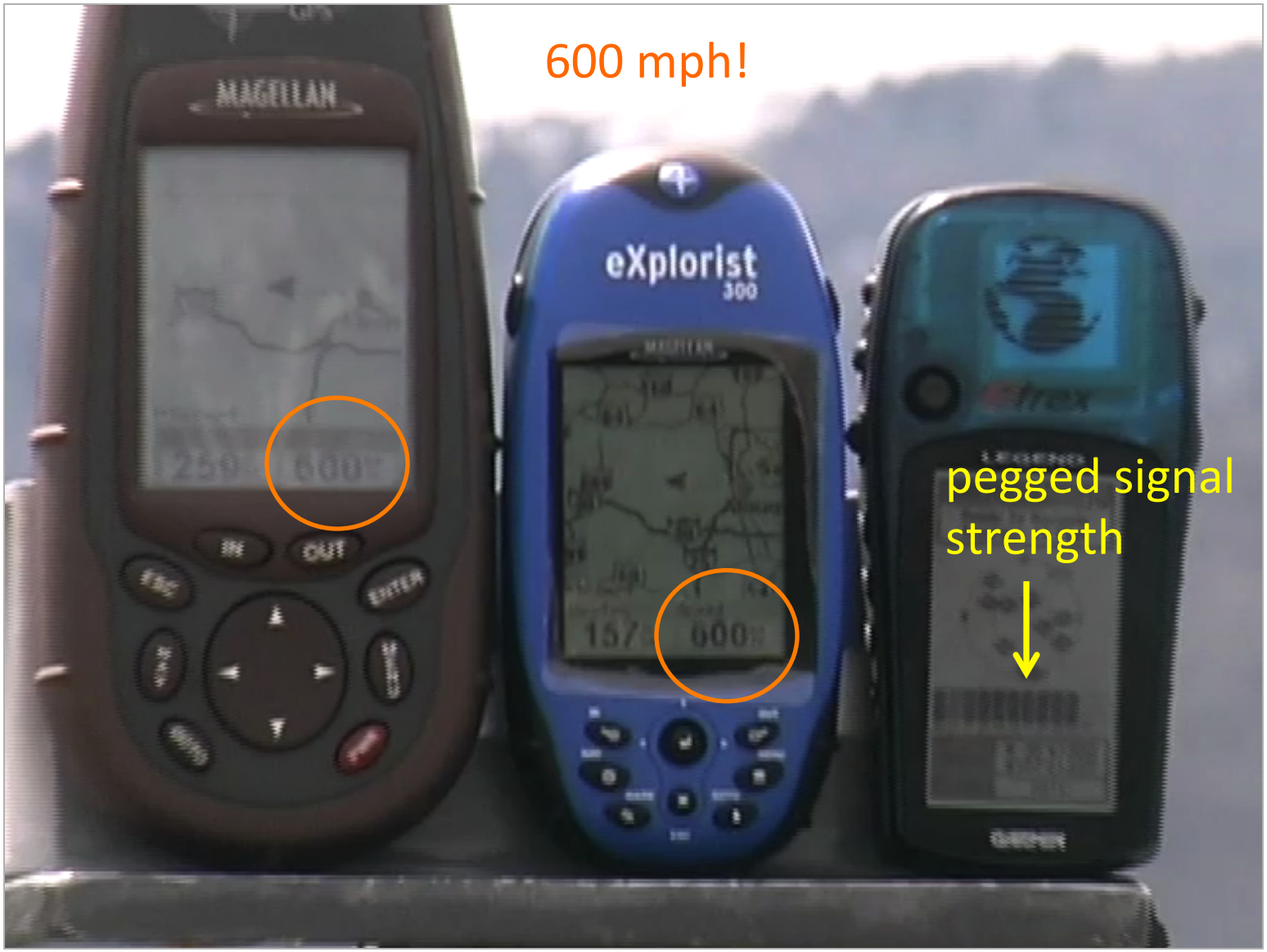
For the third goal, I blame the ball.
-- Saudi goalkeeper Mohammed Al-Deayea

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.
- Spoofing can be detected for ~$15 of parts retail (but there's no interest).

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

Facts About Security Devices & Systems

For most security devices (including biometrics and access control devices), it's easy to:

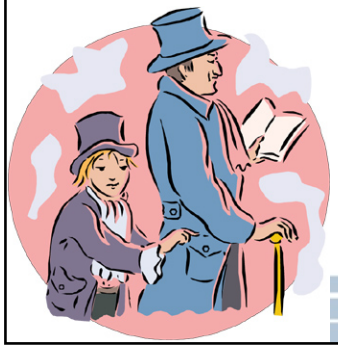
- clone the signature of an authorized person
- do a man-in-the-middle (MM) attack
- access the password or key
- copy or tamper with the database
- "counterfeit" the device
- install a backdoor
- replace the microprocessor
- tamper with the software

Backdoor, MM, or Counterfeit Attacks

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

Most security devices can be compromised in 15 seconds (at the factory or vendor, on the loading dock, in transit, in the receiving department, in storage, before or after being installed).

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

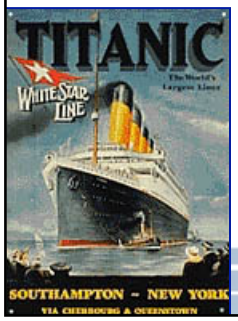


> The Air Force is pleased with the performance of the C-5A cargo plane, although having the wings fall off at eight thousand hours is a problem.
> -- Major General Charles F. Kyunk, Jr.

Security of Security Products

Why High-Tech Devices & Systems Are Usually Vulnerable To Simple Attacks

- Many more legs to attack.
- Users don't understand the device.
- The "Titanic Effect": high-tech arrogance.
- Still must be physically coupled to the real world.
- Still depend on the loyalty & effectiveness of user's personnel.
- The increased standoff distance decreases the user's attention to detail.
- The high-tech features often fail to address the critical vulnerability issues.
- Developers & users have the wrong expertise and focus on the wrong issues.



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

Blunder: Thinking Engineers Understand Security

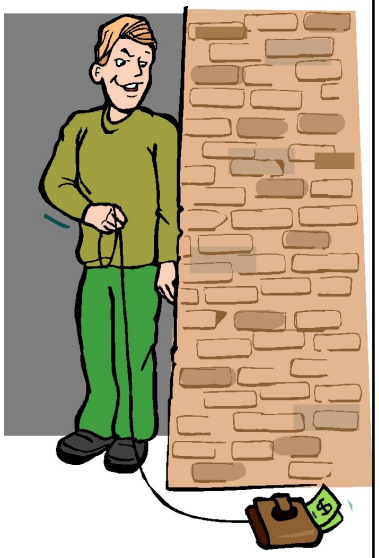
Engineers (including packaging engineers)...

- ...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
- …tend to think technologies fail randomly, not by deliberate, intelligent, malicious 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 can make them easy to attack

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

What Can We Do Better?

- ✓ More skeptical, critical, and imaginative thinking.
- ✓ Avoid confusing Threats with Vulnerabilities, & Inventory with Security.
- ✓ Bribe people!



- ✓ Stop using layered security (security in depth) as a cop out.

Cynic's Dictionary

layered security: We're desperately hoping that multiple layers of lousy security will somehow magically add up to good security.

What Do We Need To Do Better?

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)

- ✓ Be proactive to the Insider Threat—including mitigating disgruntlement and educating employees about social engineering.
- ✓ Less prevention, more mitigation & resilience!
- ✓ Posters with eyes.
  See Biology Letters **2**, 412-414 (2006).

- ✓ Embrace the new security paradigms.

Changing Security Paradigms

Old Paradigm	New Paradigm
Security is easy & binary.	It's not.
Vulnerabilities are bad news.	Vulnerabilities are good news.
High Tech is a silver bullet.	Technology can help but security is about people.
Think like bureaucrats & good guys.	Think like the bad guys.
There is one right answer. Fake rigor & reproducibility. Accountability through fear, scapegoating, & firing people.	We embrace creativity, flexibility, uncertainty, criticism, questions. We watch for the dangers of cognitive dissonance. We motivate & encourage good security practice.
Compliance-based security.	We must do more th…

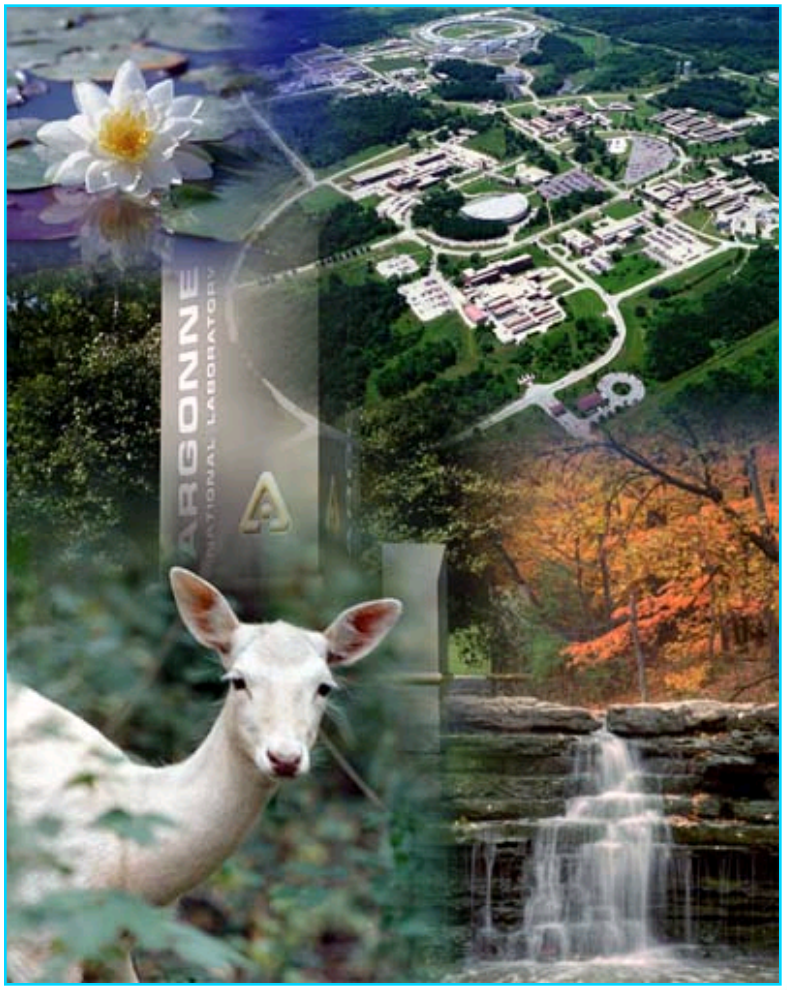
Advice to children crossing the street: Damn the lights! Watch the cars. The lights ain't never killed nobody!
-- Moms Mabley (1894-1975)

Changing Security Paradigms

Old Paradigm	New Paradigm
Security Pros provide security.	Employees, contractors, vendors, and visitors provide security. Security Pros help.
Metrics: Knowing & following the security rules.	Metrics: Being proactive, showing individual initiative, being creative and resourceful during "What if?" exercises.
Productivity & Security are enemies.	Security is harmed when Productivity is harmed.
Security gets confused with Control, Big Brother, and Security Theater.	Security is harmed by Security Theater, and when Privacy & Civil Liberties are

One should always play fairly when one has the winning cards.
-- Oscar Wilde (1854-1900)

For More Information...



~250 related papers, reports, and presentations (including this one) are available from
ROGERJ@ANL.GOV

Argonne NATIONAL LABORATORY

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)

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

VAT

Argonne National Laboratory

~$738 million annual budget
1500 acres, 3400 employees, 4400 facility users, 1500 students
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