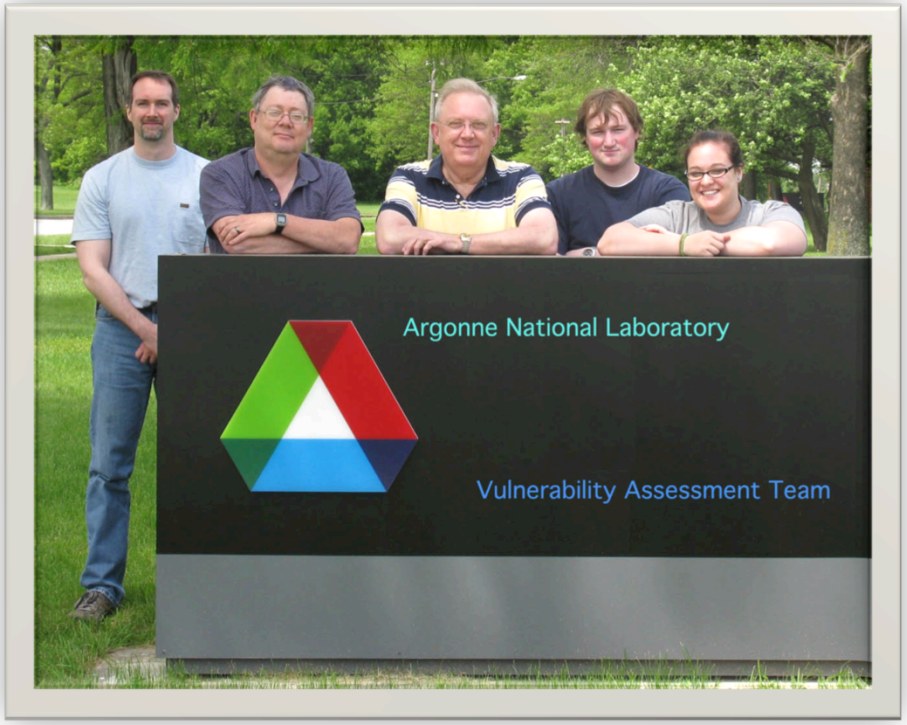
Vulnerability Assessments, Physical Security, and Nuclear Safeguards

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

Vulnerability Assessment Team (VAT)



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

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

Sponsors

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

Domestic vs. International Nuclear Safeguards

I was taking a bath in a Leningrad hotel when the floor concierge yelled that she had a cable for me. "Put it under the door," I cried. "I can't," she shouted. "It's on a tray!"

-- Anthony Burgess

Domestic Nuclear Safeguards

- is MPC&A
- is a traditional security application:
  - ✓ the "good guys" own the assets & facilities
  - ✓ the (unknown) adversaries are a small number of individuals with limited resources
  - ✓ secrecy is allowed
  - ✓ the attacks must often be quick
  - ✓ the "good guys" can use the facility infrastructure, personnel, & training to counter the adversary

International Nuclear Safeguards

- is treaty monitoring, not MPC&A
- is not a traditional security application—everything is backwards:
  - ✓ the adversary owns the assets & facilities
  - ✓ the (known) adversary is the host nation and can deploy world-class technology & resources to defeat the safeguards
  - ✓ the "good guys" aren't present most of the time
  - ✓ no secrecy—details must be negotiated & transparent
  - ✓ the attacks can often be leisurely
  - ✓ the adversary can use the facility infrastructure, personnel, & training to help defeat the safeguards

Domestic vs. International Nuclear Safeguards

The differences are so extreme, we must be suspicious when similar hardware, strategies, expertise, and personnel are used.

These differences are widely recognized in theory…but not in practice.

Other International Safeguards Problems

- Cooperative Nuclear Safeguards gets confused with International Nuclear Safeguards
- Denial & cognitive dissonance
- Vulnerability assessments that are weak, non-existent, or done too late to make changes
- Hijacking of the term & concept of “Transparency”
- Lots of bureaucrats & engineers who don’t understand physical security

Other International Safeguards Problems

- Technologists push their pet technology rather than solving the problem
- Diplomats want simple solutions
- Safeguards programs tend to have a life of their own beyond true needs
- Details of inspections & safeguards can become bones of geopolitical contention
- Disparate national and security cultures

Other International Safeguards Problems

- Poor tamper/intrusion detection in general
- Thinking a mechanical tamper switch provides effective intrusion detection
- Wishful thinking about information barriers
- No background checks on IAEA inspectors!

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

Warning!

You should always assume a security or safeguards device or system can be easily defeated, because it usually can.

Effective security & safeguards are very difficult.
We can only get good at them if we understand this.

Be wary of silver bullets—they don't exist!

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

Security Theater & Ceremonial Safeguards

Harry Potter this, Harry Potter that! I'd never even heard of Harry Potter until the book came out.
-- Caller, BBC Radio 5 Live

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

Common Mistakes in Physical Security & Nuclear Safeguards

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

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.

If you think that technology can solve your security problems then you don't understand your problems and you don't understand the technology.
-- Bruce Schneier

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
- …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

Blunder: Wrong Assumptions about Counterfeiting

- Usually much easier than developers, vendors, & manufacturers claim.

- Often overlooked: The bad guys usually only needed to mimic only the superficial appearance of the original and (maybe) some of the apparent performance.

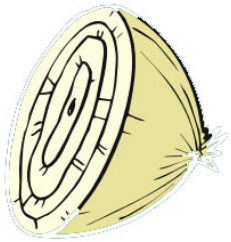
Sincerity is everything. If you can fake that, you've got it made.
-- George Burns (1885-1996)

Data Encryption/Authentication

At least currently, data encryption/authentication should have only a marginal role to play in international safeguards because:

- not conducive to transparency & international cooperation
- of minimal use given our poor physical security & tamper/intrusion detection
- the data remanence problem hasn't been solved
- pointless if you can't believe the sensors, the raw data, & the data analysis in the first place
- the adversary may have access to the plaintext so he can go beyond ciphertext-only crytoanalysis
- it's easy to eavesdrop on keys and passwords

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



- Increases complexity.
- Multiple layers of bad security do not equal good security.
- It's unlikely the adversary has to defeat all the layers.
- Often mindlessly applied: the layers are not automatically backups for each other. They may have common failure modes, or even interfere with each other.
- Leads to complacency.
- Tends to be a cop-out to avoid improving security
- Often a knee-jerk response when security hasn't been thought through.
- How many sieves do you have to stack up before the water won't leak through?

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

Blunder: The Band Aide / Kitchen Sink Approach to Security

- Only worry about security at the end
- Arbitrarily slap on a number of features, sensors, or fad technologies in hopes the whole mess somehow results in good security.

Never buy beauty products from a hardware store. -- Miss Piggy

Confusing Inventory & Security

Inventory

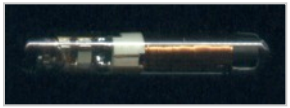
- Counting and locating stuff
- No nefarious adversary
- May detect innocent errors by insiders, but not surreptitious attacks by insiders or outsiders.

Security

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

Examples of confusing Inventory & Security

- rf transponders (RFIDs)



- prox cards

- contact memory buttons

- GPS

- Nuclear MC&A

Usually easy to:

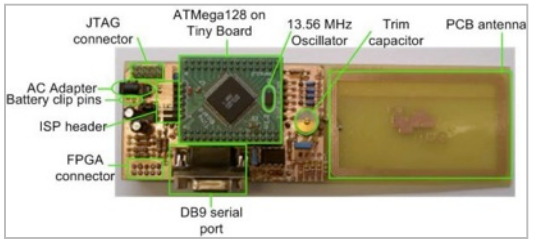
* lift
* counterfeit
* tamper with the reader
* spoof the reader from a distance

Very easy to spoof, not just jam!

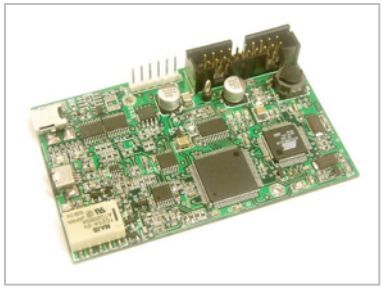
A Sampling of RFID Hobbyist Attack Kits Available on the Internet

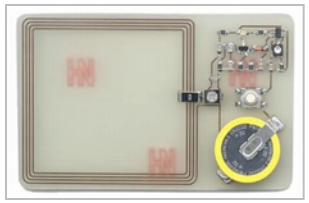
Commercial: $20 Car RFID Clone (Walmart)

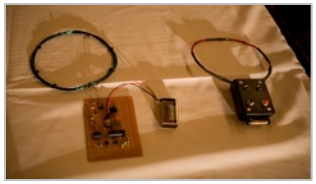
Commercial: Used for "faking RFID tags", "reader development."

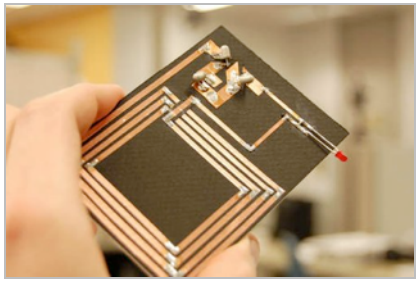


RFID Skimmers, Sniffers, Spoofers, and Cloners; oh my!

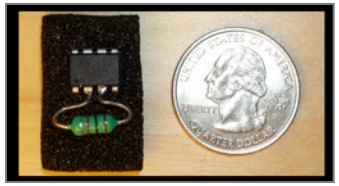


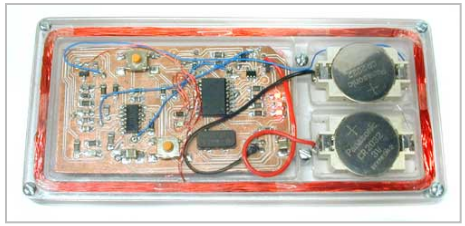


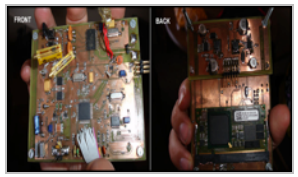




Documents, code, plans needed to build your own: free.







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

(Incidentally, Prox Cards are RFIDs!)

[But then most (all?) access control and biometric devices are easy to defeat.]

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

GPS Jammers

Please provide contact phone number for DHL when you pay.

GMC07 - Car GPS L1 Jammer

Quantity: 1set $63.00

Add to Cart

GMT04 - Mini GPS L1 Jammer (Works on Battery Only)

Quantity: 1set $64.00

Add to Cart

GMT04V - Mini GPS L1 Jammer (Works on Both of Battery and Adaptor)

Quantity: 1set $68.00

Add to Cart

GMT05 - Portable GSM & GPS L1 Jammer (works only on battery)

Quantity: 1set $68.00

Jammer Frequency: European Version

Add to Cart

GMT05V - Portable GSM & GPS L1 Jammer (works on adaptor and battery)

Quantity: 1set $72.00

Jammer Frequency: European Version

Add to Cart

GMT11 - Powerful GSM & GPS L1 Jammer

Quantity: 1set $150.00

Jammer Frequency: European Version

Add to Cart

GMT09 - Portable Mobile & GPS L1 Jammer

Quantity: 1set $119.00

Jammer Frequency: European Version

Colors: Silver

Add to Cart

GMT10 - Portable GPS L1/2/5 & Wi-Fi Jammer

Quantity: 1set $122.00

Add to Cart

GMW12 - Desktop Mobile & GPS L1 Jammer

Quantity: 1set $163.00

Jammer Frequency: European Version

Add to Cart

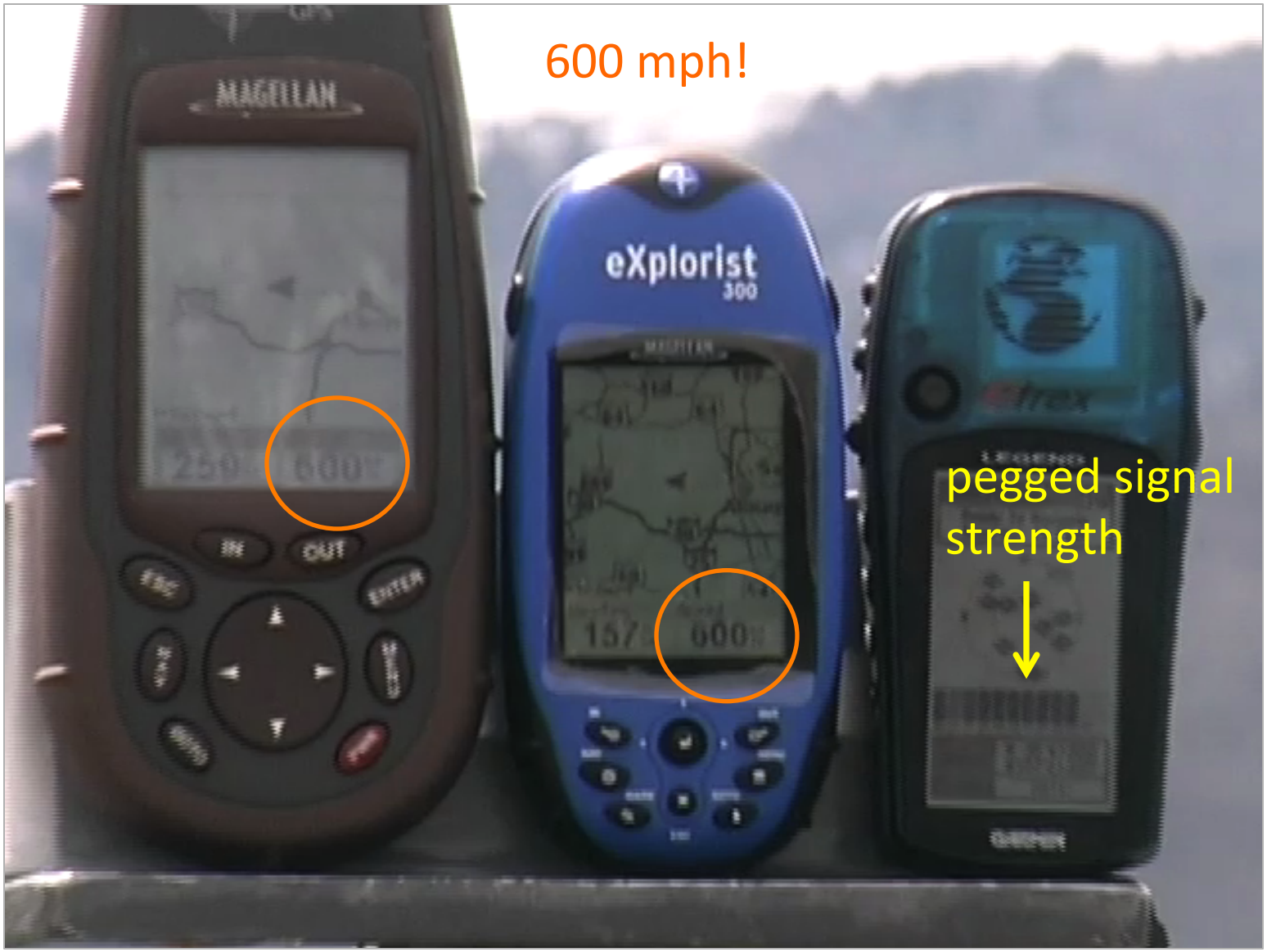
For the third goal, I blame the ball.
-- Saudi goalkeeper Mohammed Al-Deayea

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

Locks & Seals

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

Terminology

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

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

I'd say, "It's a Buttmaster, Your Holiness."
-- Actress Suzanne Somers on how she would respond if the Pope asked her the name of the exercise machine she promotes

Terminology

defeating a seal: opening a seal, then resealing (using the original seal or a counterfeit) without being detected.

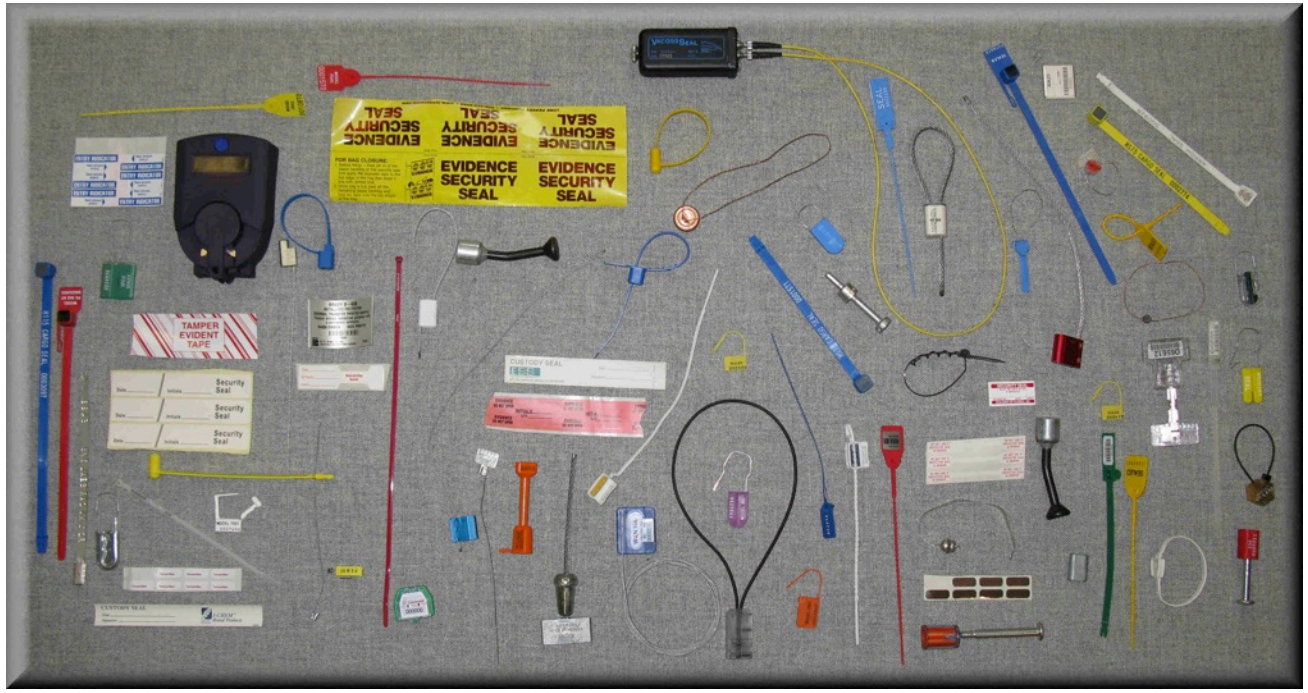
attacking a seal: undertaking a sequence of actions designed to defeat it.

Seal Fact

A seal is not a lock.

Yanking a seal off a container is not defeating it!

Seals



Some examples of the 5000+ seals

Example Seal Applications:

- customs
- cargo security
- counter-terrorism
- nuclear safeguards
- treaty inspections
- banking & couriers
- drug accountability
- records & ballot integrity
- evidence chain of custody
- weapons & ammo security
- IT security
- medical sterilization
- instrument calibration
- tamper-evident packaging
- waste management & HAZMAT accountability

Seal Use Protocol

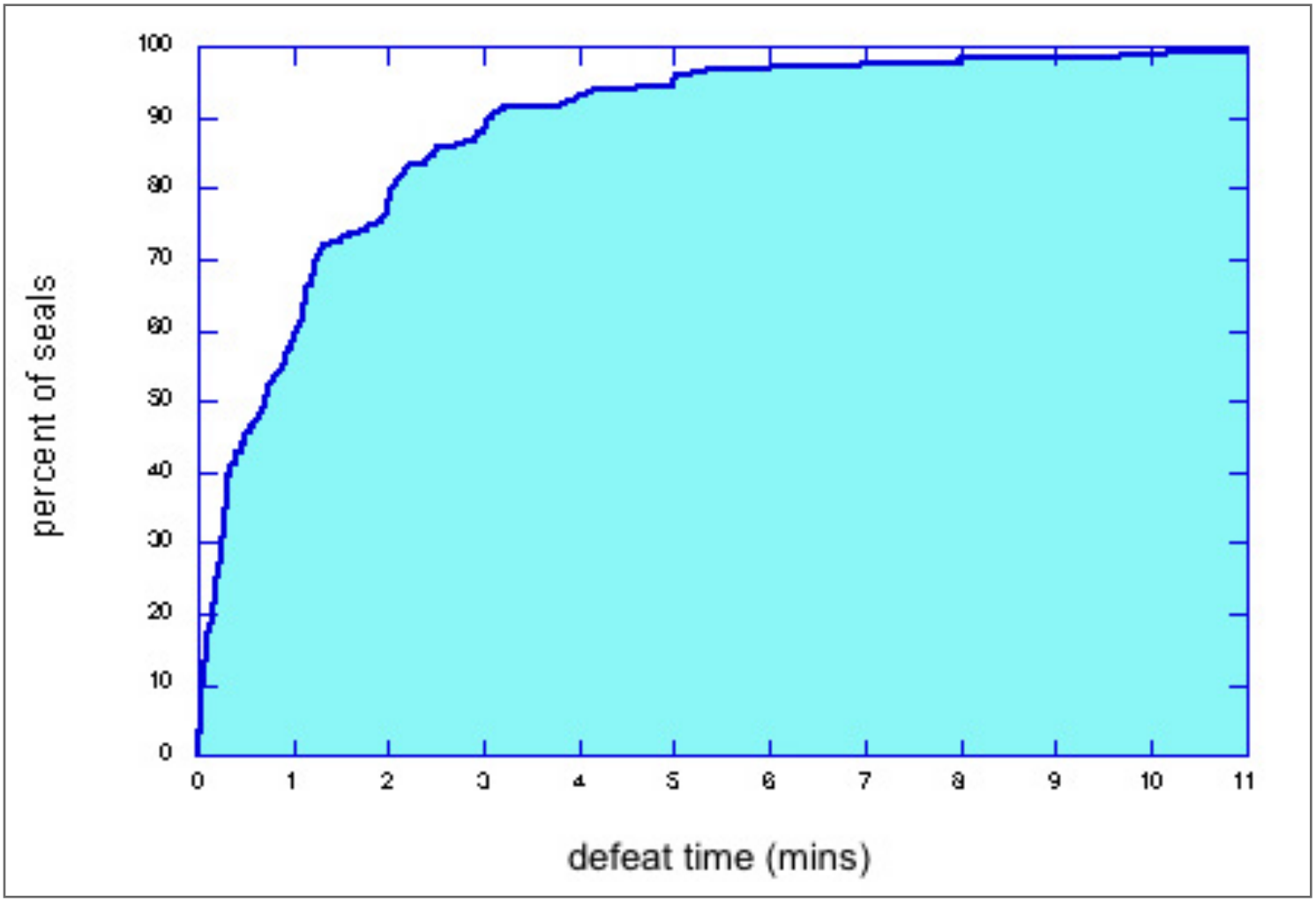
A seal is no better than its formal and informal "use protocol"...

...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.

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



The Good News: Countermeasures

- Most of the seal attacks have simple and inexpensive countermeasures, but the seal installers & inspectors must understand the seal vulnerabilities, look for likely attacks, & have extensive hands-on training.

- Also: better seals are possible!

We're going to turn this team around 360°.
-- Basketball player Jason Kidd

Conventional Seal: Stores the evidence of tampering until the seal can be inspected. But this 'alarm condition' is easy to erase or hide (or a fresh seal can be counterfeited).

Anti-Evidence Seal: When the seal is first installed, we store secret information that tampering hasn't been detected. This is deleted when the seal is opened. There's nothing to erase, hide, or counterfeit.

Don't play what's there, play what's not there.
-- Miles Davis (1926-1991)

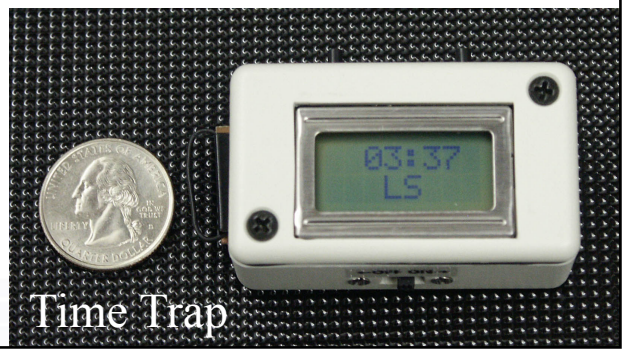
20+ New "Anti-Evidence" Seals

- better security
- no hasp required
- no tools to install or remove seal
- can go inside the container
- 100% reusable, even if mechanical
- can monitor volumes or areas, not just portals
- anti-gundecking and host-inspected seals are possible

Talking Seal

Tie Dye Seal

Chirping Tag/Seal



Time Trap

Access Control

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

Facts About Access Control & Biometric Devices

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, Counterfeit, and MM Attacks

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

As with most security devices, AC devices can usually be compromised in 15 seconds (at the factory or vendor, on the loading dock, in transit, in the receiving department, or after being installed).

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

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

Security of Security Products

Human Factors

You'll meet someone. Someone very special. Someone who won't press charges. -- From the movie *Addams Family Values* (1993)

http://wn.com/Transport_for_London__Whodunnit

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.
- "Change Blindness" (a kind of Perceptual Blindness): observers often fail to notice changes—including blatant ones—even when the changes are expected.

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

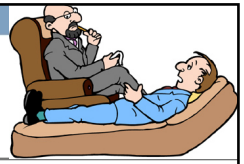
Consequences for Security

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

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

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

Largely Unstudied Human Factors in Security



- Two-Person Rule
- Security Culture & Security Climate
- Correlations between employee attitudes & the rate of security incidents
- Reducing security guard turnover
- The psychology of seal inspection
- Countermeasures to perceptual blindness
- Human factors in nuclear safeguards inspections
- Mitigating the Insider Threat

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)

Unconventional Approaches to Verification & Dismantlement

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)

Transparent, Negotiable, Reliable Video Verification for Treaty Inspection

Relatively low-tech ways to make faking live streaming video difficult in real-time.

Live Verify: Show that the video signals are real-time, not pre-recorded.

Local Verify: Show they originate within at least a few km of the monitored nuclear facility (based on time of flight).

Time of flight of electronic signals down a wire: 20 cm per nsec

Video bandwidth: 27-140 MHz
(37 nsec → 7 meters to 7 nsec → 1.4 meter)

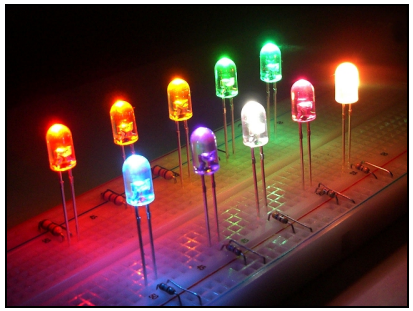
Live & Local Video Verify

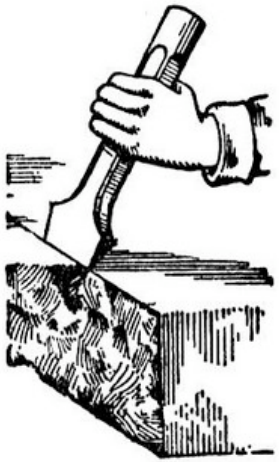
Works best if the inspectors are a few km outside the facility, recording the live video.

They can occasionally enter the facility for in-person inspections.

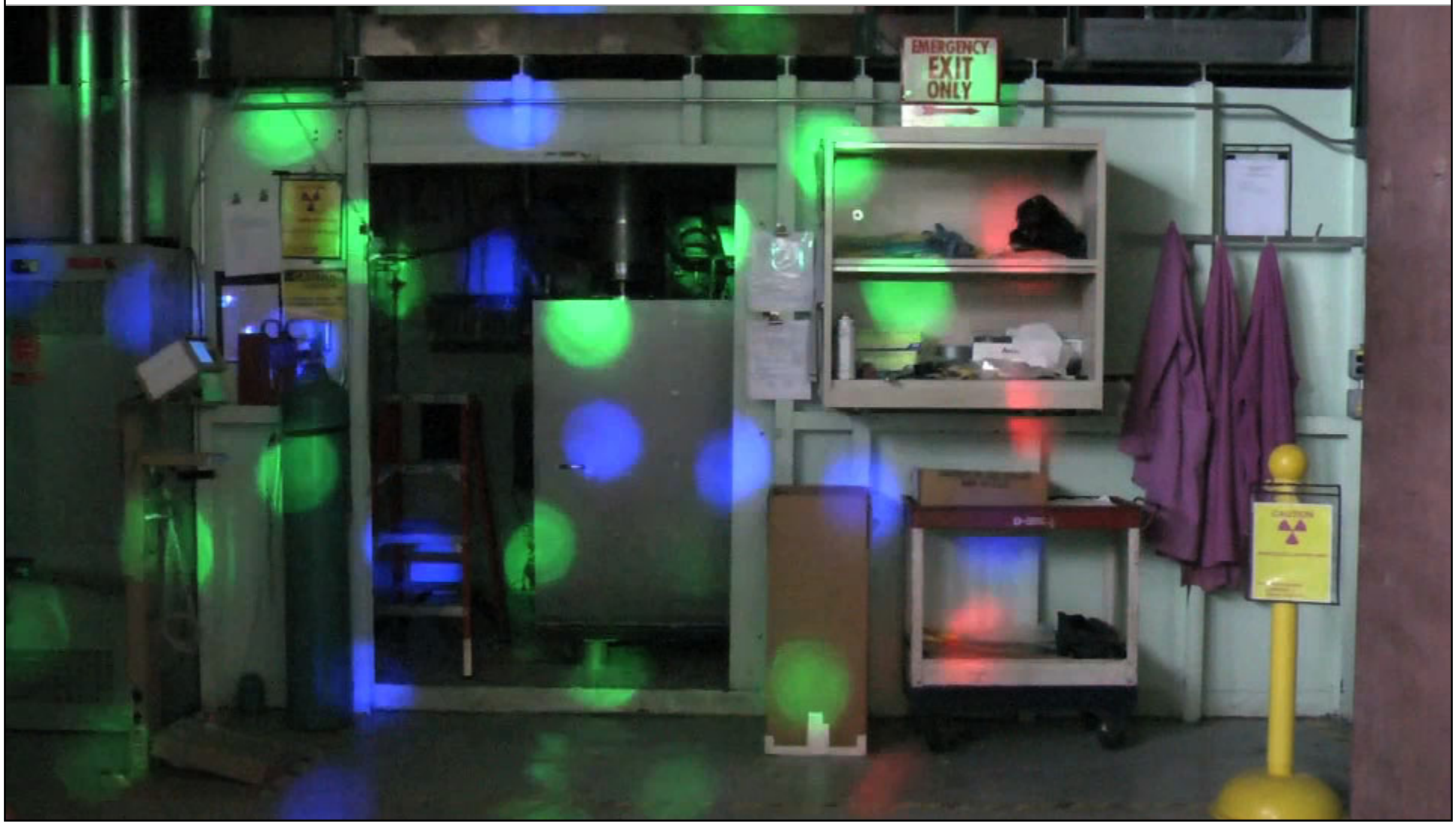
Recorded live video can be analyzed later (frame by frame, pixel by pixel) for evidence of fakery.

Challenge-Response Live Video

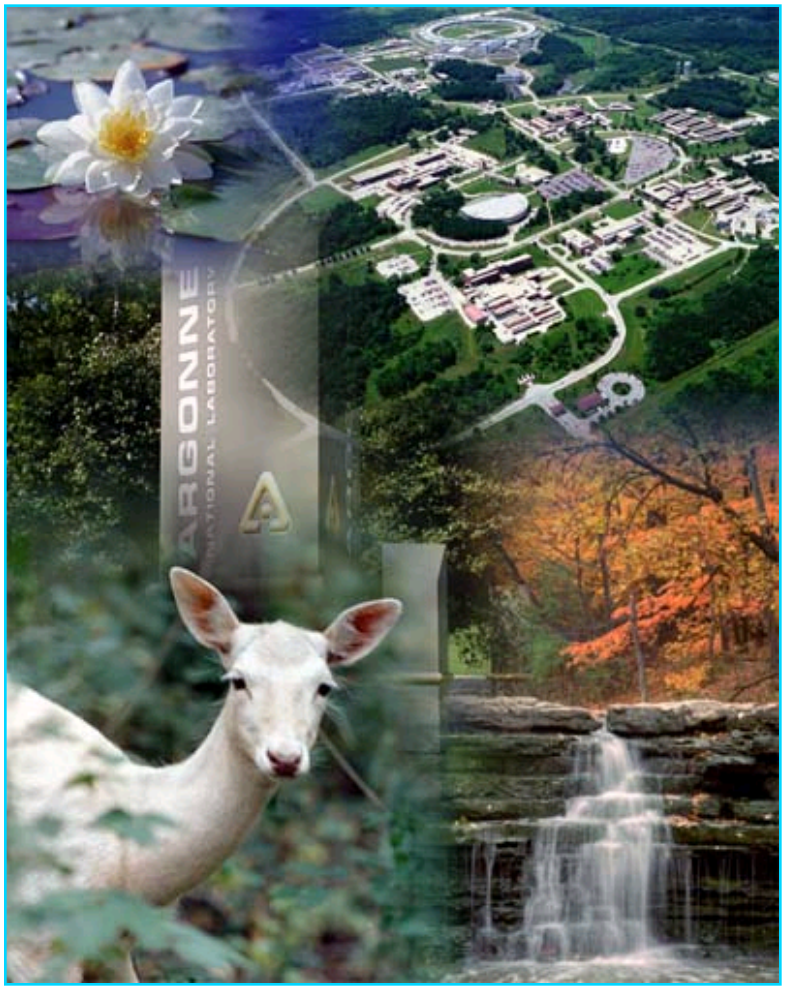




Disco Verification



For More Information...



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

Argonne NATIONAL LABORATORY

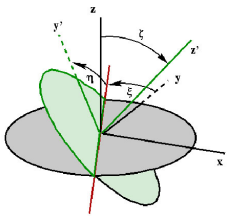
If you look for truth, you may find comfort in the end; if you look for comfort you will get neither truth nor comfort…only soft soap and wishful thinking to begin, and in the end, despair.
-- C.S. Lewis (1898-1963)

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

VAT

supplemental material not part of the presentation…

Adversarial Vulnerability Assessments



- Perform a mental coordinate transformation and pretend to be the bad guys. (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."

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

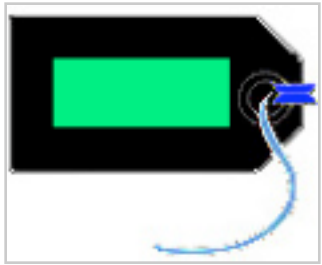
I told my psychiatrist that everyone hates me. He said I was being ridiculous--everyone hasn't met me yet.
-- Rodney Dangerfield (1921-1997)

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

Terminology

tag: an applied or intrinsic feature that uniquely identifies an object or container.

<u>types of tags</u>



inventory tag (no malicious adversary)

*security tag (counterfeiting & lifting are issues)

*buddy tag or token (only counterfeiting is an issue)

anti-counterfeiting (AC) tag (only counterfeiting is an issue)

lifting: removing a tag from one object or container and placing it on another, <u>without being detected</u>.

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…"