Physical Security for Cyborgs

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

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

VAT

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 detailed vulnerability assessments on hundreds of different security devices, systems, & programs.

Sponsors

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

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

Facts About Locks

1. Locks are meant to delay, complicate, and discourage unauthorized access.

2. All locks can be defeated quickly, even by sufficiently motivated amateurs.

3. Ways to defeat locks include picking, bumping, rifling, jiggling a blank key, drilling out the lock, attacking the electronics, etc.

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

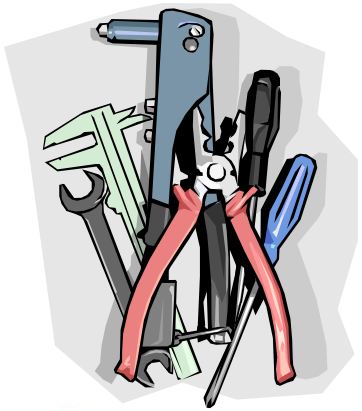
Blunder: Cheap Locks on Security Hardware

Facts About Access Control Devices

For most AC systems (including biometrics), it's easy to tamper with the:

- power
- software
- hardware
- database
- tamper switch
- microprocessor
- communications
- key or password
- door lock or turnstile

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




Visitor
Visitor
Your Logo Here VISITOR
Name:
Company:
Date: Time In:
V
Your Logo Here VISITOR
Name:
Company:
Date: Time In:
V
Your Logo Here
Date:
VISITOR
Name:
Company:
Visiting:
VOID
Your Logo Here
Date:
VISITOR
Name:
Company:
Visiting:

Facts About Access Control Devices

For most AC systems (including biometrics), it's easy to:

- clone the signature of an authorized person
- do a man-in-the-middle (MM) attack
- access the database or password
- "counterfeit" the device
- install a backdoor

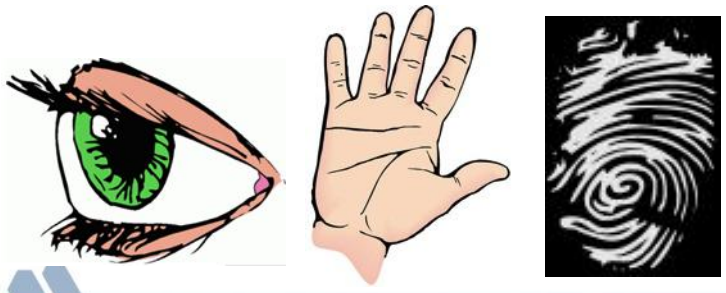
The first time we ever made love, I said, "Am I the first man who ever made love to you?" She said, "You could be. You look damn familiar.
-- Ronnie Bullard

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

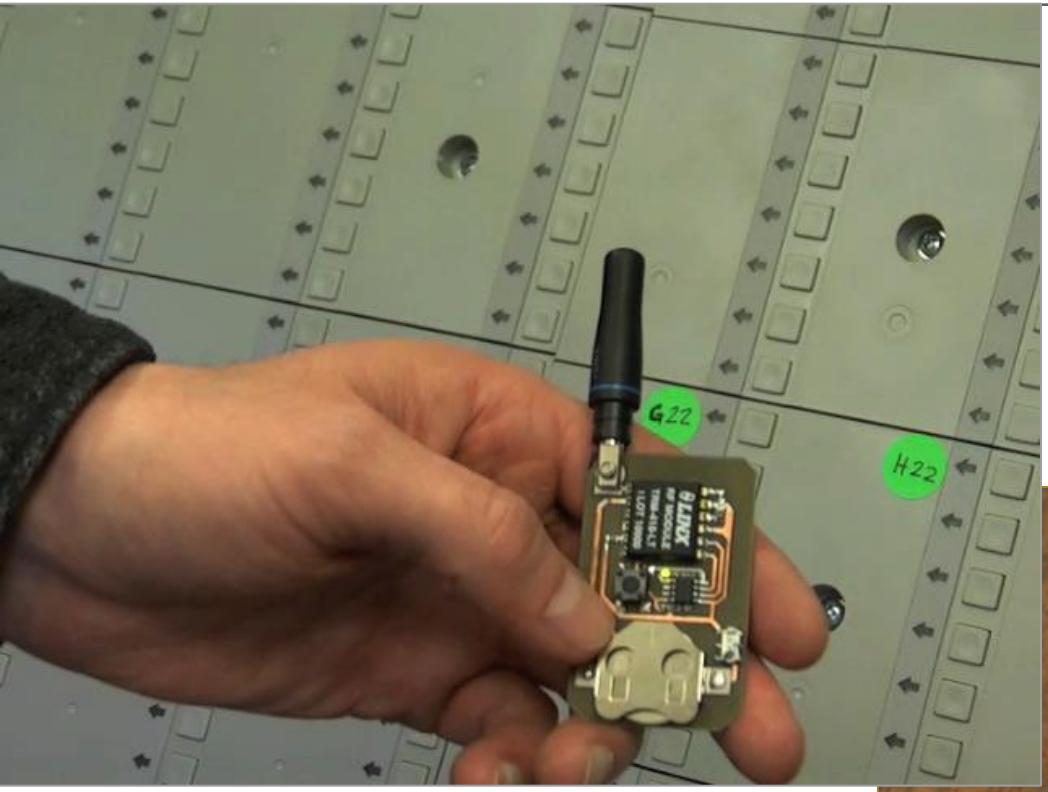


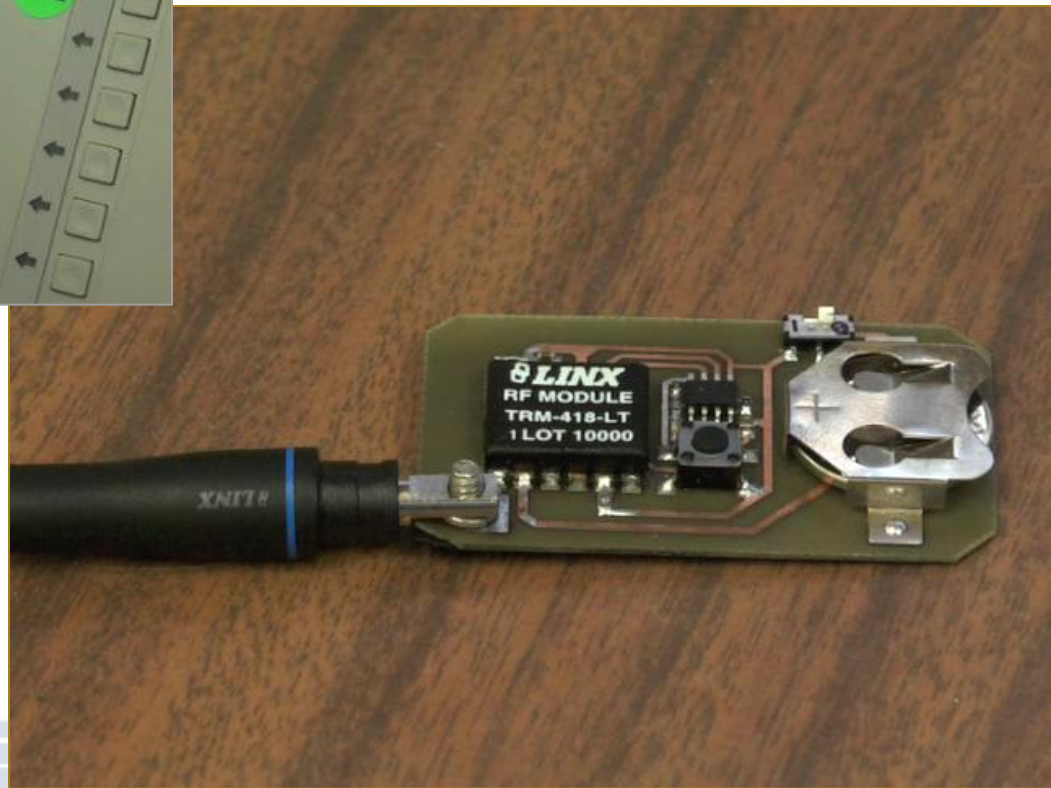
Sometimes security implementations look fool proof. And by that I mean proof that fools exist.

-- Dan Philpott

Security of Security Products

Remote Toggling On/Off of Cheating





I have been called dumb, crazy man, science abuser, Holocaust denier, villain of the month, hate-filled, warmonger, Neanderthal, Genghis Khan, and Attila the Hun. And I can just tell you that I wear some of those titles proudly.

-- Oklahoma Senator James Inhofe

Blunder: Wrong Assumptions about Counterfeiting

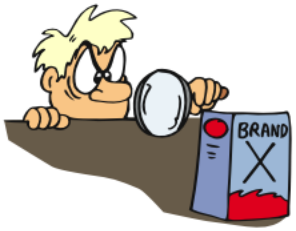
- Usually much easier than developers, vendors, & manufacturers claim.
- Often overlooked: The bad guys usually only needed to mimic only the superficial appearance of the original and (maybe) some of the apparent performance of the product or the security device, not the thing itself, or its real performance.
- Rarely is full reverse engineering necessary.

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

Access Control (AC)

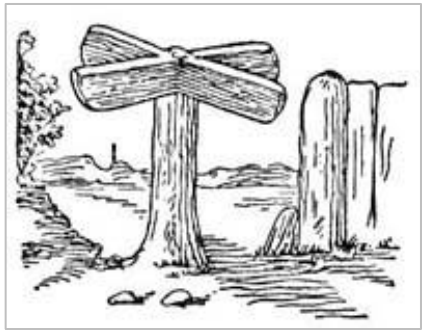
Question: Is that really your AC device, or is it a counterfeit or a tampered version?
(…perhaps one that lets anybody in, with occasional random false rejects to look realistic.)

- 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 would an adversary 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

Terminology

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

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

Terminology (con't)

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.

Radisson Welcomes
Emerging Infectious Diseases

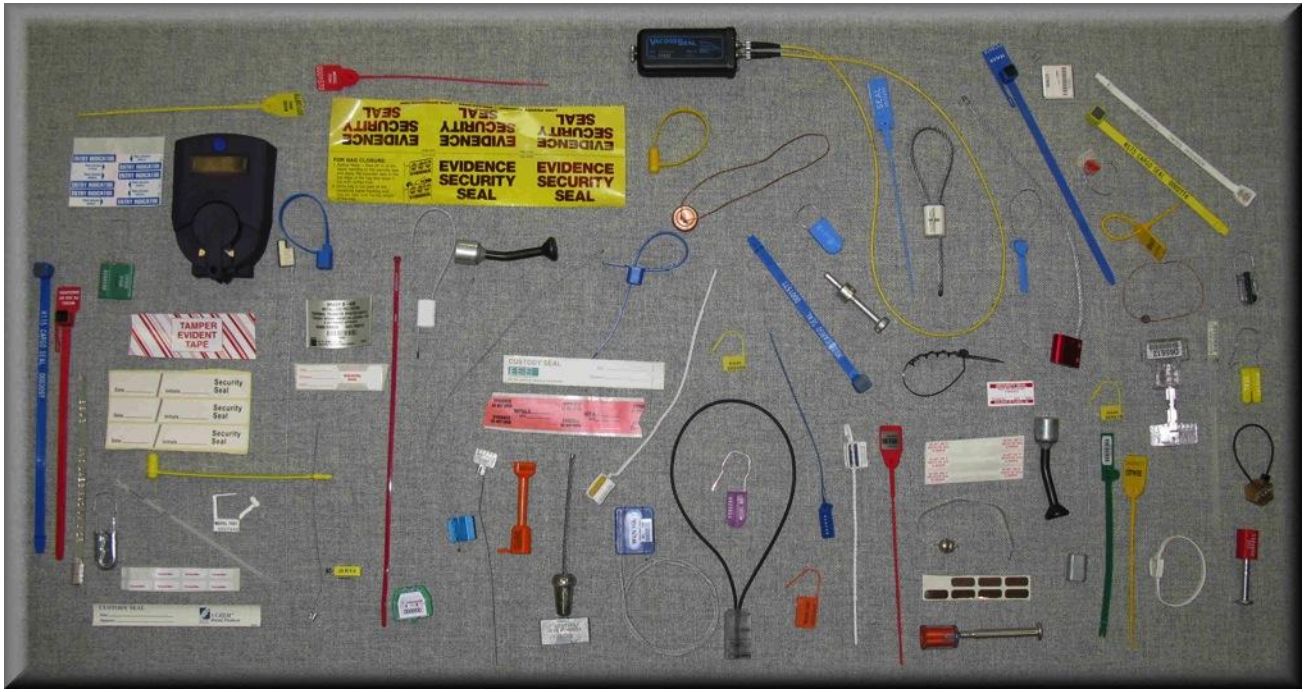
-- Sign outside a Radisson Hotel

Seal Fact

A seal is not a lock.

Yanking a seal off a container is not defeating it!

Seals

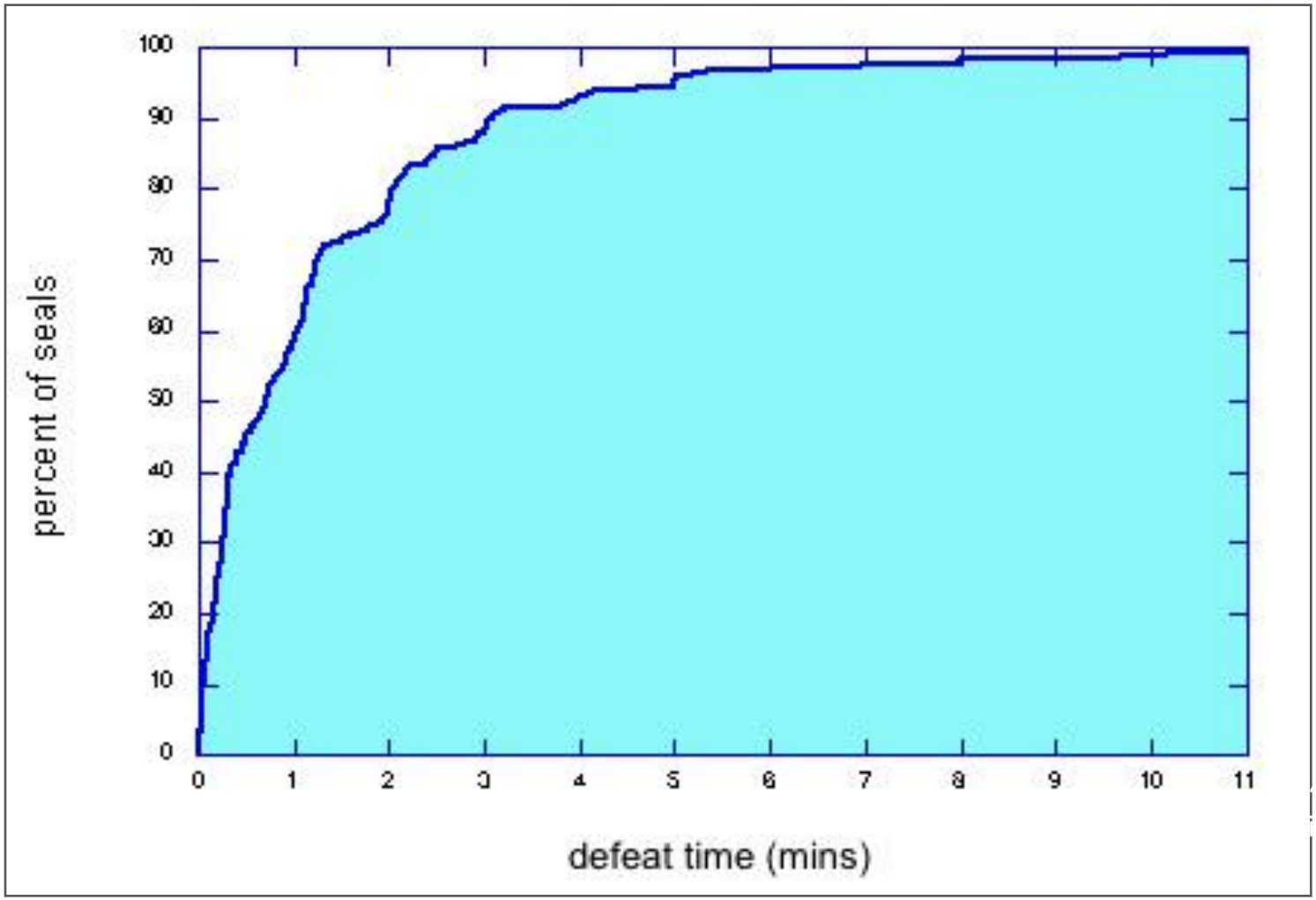


Some examples of the 5000+ commercial seals

Example Seal Applications:

- customs
- cargo security
- counter-terrorism
- nuclear safeguards
- counter-espionage
- 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

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



Summary of Seals Results

parameter	mean	median
attack time	1.4 mins	43 secs
cost of tools & supplies	$78	$5
marginal cost of attack	62¢	9¢
time to devise successful attack	2.3 hrs	12 mins

Seal Facts

1. All seals need a unique identifier (like a serial number).

2. 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.

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

4. Adhesive label seals do not provide effective tamper detection, even against amateurs.

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.

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.
- If the recipient doesn't know what the seal and envelope (or container) is supposed to look like, you are wasting your time. [This information cannot accompany the seal.]

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.

- Full adhesion requires 48+ hours. A PSA seal is particularly easy to lift the first few minutes to hours. Heat can help.

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

Inspection

- Smell can be a powerful tool for detecting attacks. Or use a hand-chemical “sniffer” ($150-$9K).

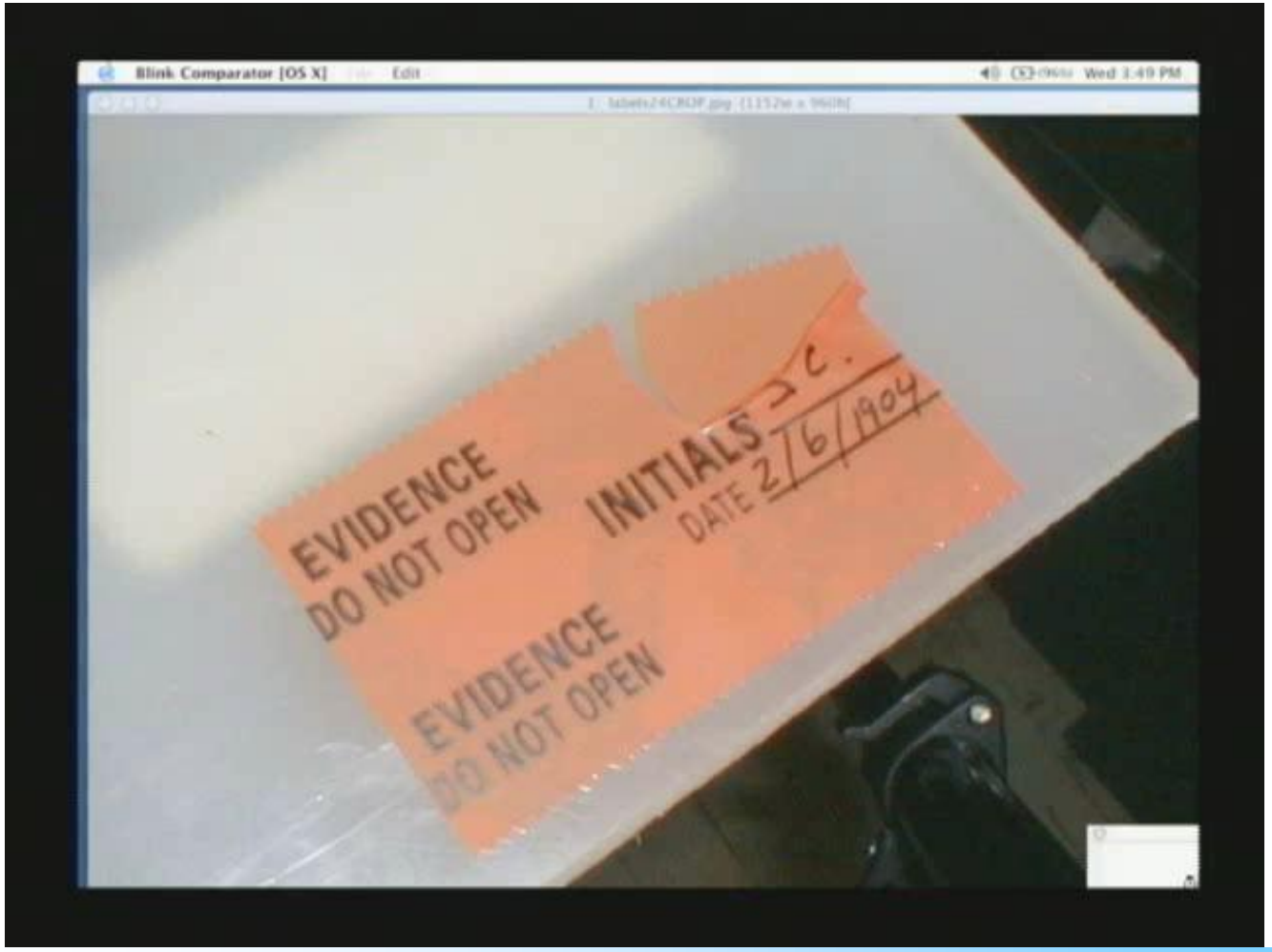
- (As with all seals) compare the seal side-by-side with an unused seal you have protected. Check size, color, gloss, font, & digit spacing/alignment.

- Carefully examine the surface area outside the perimeter of the label seal.

- **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.



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!

> The prophet who fails to present a bearable alternative and yet preaches doom is part of the trap he postulates.
>
> -- Margaret Mead (1901-1978)

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. When the seal is opened this "Anti-Evidence" is quickly erased. There's nothing left 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"—automatically verifying that the seal was inspected

Talking Cargo Seal

Tie Dye Seal


Chirping Tag/Seal

Time Trap

Tampering with 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)

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)

- contact memory buttons

- GPS

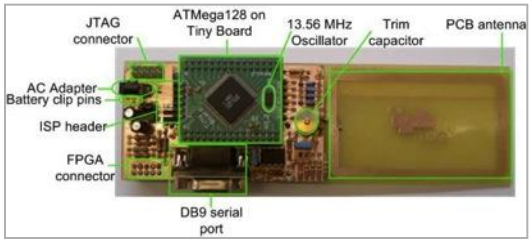
Usually easy to:
* lift
* counterfeit
* tamper with the reader
* spoof the reader from a distance

Very easy to spoof, not just jam!

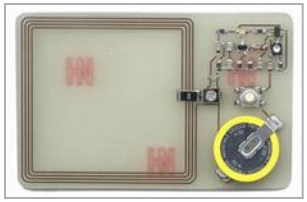
A Sampling of RFID Hobbyist Attack Kits Available on the Internet

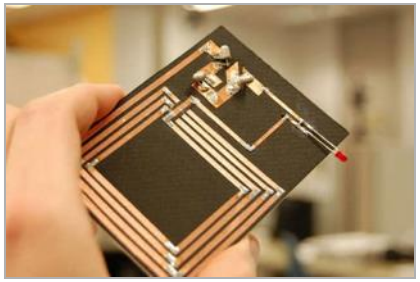
Commercial: $20 Car RFID Clone (Walmart)

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

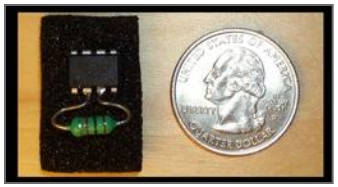


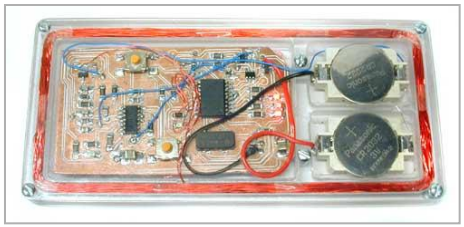
RFID Skimmers, Sniffers, Spoofers, and Cloners; oh my!

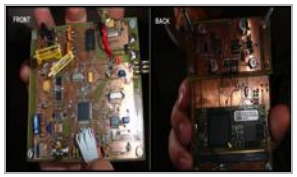




Documents, code, plans needed to build your own: free.







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

Facts About Prox Cards

- All the vulnerabilities of regular access control technologies.
- Plus, they are RFIDs (so they're *really* not secure)!

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

GPS: Not a Security Technology

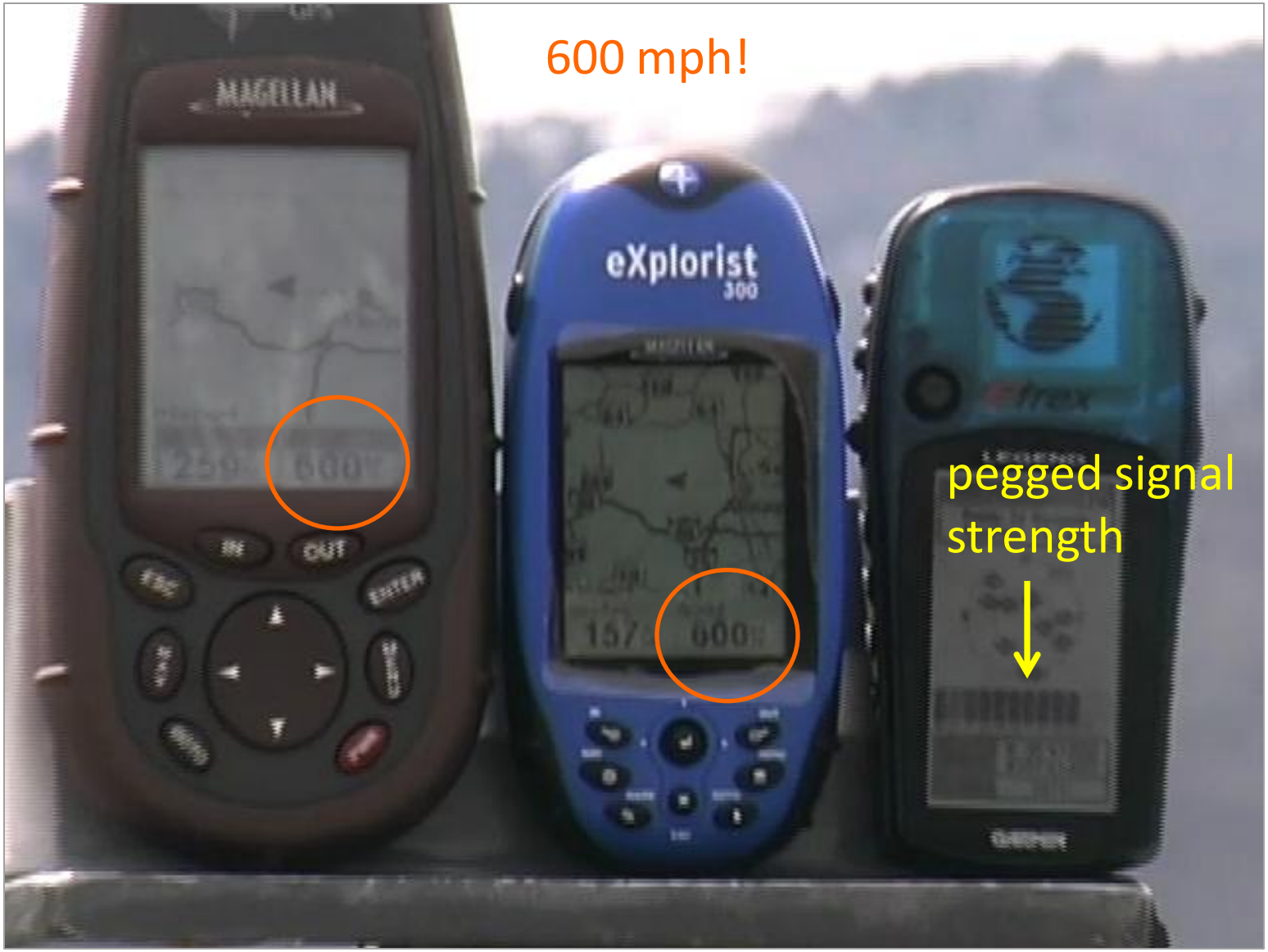
- The private sector, foreigners, and 90+% of the federal government must use the civilian GPS satellite signals.
- These are unencrypted and unauthenticated.
- They were never meant for critical or security applications, yet GPS is being used that way!
- GPS signals can be: Blocked, Jammed, or Spoofed

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

Blunder: Poor Insider Threat Countermeasures

- Employee disgruntlement is a risk factor for workplace violence, sabotage, theft, espionage, and employee turnover (which is not good for security).

- While disgruntlement is certainly not the only insider threat issue, it is an important one.

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: Poor Insider Threat Countermeasures

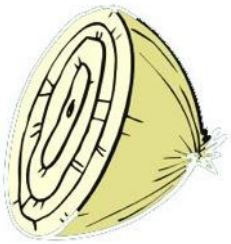
- Phony or non-existent grievance & complaint resolution processes (Note: if good, they'll be used a lot)

Employee perceptions are the only reality!

- Phony or non-existent anonymous whistle blower program & anonymous tip hot line
- No constraints on bully bosses or HR tyranny
- Emphasis on being "fair" instead of treating EVERYBODY well
- Not managing expectations.

Wow…if only a face could talk!
-- Sportscaster John Madden
during Super Bowl coverage

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



- Increases cost & 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
- How many sieves do you have to stack before the water won't leak through?

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

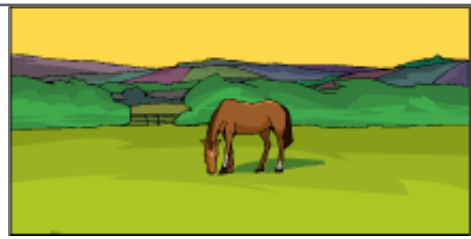
So Why So Much Bad Physical Security?

- Security Theater is easy, thinking and Real Security is hard
- Committees, bureaucrats, & other knuckleheads are in charge
- People & organizations aren't used to thinking critically about it
- Physical Security as a "Taking Out the Garbage" slam dunk thing
- "If it's important, somebody must have thought it through" Myth
- Lots of hype, snake oil, & bad products
- Blind faith in precedence and "authorities"
- Physical security is not a well developed field

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)

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.

Harry Solomon: I didn't have enough experience to sell hot dogs, so they made me a security guard.

-- *Third Rock from the Sun*

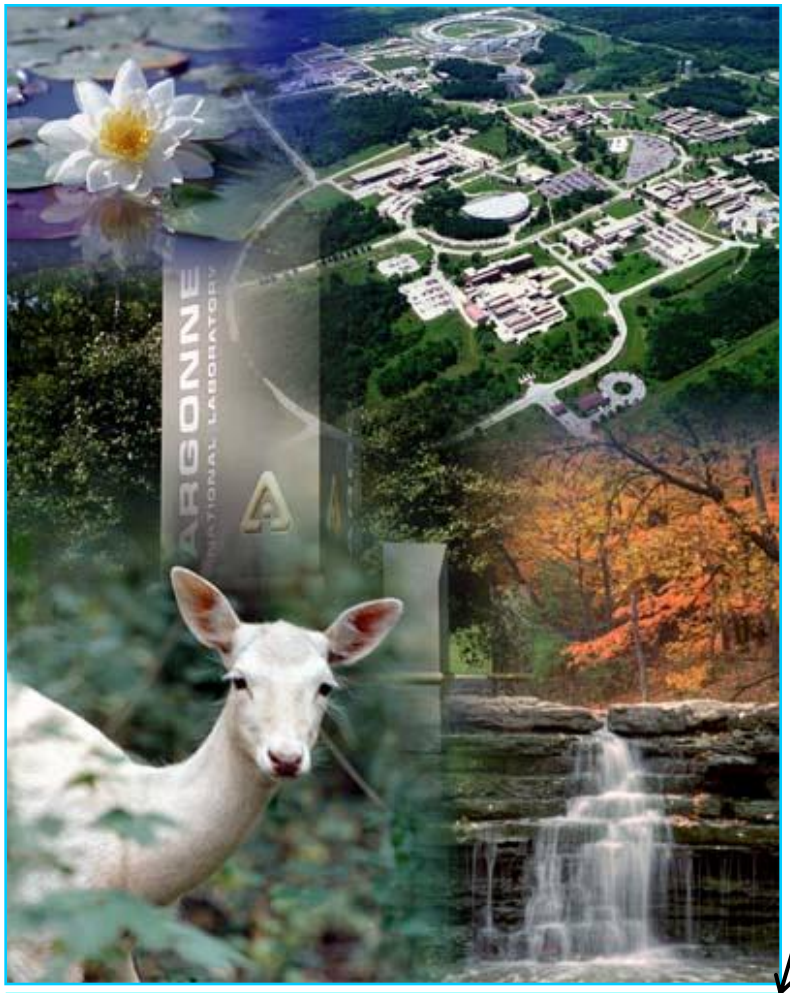
What Physical Security Could Learn From Cyber Security

- ✓Vulnerabilities are numerous, ubiquitous, inevitable, & constantly evolving
- ✓They don't automatically mean somebody has been screwing up
- ✓Scapegoating isn't very helpful
- ✓Security is not binary, it's a continuum
- ✓Customer focus: productivity has to be an issue in security
- ✓How to motivate good security practice among regular employees
- ✓Past criminals can make good consultants
- ✓Technology is not a panacea—security is really about people
- ✓Regular employees *are* the security, not the enemy of security
- ✓Lose the coat & tie!

What Cyber Security Could Learn From Physical Security

- ✓Discipline, Leadership, Organizational Skills, & Being a Team Player
- ✓Understanding where you fit into the organization
- ✓Techniques for dealing with upper management
- ✓Making the business case for security
- ✓Effective project management & budgeting; meeting deadlines
- ✓Females can be very effective security professionals
- ✓Street smarts, people skills, & a good understanding of psychology
- ✓Dealing with Social Engineering & the Insider Threat
- ✓Realization that good cyber security requires good physical security
- ✓Maybe that T-shirt could be washed once in a while!

For More Information...



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

Related papers, reports, and presentations are available from rogerj@anl.gov

(includes Security Maxims)

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)

Supplemental material…

Talking Truck Cargo Seal: An Anti-Evidence, Audio Seal

Seal: $15 of parts (retail)
Reader: $40 of parts (retail)

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)

Talking Truck Cargo Seal: Sample Slogans

- At Least One Fire Extinguisher per Dozen Trucks
- The Best People You Can Hire for $8 an Hour
- The Center Lane Marker is Only a Suggestion
- Amphetamines Aren’t for Amateurs
- We Break for Small, Furry Animals
- Not in Front of the Teamsters!
- Mad Max Works for Us
- We Eat Our Road Kill
- The “Go” in Cargo
- We’ll Make it Fit!

Security Cameras

- Research (for the most part) shows that security cameras:
  - Don't prevent crime
  - Can sometimes help solving crimes
  - Can be useful for criminal prosecution

- Common Sense Rule: If you're going to bother having a security camera, make sure the resolution is sufficient to recognize your own mother.

- The video recording system is the main cause of poor quality images.

Shoot a few scenes out of focus. I want to win the foreign film award. -- Billy Wilder (1906-2002)