LAUR-06-5375

Research on Improving Cargo Security

Roger G. Johnston, Ph.D., CPP

Vulnerability Assessment Team
Los Alamos National Laboratory

505-667-7414 rogerj@lanl.gov
http://pearl1.lanl.gov/seals

Los Alamos NATIONAL LABORATORY

VAT

LANL Vulnerability Assessment Team

Physical Security

- consulting
- cargo security
- tamper detection
- training & curricula
- nuclear safeguards
- new tags, seals, & traps
- vulnerability assessments
- novel security approaches
- security psychological issues

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

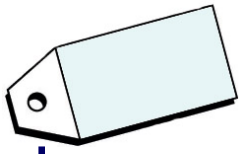
The greatest of faults, I should say,
is to be conscious of none.
-- Thomas Carlyle (1795-1881)

Terminology

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

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

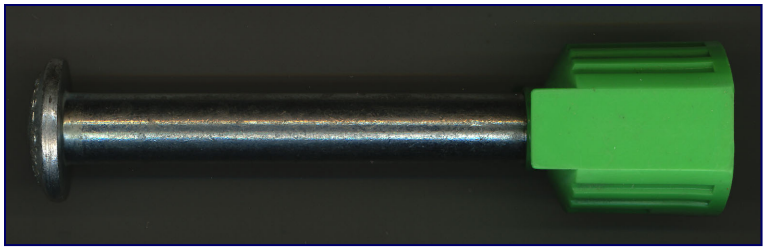
seal: a tamper-indicating device (TID) designed to leave non-erasable, unambiguous evidence of unauthorized entry or tampering. Unlike locks, seals are not necessarily meant to resist access, just record that it took place.



tag: a unique identifier of an object or container

Terminology

barrier seal: a single device that is both a lock & a seal



Problematic because:

(1) It's a compromise; neither the best seal nor the best lock for a given application.

(2) Its multi-functionality confuses people.

> Why don't they make the whole plane out of that black box stuff?
>
> -- Stephen Wright

Terminology to Avoid

"tamper-proof" seal: No such thing. Unprovable even if there were. Silly, because a seal that can't show tampering is of no use. The correct term is "tamper-indicating" seal.

"tamper-resistant" or antipilferage seal: Locks resist tampering & pilferage, not seals. Seals record that trespassing took place.

"security" seal: Not a good substitute for the term "barrier seal" because all seals do tamper detection, which is a security function.

"high security" seal (ISO 17712): Really unfortunate because pull strength is not the measure of a good lock, much less a seal.

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

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.

Defeating seals is mostly about fooling people, not beating hardware (unlike defeating locks, safes, or vaults)!

A Seal is Not a Lock!

(Yanking a seal off a container is not defeating it, because it will be noted at the time of inspection that the seal is damaged or missing.)

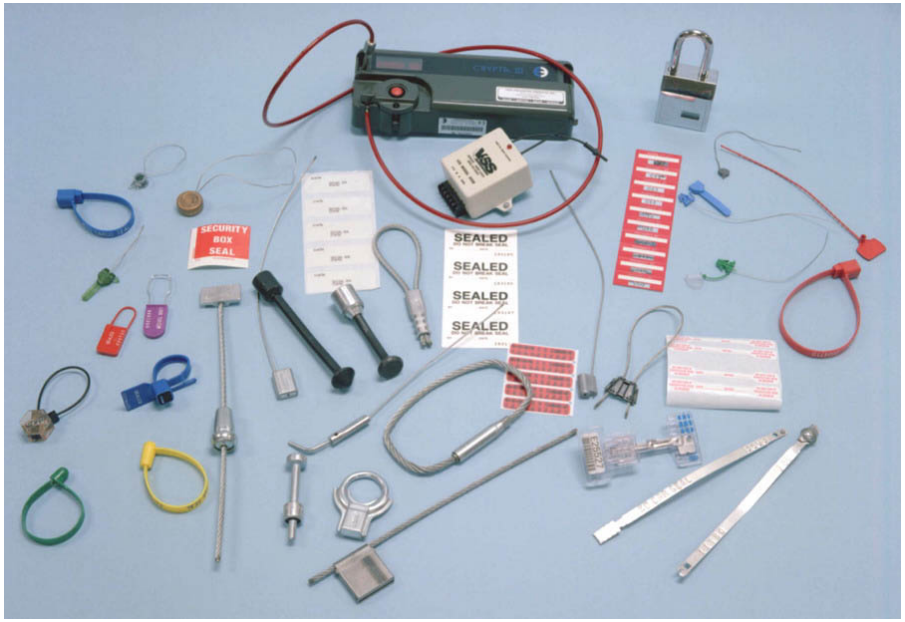
Now that the world is getting over the initial shock, and the war against terrorism has begun, what now for bridal retailers?

-- Actual editorial in the trade magazine *Bridal Buyer*

Tags & Seals

Tags: Uniquely identify an object or container

Seals: Detect tampering or unauthorized access



Some of the 5000+ commercial seals

Applications

- customs
- cargo security
- non-proliferation
- treaty verification
- counter-terrorism
- counter-espionage
- banking & couriers
- drug accountability
- records & ballot integrity
- evidence chain of custody
- weapons & ammo security
- tamper-evident packaging
- anti-product counterfeiting
- protecting instrument calibration
- protecting medical sterilization
- waste management & hazardous materials accountability

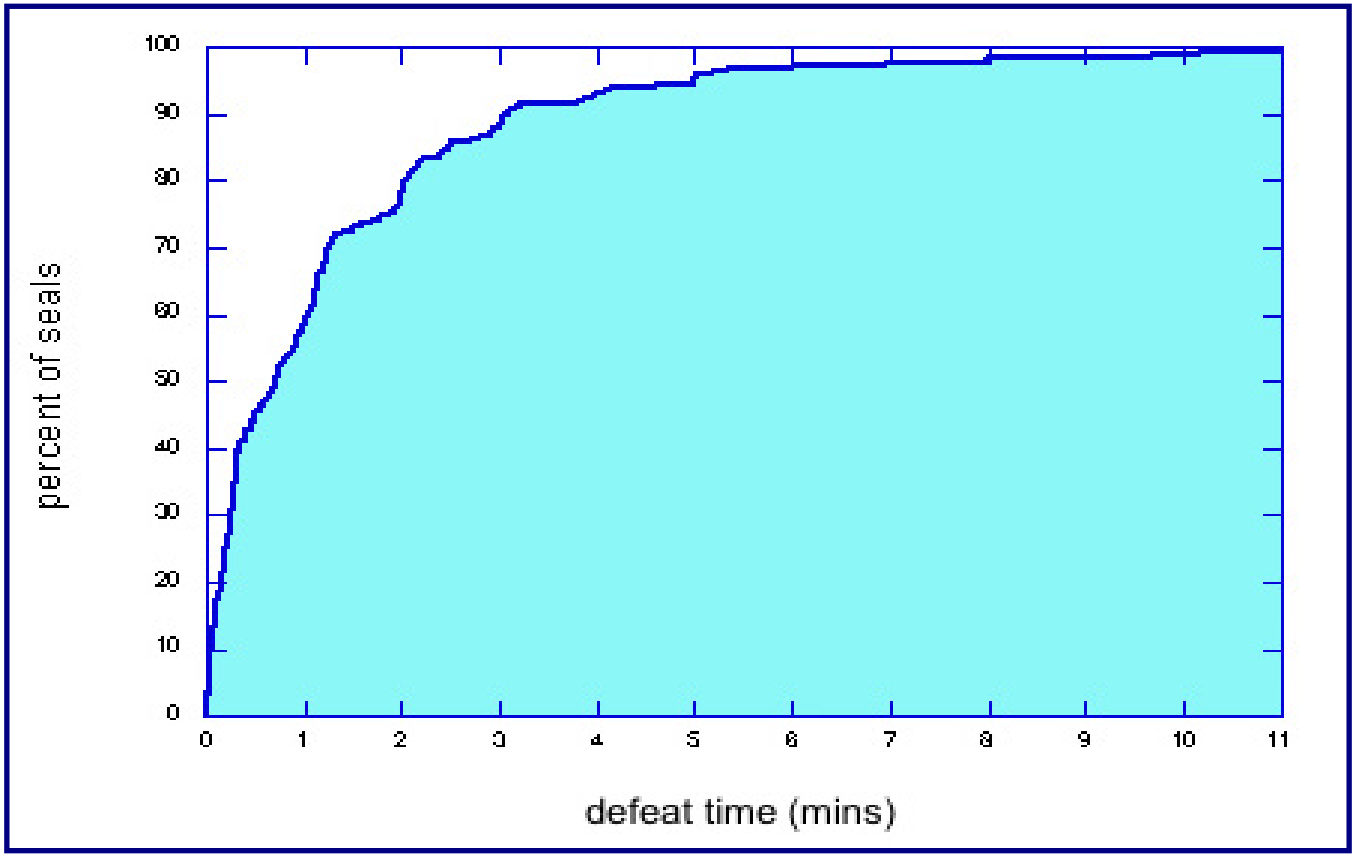
Seals Vulnerability Assessment

We studied 244 different seals in detail:

- government & commercial
- mechanical & electronic
- low-tech through high-tech
- cost varies by a factor of 10,000

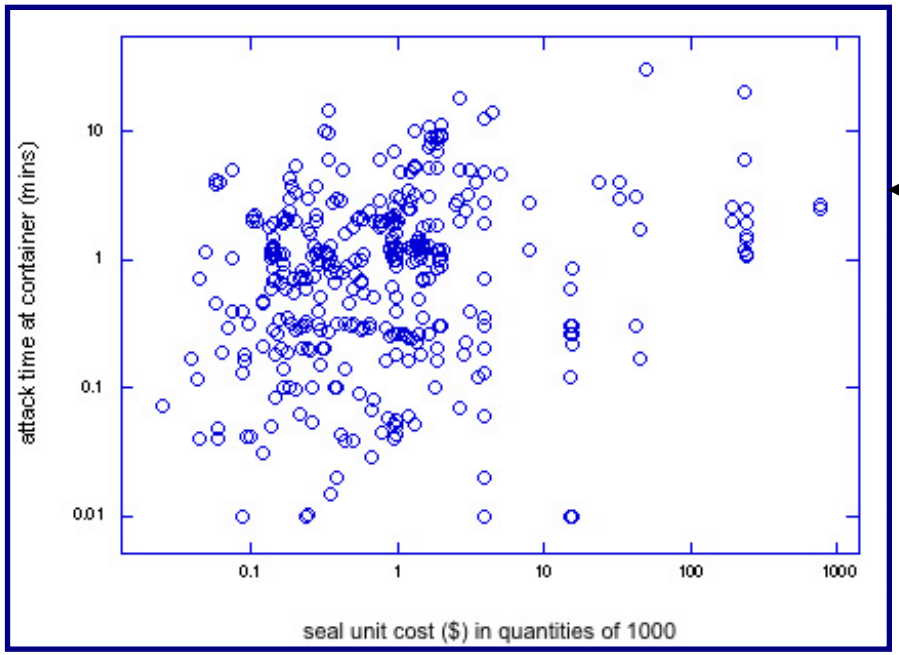
Over half are in use for critical applications, and ~19% play a role in nuclear safeguards.

Percent of Seals That Can Be Defeated in Less Than a Given Amount of Time



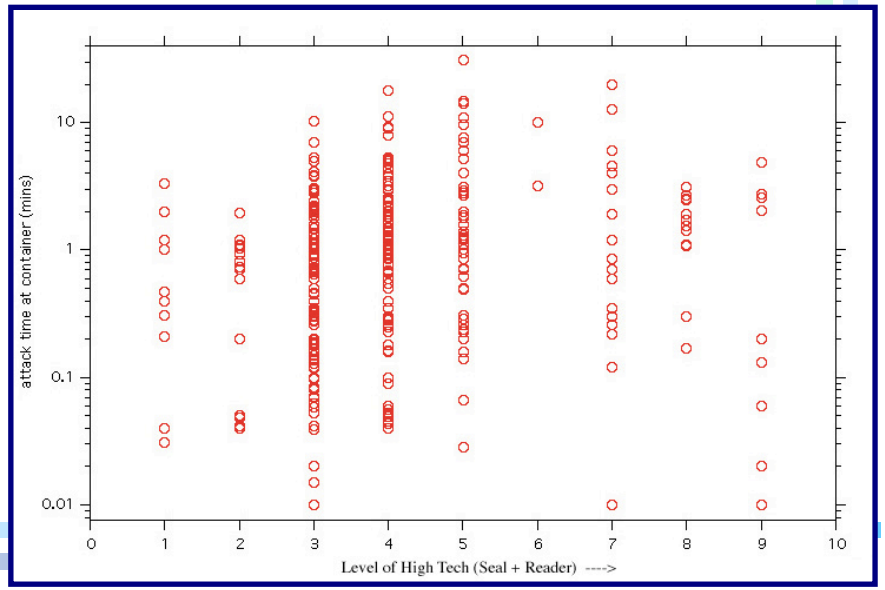
High Tech Isn't Automatically Better!

393 attacks



Linear LS fit
r = 0.10
Slope = 270 msec/$

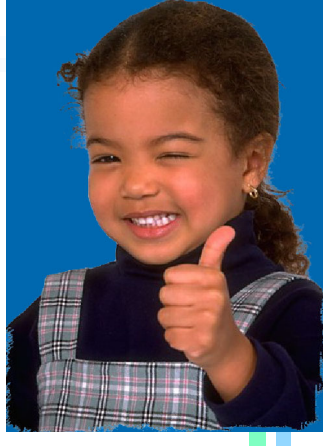
Linear LS fit
r = 0.19
Slope = 170 msec/tech level



Results for 244 Different Seal Designs

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

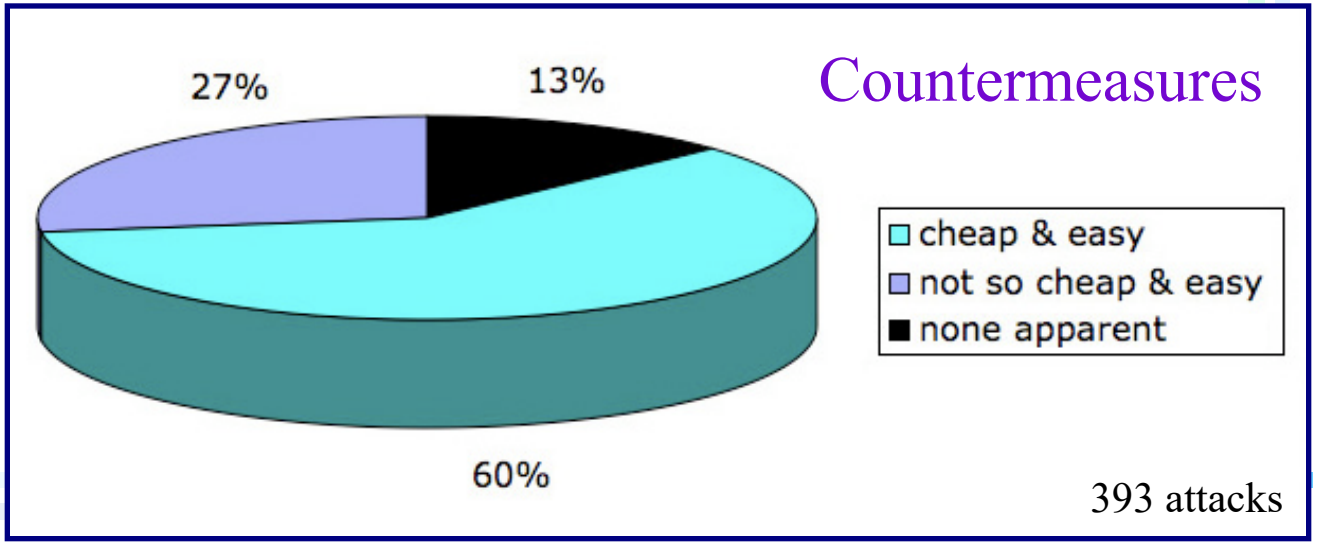
The Good News



Simple countermeasures usually exist, but require:

- understanding the seal vulnerabilities
- looking for likely attacks
- having seen examples

If a thing is worth doing, it is worth doing slowly. Very slowly.
-- Gypsy Rose Lee (1914-1970)



The Good News (con't)

But better seals are also possible!

conventional seals:

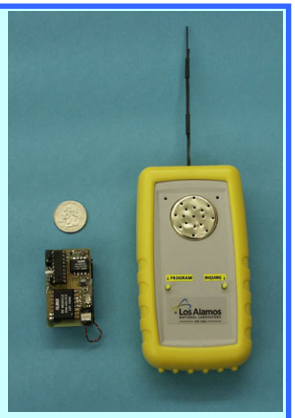
They must store the fact that tampering has been detected until the seal can be inspected. But this 'alarm condition' can be easily hidden or erased, or eliminated by making a fresh counterfeit seal.

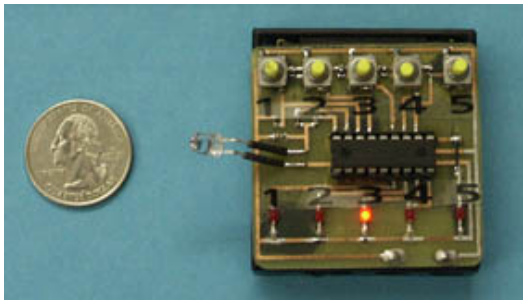
anti-evidence seals:

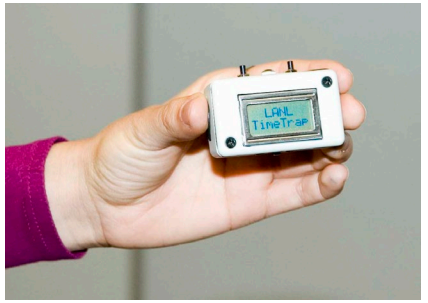
At the start, when the seal is first installed, store information that tampering hasn't yet been detected. Erase this 'anti-evidence' when tampering is detected. This leaves nothing for an adversary to hide, erase, or counterfeit!

20+ New LANL "Anti-Evidence" Seals

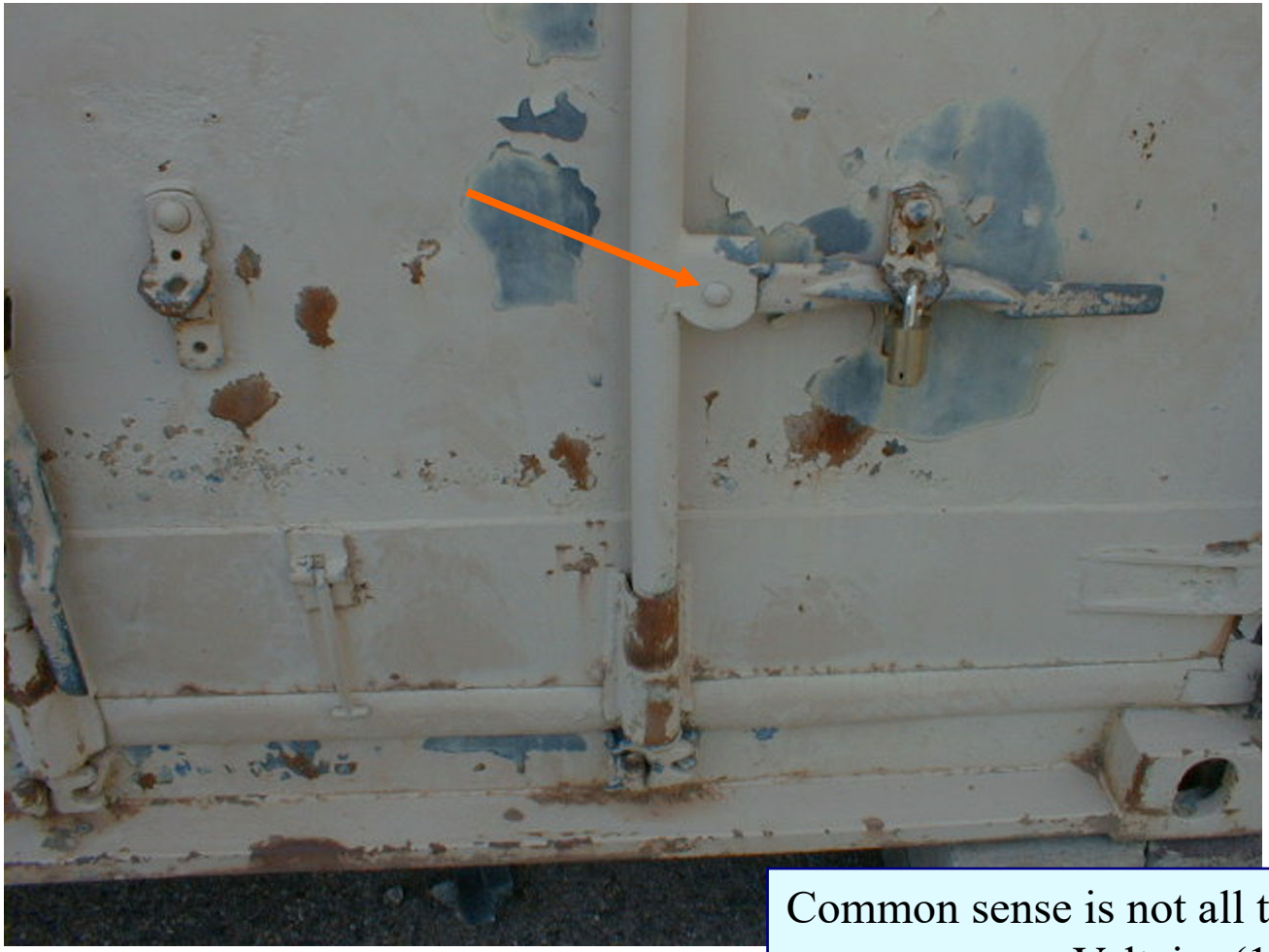
- better security
- no hasp required
- no tools to install or remove seal
- 100% reusable, even if mechanical
- the seal can go inside the container
- can monitor volumes or areas, not just portals
- can automatically verify the seal inspector actually checked the seal ("anti-gundecking")







Why do we lock or seal the handle when it is the locking rod we care about?



Common sense is not all that common.
-- Voltaire (1694-1778)

Warning: Containers are easy to enter surreptitiously through the walls

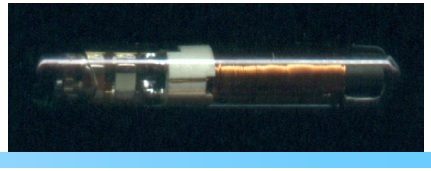
- Entry can be very fast
- Repair can be fairly quick & surprisingly good
- Repair may involve alternate materials

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

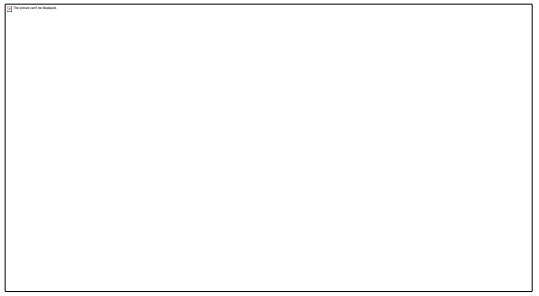
RFIDs:
Radiofrequency Identification Devices

- RFID tags transmit serial numbers using radio waves.
- Most RFIDs do not use batteries (passive), but some do (active). Some are even “semi-passive.”
- Passive RFIDs draw power from a rf pulse generated by the reader.
- Frequencies: low (~125 KHz), high (~13.56 MHz) and ultra-high (~900 MHz), and sometimes microwave (2.45 GHz).
  RuBees: < 450kHz.

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



RFIDs: fine for inventory, problematic for security

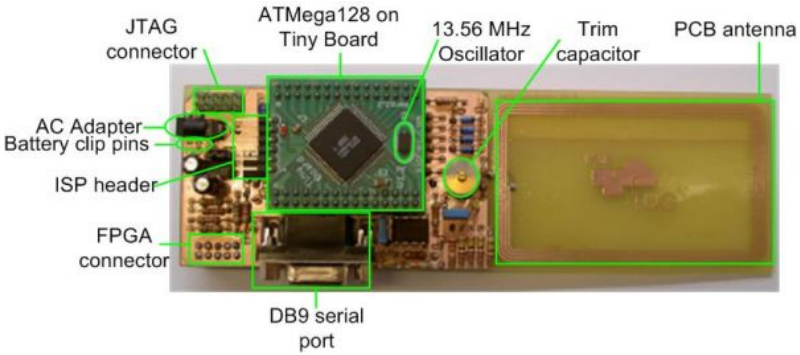


- Easy to lift.
- Easy to block or jam signals.
- Easy to counterfeit. All needed information, software, & parts are readily available.
- Easy to eavesdrop on a RFID and record its signal. Free software and information are on the Internet.
- Easy to spoof or tamper with the reader. No access to the RFID itself is needed.

Our first attempt at attacking RFIDs: Starting with zero knowledge, it took 2 weeks, and < $20 in parts to demonstrate 5 different defeats.

RFID Counterfeiting Devices

Commercial: Used for “faking RFID tags”, “reader development.”



Commercial: $20 retail, Cloner.

Hobbyist: RFID Skimmer, Sniffer, Spoofer, Cloner.

See also http://www.examiner.com/a-234701~Digital_dog_tag_already_cloned.html

What about cryptographic RFIDs?

- Used in Vehicle Immobilizers, Electronic Payment, and other high importance systems.
- Typically weak or non-existent physical tamper detection capabilities.
- People have also defeated them other ways:
  http://rfidanalysis.org/DSTbreak.pdf http://rfidanalysis.org/#signifigance
  http://www.wired.com/wired/archive/14.05/rfid.html

  http://www.eetimes.com/news/latest/showArticle.jhtml;jsessionid=E4UP4JUJB3I4UQSNDBESKHA?articleID=180201688

It's basically a bar code that barks.
-- Robin Koh, MIT Auto-ID Lab

GPS: A classic example of confusing Inventory with Security, and High-Tech with High-Security

- 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!

Never purchase beauty products in a hardware store.
-- Miss Piggy

Attacking GPS Receivers

Blocking: just break off the antenna, or shield it with metal; not surreptitious.

Jamming: easy to build a noisy rf transmitter from plans on the Internet; not surreptitious.

Spoofing: surreptitious & (as we've demonstrated) surprisingly easy for even unsophisticated adversaries using widely available GPS satellite simulators.

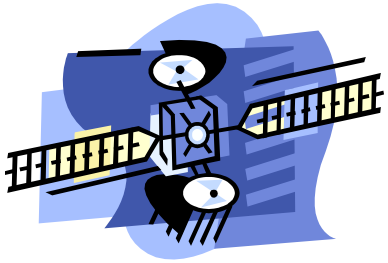
Physical attacks: appear to be easy, too.

Spoofing GPS Civilian 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, rf, or GPS to use them.

GPS Cargo Tracking

GPS Satellite



Tracking Information
Sent to HQ
(perhaps encrypted/authenticated)

GPS
Signal

(vulnerable here)

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

Time Vulnerabilities

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

- An alternate time standard (NIST atomic clock) is also not authenticated or encrypted.

I don't know a greater advantage than to appreciate the worth of an enemy.
-- Johann Wolfgang von Goethe (1749-1832)

Spoofing Countermeasures

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

- wrong time
- suspiciously low noise
- excessive signal strength
- artificial spacing of signals
- no time variation in signal strength
- all satellites have the same signal strength
- do a sanity check (e.g., no 10g accelerations)

Just once, I would like someone to call me "Sir" without adding, "You're making a scene."

-- Homer Simpson

Warning: Access Control & Biometric Systems

Most access control & biometric systems are easy to defeat:

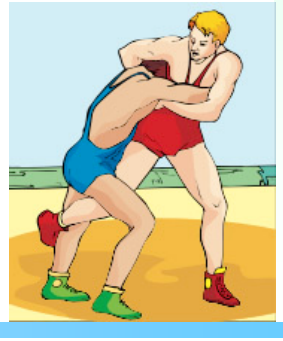
- tamper with the device
- counterfeit the device
- counterfeit the access or biometric signature
- attack the door lock or turnstile

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

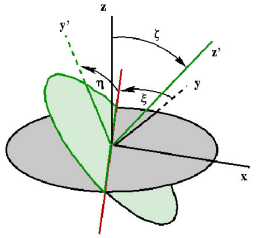
Vulnerability Assessment (VA)

Discovering and demonstrating ways to defeat a security device, system, or program. Should include suggesting counter-measures and security improvements.

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



Effective 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 your adversaries. They need only stumble upon 1 vulnerability, you have to worry about all of them.

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

- Gleefully look for trouble, rather than seeking to reassure yourself that everything is fine.

Warning on a laser printer cartridge: "Warning. Do not eat toner."

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

- 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.

Summary

- Tampering-indicating seals aren't very good, but could be a lot better.
- RFID is great for inventory, but problematic for security.
- GPS is highly vulnerable to spoofing, not just jamming
- Access control & biometric systems have a lot of easy-to-exploit vulnerabilities
- There are better ways to do vulnerability assessments

The LANL Vulnerability Assessment Team

Dr. Peter Chen, Dr. Roger Johnston, CPP, Michael Timmons, Anthony Garcia, Eddie Bitzer, M.A., Ron Martinez, Leon Lopez, Lance Griego, Dr. Jon Warner, Sonia Trujillo

http://pearl1.lanl.gov/seals

We have a CD containing related papers & reports.

Available today or request a copy at rogerj@lanl.gov

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)