Product Authenticity Issues

Roger G. Johnston, Ph.D., CPP

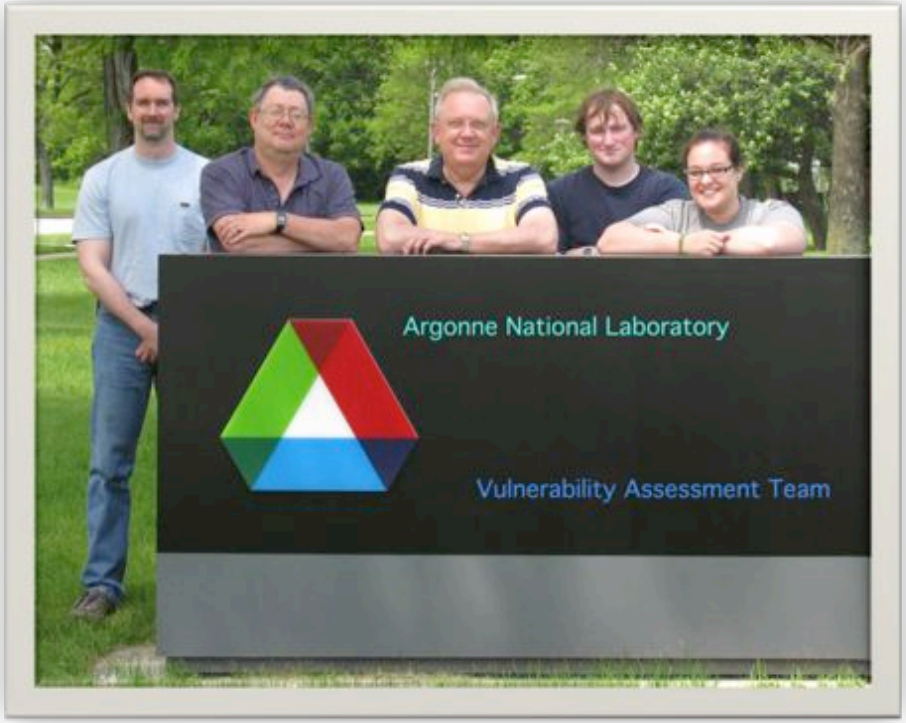
Vulnerability Assessment Team
Argonne National Laboratory

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

Argonne National Laboratory

~$738 million annual budget (16% defense, homeland security, or intelligence)
1500 acres, 3400 employees, 4400 facility users, 1500 students
R&D and technical assistance for government & industry

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

Sponsors

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

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

Counterfeiting & Tampering

Both represent a security failure in the logistics chain of custody.

Topics today:

- General Security Issues & Warnings Relevant to Counterfeiting
- Product Counterfeiting, AC Tags, & Alternatives
- Product Tampering
- Virtual Numeric Tokens
- The Future

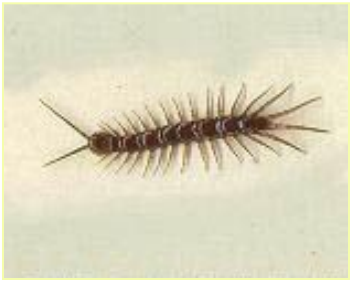
I watch a lot of game shows and I've come to realize that the people with the answers come and go, but the man who asks the questions has a permanent job.
-- Gracie Allen (1895? – 1964)

General Security Issues & Warnings

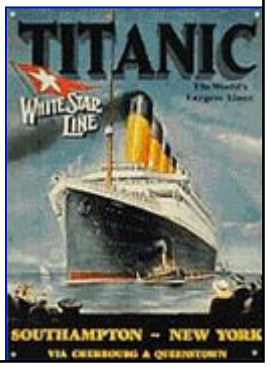
Sometimes security implementations look fool proof.
And by that I mean proof that fools exist.
-- Dan Philpott

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 usually makes them easy to attack

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

Examples of Confusing Inventory with Security

- rf transponders (RFIDs)

- prox cards

- contact memory buttons

- GPS

- Nuclear MC&A

Usually easy to:

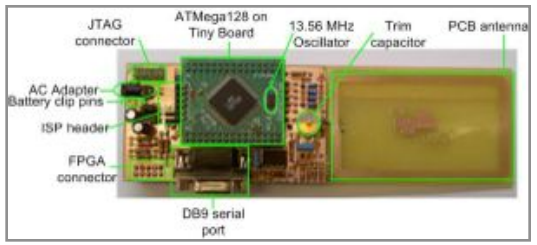
* lift
* counterfeit
* tamper with the reader
* spoof the reader from a distance

Very easy to spoof, not just jam!

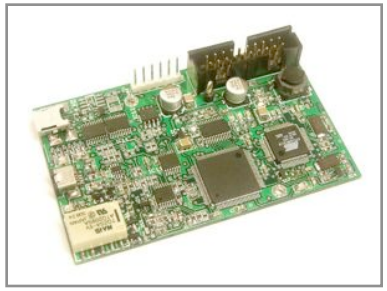
A Sampling of RFID Hobbyist Attack Kits Available on the Internet

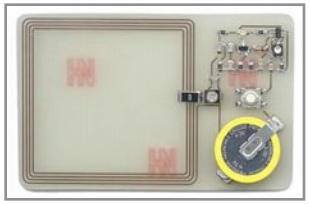
Commercial: $20 Car RFID Clone (Walmart)

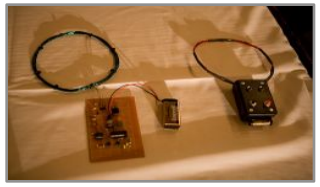
Commercial: Used for "faking RFID tags", "reader development."

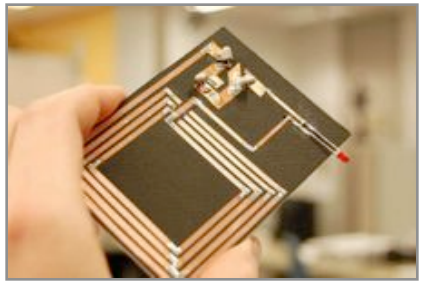


RFID Skimmers, Sniffers, Spoofers, and Cloners; oh my!

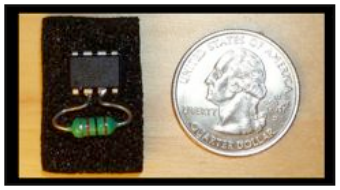


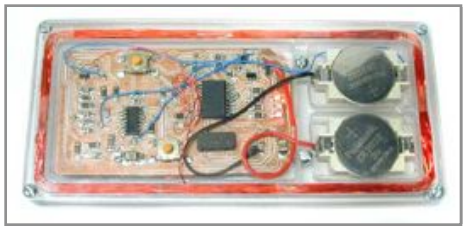


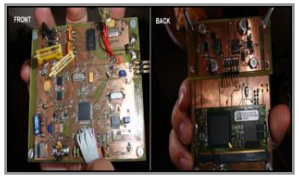




Documents, code, plans needed to build your own: free.







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

Blunder: Wrong Assumptions about Counterfeiting

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

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

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

Tags & Product Counterfeiting

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

Pharmaceutical Counterfeiting

The following are largely made-up estimates because nobody knows the true extent of the problem:

North America: ~1% of all pharmaceuticals in the legitimate market are counterfeits.

U.S.: Seizures of counterfeit pharmaceuticals by the feds increase ~150% annually.

Worldwide: ~10% of pharmaceuticals are counterfeit (maybe 30%).

Worldwide: Pharma counterfeiting is a $75 billion per year "business", growing 13% annually (twice the rate of legitimate pharmaceuticals).

Worldwide: ~97% of online pharmacies sell counterfeits.

Worldwide: ~200,000 deaths from counterfeit pharmaceuticals annually. [Estimates range from a few thousand to 700,000.]

Fakes Aren't Always Bad For Manufacturers

Fakes as a gateway product: Consumers who buy fakes as "low-risk trials" of products they really want often end up buying the real thing when they see the difference in the quality, according to researcher Renee Richardson Gosline.

http://www.portfolio.com/executive-style/2010/01/11/conterfeit-goods-can-lead-to-purchasing-the-real-thing/#ixzz1OcC7IybP

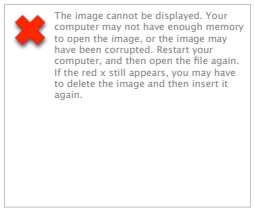
Harry Potter this, Harry Potter that! I'd never even heard of Harry Potter until the book came out.

-- Caller, BBC Radio 5 Live

Terminology

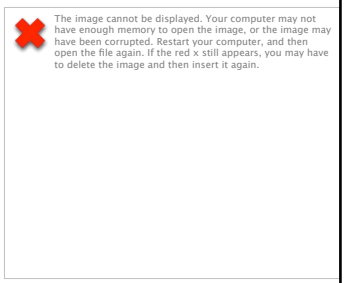
tag: an applied or intrinsic feature that uniquely identifies an object or container.

types of tags



- inventory tag (no malicious adversary)
- security tag (counterfeiting & lifting are issues)
- buddy tag or token (only counterfeiting is an issue)
- → anti-counterfeiting (AC) tag (usually only counterfeiting is an issue)*

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



Alternative Definition

Product Anti-Counterfeiting Tag: (noun)-Something that product manufacturers and counterfeiters place on a product to convince the customer that it is authentic.

It is estimated that only 1% of "Louis Vuitton" designer handbags are authentic.

Anti-Counterfeiting Tags

Smoke & Mirrors

hawking
pet technology

HYPE

Misleading Statements

Fuzzy Thinking

Snake Oil

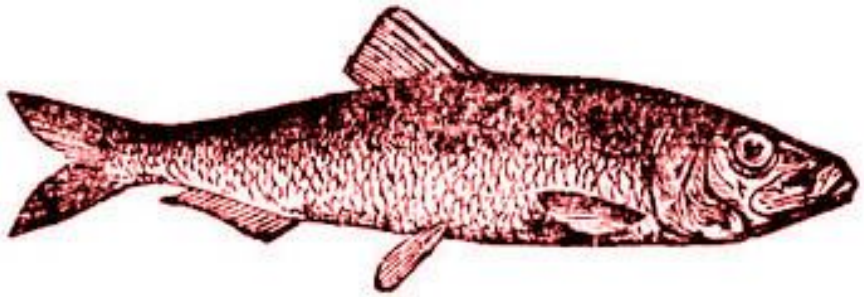
Track & Trace?

Great for investigations, but…

- It's complicated, especially for commodities and for brokered or repackaged products.
- The RFIDs aren't the security.
- Requires a call back.
- Is often a poorly executed virtual numeric token scheme.
- Putting the provenance data on the product provides no security.
- Encrypting the provenance data on the product provides no security.

Security Maxims

Red Herring Maxim: At some point in any challenging security application, somebody (or nearly everybody) will propose or deploy more or less pointless encryption [or data authentication] and justify it with the often incorrect and largely irrelevant statement that “the cipher [or hash] cannot be broken”.



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!”

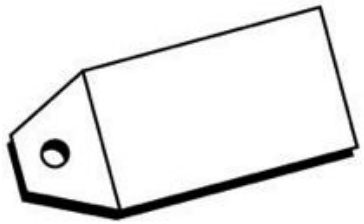
-- Anthony Burgess

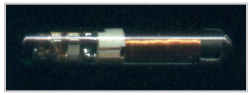
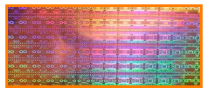
Anti-Counterfeiting Blunder

- Putting information about how to spot the authentic product in with the product!

"Product not actual size."
-- Disclaimer on a TV ad for Burger King that showed a giant Whopper crushing a car

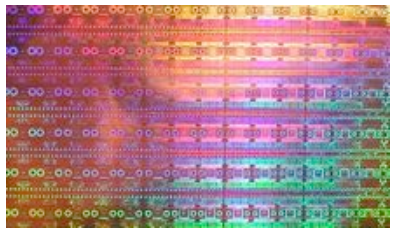
Common Anti-Counterfeiting Tags



- RFIDs 
- holograms 
- color changing films 
- covert marks, inks, or micro-patterns (secret tags)
- taggants

Everyone wants to be Cary Grant.
Even *I* want to be Cary Grant.
-- Cary Grant (1904-1986)

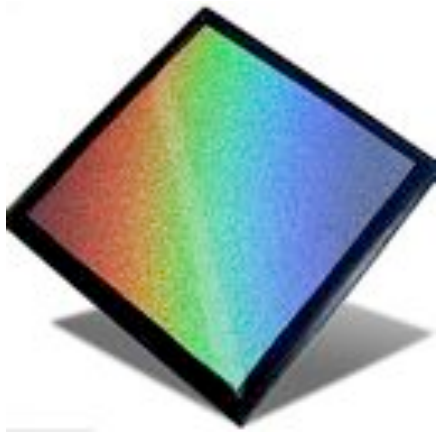
The Problems with Holograms



- easy to counterfeit (See, for example, http://www.nli-ltd.com/publications/hologram_counterfeiting.php)
- easy to fool consumers & retail clerks with flashy colors
- embossed (stamped) holograms are especially trivial to duplicate
- a number of companies will copy holograms for you, few questions asked
- do-it-yourself hologram turnkey systems are available

The Problems with Color Shifting Ink

- Manufacturers will usually sell the ink to almost anybody (despite claims otherwise).
- There are lots of cheap, readily available color-shifting pigments, paints, cosmetics, & coatings that'll fool consumers & retail clerks.



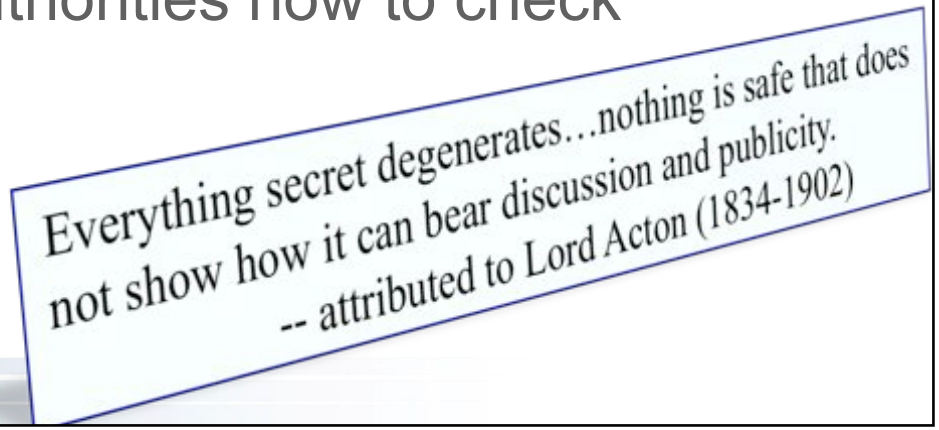
The Problems with Blister Packs

- Packaging companies will blister pack for anybody, few questions asked.
- Blister pack supplies are readily available.
- New & used blister pack machines are relatively inexpensive (though aren't really necessary).

If ignorance were bliss,
he'd be a blister.
-- Anonymous

The Problems with Covert Marks, Inks, Micro-Patterns & Other Secret Tags

- Counterfeiters already pore over the packaging, so they will figure out the secret.
- Likely to be better at graphic arts than the real manufacturer.
- Secrets are hard to keep. Shannon's Maxim: The bad guys know what you are doing ("security by obscurity" won't work).
- Use it & lose it: The secret is compromised when you tell a customer or government authorities how to check authenticity.



The Problems with Covert Marks, Inks, Micro-Patterns & Other Secret Tags

- Constantly swapping out secret tags to stay ahead of the counterfeiters is expensive & confusing—ultimately a losing game except maybe against amateur counterfeiters.

Printing on a Chinese medicine bottle:
"Expiration date: 2 years"

The Problems with Covert Marks, Inks, Micro-Patterns & Other Secret Tags

- Fooling the eye (and simple readers) with fake inks & patterns is easy.
- The public has known about UV fluorescent dyes & black lights since the 1960s. The new IR dyes are also becoming known.
- Can require high levels of quality control in the printing—often the counterfeiters are better.

How do you know when you've run out of invisible ink?
-- Steven Wright

The Problems with Covert Marks, Inks, Micro-Patterns & Other Secret Tags

- Can't be used by the consumer.
- For pharmaceuticals: Repackagers, Consolidators, Commercial & Institution Pharmacies may dispense authentic drugs, then place fake drugs in the authentic packaging & resell.
- Suspicious products needs to be analyzed, anyway.

"Warning: do not use if you have prostate problems."
-- *On a box of Midol PMS relief tablets*

The Problems with Taggants

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

- Requires reformulating the product.
- Many of the same problems as with secret tags.
- Why not analyze the product instead? That's the best possible taggant, and the only important issue, anyway!

+ New (fast/cheap/small) field analytical devices are becoming available: GC/MS/FTIR/LIBS/Raman/other spectroscopies.

+ Other physical/mechanical properties are fast, cheap, & easy to measure, but tricky for counterfeiters to duplicate if they must match 2 or 3 simultaneously. Examples: density, gloss, hardness, porosity, viscosity, water content, melting point, dielectric constant, optical activity, thermal conductivity, vapor pressure, colorimetry, friction coefficient, outgassing, breaking strength, speed of sound, magnetic permeability, refractive index, etc.

Packaging should permit optical examination of the product.

XRD

LIBS

UV, visible, NIR
spectrometers & fluorometers

RAMAN

GC/MS

ultrafast GC

handheld X-ray
fluorescence

FTIR

Public Training/Awareness on Counterfeits

- ✓ Encourage Intuition (as with seals & suspicious mail packages)
- ✓ Someone to contact, someone to send a suspicious sample to
- ✓ Rewards for detecting counterfeits

1 of every 3400 Americans is an Elvis impersonator.

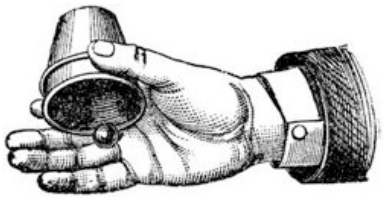
Other Countermeasures

- ✓ Lab forensics: Great investigation tool, not very practical for routine screening (including random sampling because counterfeits cluster)
- ✓ Greater penalties for trafficking in fakes
- ✓ Civil/Criminal/Regulatory actions, public shaming/jawboning by the feds for manufacturers who aren't proactive
- ✓ Better seals & cargo security when there is a trusted manufacturer
- ✓ Subsidize US manufacturers of critical products

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)

Other Countermeasures

- ✓ Make it clear to manufacturers that pretending that counterfeiting doesn't exist will backfire (and really make it so)
- ✓ Fix the legal situation & public perception that implementing a partial security measure is punished more than ignoring the problem
- ✓ National virtual numeric token program



I don't want any yes-men around me. I want everyone to tell me the truth—even if it costs him his job.
-- Movie mogul Samuel Goldwyn (1879-1974)

Product Tampering & Cargo Security

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

Terminology

A tourist once stopped to admire a mule. He asked the mule's owner what the animal's name was. The farmer said, "I don't know, but we call him Bill."
-- Sen. Sam Erwin (1896-1985)

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

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

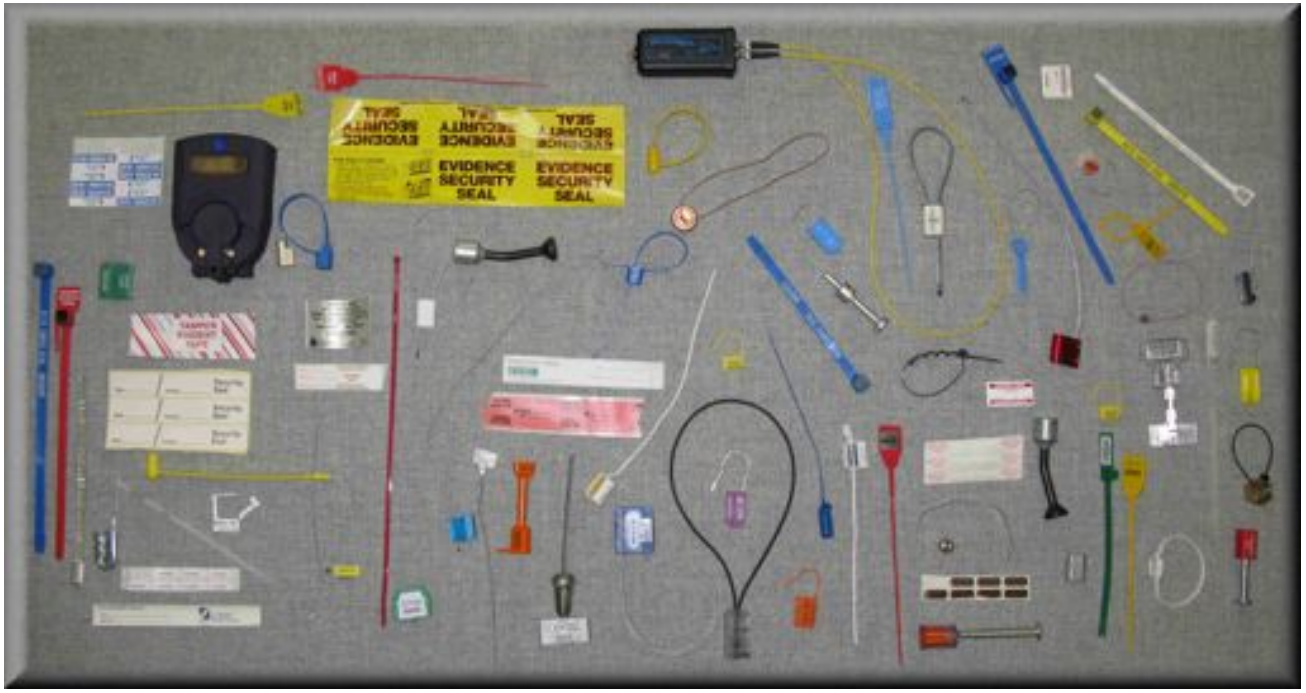
Terminology

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, as with tags, is mostly about fooling people, not beating hardware (unlike defeating locks, safes, or vaults)!

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
- tamper-evident packaging
- anti-product counterfeiting
- medical sterilization
- instrument calibration
- waste management & HAZMAT accountability

Seal Facts

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

1. Misleading terminology: “tamper-proof”, “tamper-resistant”, “high security”.

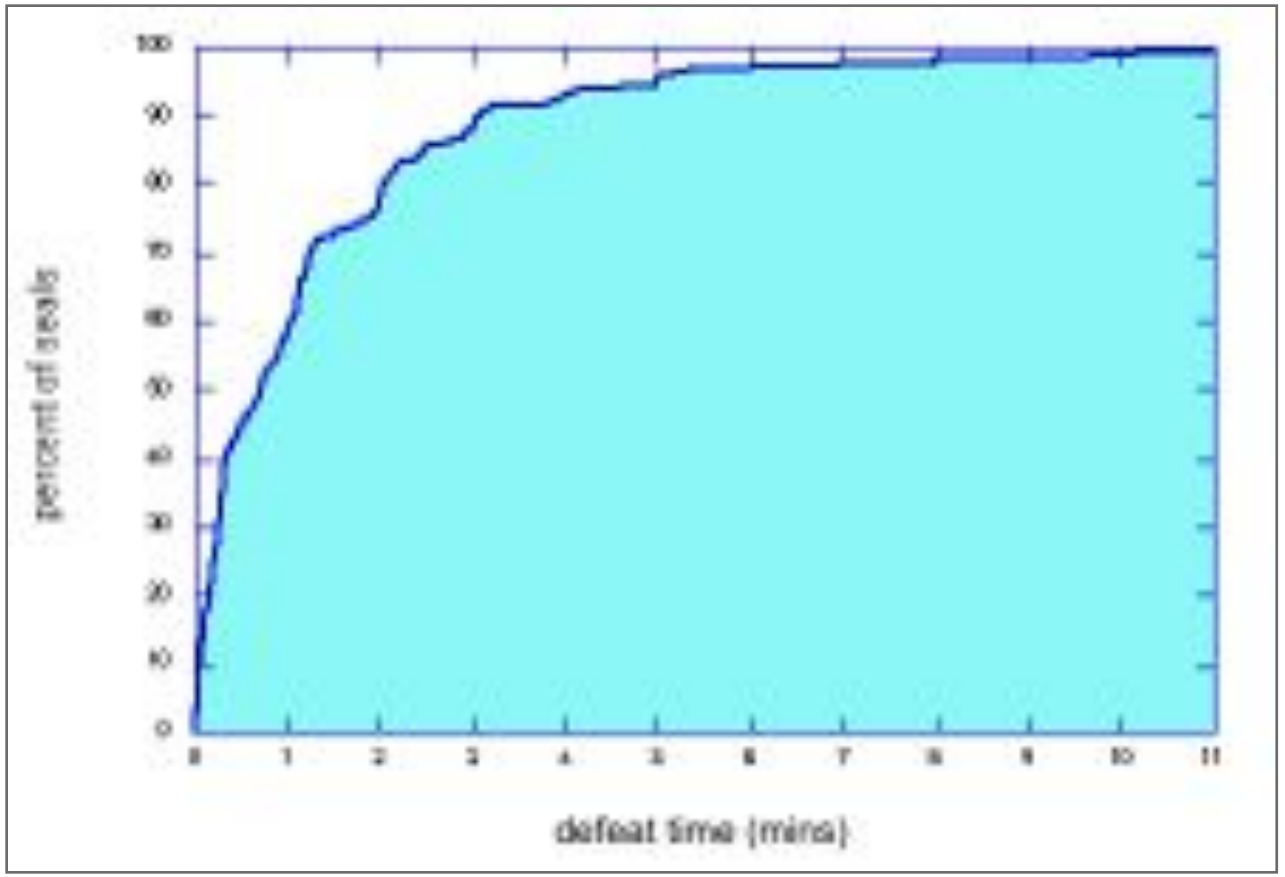
2. All seals need some kind of unique identifier (like a serial number).

3. 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.

4. Most seals aren’t very effective. Better seals & seal use protocols are possible.

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

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, inexpensive methods



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)

The Good News: Countermeasures

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

- Also: better seals are possible!

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.

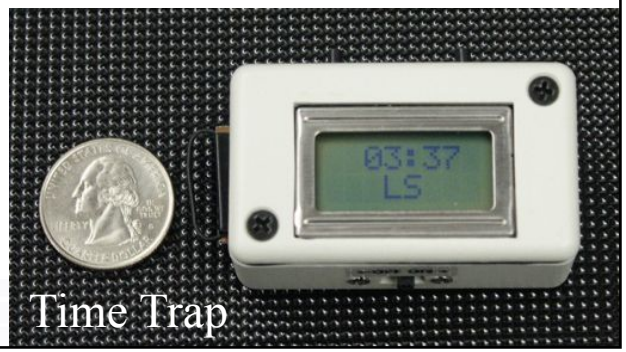
20+ New "Anti-Evidence" Seals

- better security
- simple & low cost
- some don't need a reader
- 100% reusable, even if mechanical
- no tools to install or remove the seal
- no hasp required—can go inside the container
- can monitor volumes or areas, not just portals
- anti-gundecking

Talking Seal

Tie Dye Seal

Chirping Tag/Seal



Time Trap

Wine Authenticity:
Detects Tampering & Counterfeiting

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."

Problems with Consumer Tamper-Evident Packaging

- Mostly about Displacement, Due Diligence, Compliance, & Reducing Jury Awards—not effective Tamper Detection
- TEP has not greatly improved since shortly after the 1982 Tylenol poisonings. Little ongoing R&D.
- No meaningful FDA Definitions, Standards, Guidelines, or Tests
- Consumers lack sufficient information to use properly
- Poor, easy-to-miss labeling. If the seal is removed, the consumer may not realize a seal originally existed.

"Do not eat if seal is missing."
-- Actual printing on the seal of a food package

Problems with Consumer Tamper-Evident Packaging (con't)

- What is the seal supposed to look like?
- Euphemisms (e.g., "freshness seal") and manufacturer obscurations.
- Relatively unimaginative, cost-driven designs
- Few useful vulnerability assessments
- Not proactive to the threat

Weakest Link host Anne Robinson: Watling Street, which now forms part of the A5, was built by which ancient civilization?
Contestant: Apes?

Virtual Numeric Tokens

The search for perfection often impedes improvement.
-- George Will

Imagine an Anti-Counterfeiting Tag That...

1. Is inexpensive & unobtrusive.
2. Is very difficult to counterfeit in large numbers.
3. Doesn't need a reader.
4. Can be checked by consumers, retailers, or wholesalers.
5. Typically detects more than 98% of the fakes checked.
6. Does not become easier to defeat over time, or as technology advances.
7. Is non-proprietary(?)

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

"Call-In the Numeric Token" (CNT) Technique

In the absence of effective AC Tags, this is one method to impede & detect product counterfeiting.

- virtual numeric token
- imperfect, but inexpensive & painless
- a societal/statistical approach to counterfeiting
- participants help others & themselves

Shouldn't the Air and Space Museum be empty? -- Dennis Miller

CNT

*"An Anti-Counterfeiting Strategy Using Numeric Tokens", International Journal of Pharmaceutical Medicine **19**, 163-171 (2005).*

Lot: 4ZB1026
Exp: 04/06
Bottle ID: MPD709

Bottle ID

- unique
- unpredictable
- random, non-sequential
- at least 1000 times more possible 'Bottle' IDs per Lot than actual bottles

("Bottle" can really mean bottle, tube, box, container, pallet, truck-load, etc.)

CNT Technique (con't)

- Print "Bottle" ID on bottles, or other packaging at the factory, or attach printed adhesive labels later.
- We don't care what number goes on what bottle, just that it is the right lot.
- Keep a secure computer list (database) of valid Bottle IDs for each Lot back at HQ.

CNT Technique (con't)

- **"Calling-in":** Customers log into a web site, or call an automated phone line (or the product beeps into the phone) to quickly check if their Bottle ID is valid for the given Lot number. (Yes/No response.)
- Works at the consumer, pharmacy, or wholesale level.
- Callers may or may not remain anonymous. (Pros & Cons).
- Useful even if only a very small fraction of customers participate. A very high percentage of the fakes called-in will be detected.

Counterfeits are spotted by…

1. Invalid Bottle IDs that are called-in will be immediately recognized as counterfeits.

2. Any duplicate valid Bottle IDs that are called-in will be flagged as counterfeits with fairly high reliability.

3. Wholesalers, re-packagers, and other handlers of large quantities can spot counterfeits even without calling-in by finding duplicate Bottle IDs in their own database of past and present stock. ("**Self-checking**".) This works well because fakes tend to cluster.

Counterfeiters

The bad guys are hampered by these problems:

- Guessing valid ID numbers isn't practical.
- Getting dozens or hundreds of valid Bottle IDs is easy but getting large numbers of valid IDs is challenging, and they change with each new Lot.
- Making counterfeit products with duplicate IDs will likely be detected via call-ins or self-checking.
- Counterfeiting the packaging, bar code, or RFID gains them nothing.

CNT: What We Tell Call-Ins

- ✓ Any caller with an **invalid** Bottle ID: "You have a fake with 100% certainty."

- ✓ 1st caller through caller T-1 for a given **valid** Bottle ID, where T is the counterfeiting threshold: "Thanks for contributing to everybody's safety! We have no information at this time that there is a problem with your drugs but you can optionally:

(1) check back later, but be sure to tell us you are rechecking,

or

(2) give us your contact info & we'll get back to you if new information becomes available."

CNT: What We Tell Call-Ins

- ✓ Caller T and greater for a given **valid** Bottle ID:

  "You probably have a fake. Send it in for analysis and don't use this medicine."

The probability it is a fake is ~ (1 – 1/n), where n is the total number of fakes in the world with that valid Bottle ID (called in or not).

This is ~90% for n=10 and ~99% for n=100.

Important Points

- A buddy tag. Need not be physically co-located.
- Our focus needs to be on the high percentage of callers who we help, not the non-callers we don't.
- But, those who don't call-in are still helped by pharmacies and wholesalers who *do* call-in, or self-check.
- CNT can be quietly implemented, then activated when a crisis occurs just by holding a press conference.
- This is a very cheap approach to helping a lot of customers.
- Effectiveness automatically scales with the level of concern.
- Typically done wrong.

If people don't want to come to the ballpark, how are you going to stop them? -- Yogi Berra

The Future

Now that the world is getting over the initial shock, and the war against terrorism has begun, what now for bridal retailers?
-- Actual 2002 editorial in the trade magazine *Bridal Buyer*

Bad Tampering is Coming!

Major tampering with OTC pharmaceuticals is inevitable: multiple cities, multiple products, by 1 person or a small group.

Results:

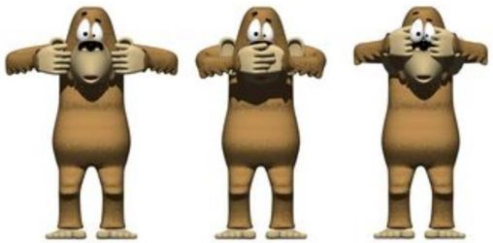
- Recall of **all** OTC products in the US
- Americans fearful of buying OTC products for years
- Major litigation against OTC manufacturers

- Severe recriminations and charges of negligence against pharma by the press, Congress, courts, juries, & the public, alleging a lack of due diligence, transparency, significant ongoing R&D, and concern for customers & public welfare

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

Other Pharma Security Problems

- ✓ Poor cargo & plant security
- ✓ Little or no countermeasures to the Insider Threat.
- ✓ Waiting for the FDA or Congress to mandate better security probably isn't prudent.
- ✓ Denial, fear of partial solutions, & trying to suppress internal discussion of security problems will back fire (and is ethically dubious).

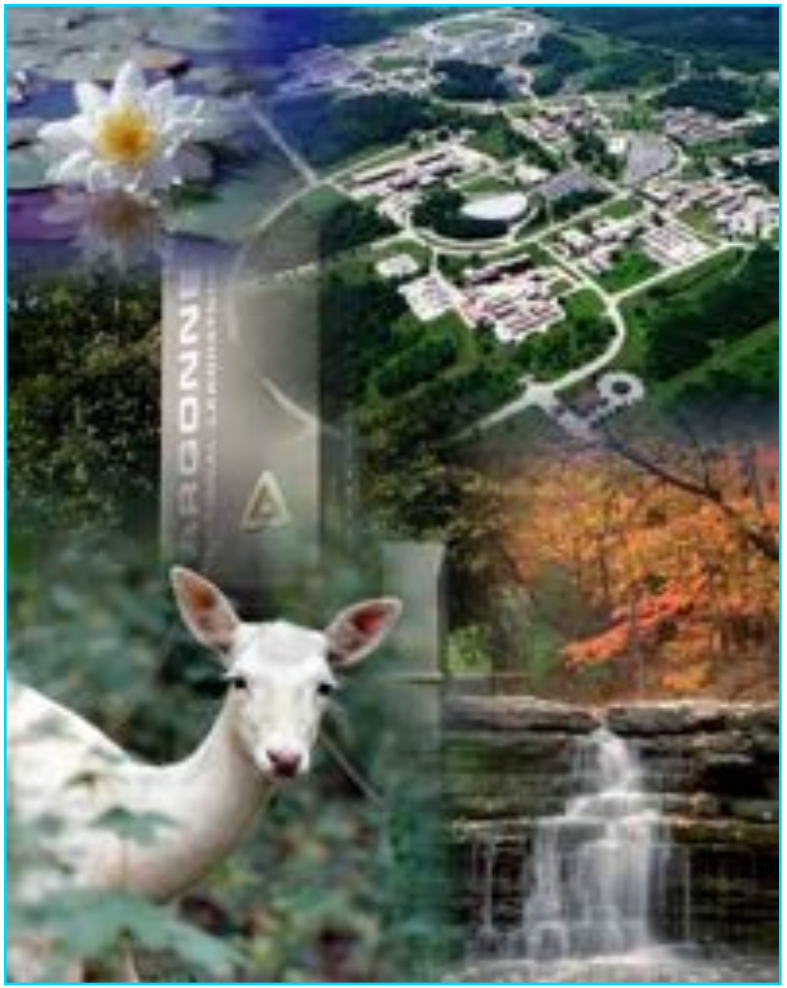


For the third goal, I blame the ball.
-- Saudi goalkeeper Mohammed Al-Deayea

Other Pharma Security Problems

- ✓ The lessons of the 1982 Tylenol poisonings seem to have been lost in the recent J&J product recalls.
- ✓ Little meaningful R&D is underway on either product tampering or counterfeiting.
- ✓ Most existing work & products involve force-fitting a pet technology, not fundamentally addressing the problem.
- ✓ How is Pharma going to claim Due Diligence to juries, the FDA, Congress, the public, and the press after serious incidents if it is not even supporting modest research efforts on anti-tampering and anti-counterfeiting, and has no planned, coherent crisis response?

For More Information...



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

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

Argonne NATIONAL LABORATORY

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)

Supplemental material not part of the presentation…

Common Virtual Numeric Token Mistakes

1. Failure to use the technique to gauge the extent of counterfeiting
2. Failure to consider using the technique as an invisible standby, brought out in an emergency
3. Not viewed (as it should be) as a societal/statistical/probabilistic approach, not a way to guarantee absolute authenticity
4. Poor strategies or outright misrepresentation for caller T=1
5. Poor strategies or outright misrepresentation for callers T>1
6. Threshold mindlessly set to T=2 when it probably should be 3-5
7. Incomplete use (or no use) of the multiply called-in valid Bottle IDs

Common Virtual Numeric Token Mistakes

8. Failure to apply to consumers, pharmacies, institutions, and volume customers

9. Failure to exploit self-checking

10. Failure to exploit automated use of bar codes or RFIDs

11. Failure to employ options & strategies for repackaging, brokering, and resale

12. Failure to employ options & strategies for inadvertent re-calling in, and for dealing with a caller who reports many invalid Bottle IDs

13. Failure to exploit counterfeit clustering & information on the order of call-ins

Common Virtual Numeric Token Mistakes

14. Failure to invoke effective strategies for dealing with typos and check-back

15. Failure to explore DTMF-type phone solutions

16. Serialization of the Bottle IDs

17. Not a large enough universe of possible Bottle IDs

18. Failure to use the lot number, thus unnecessarily increasing the length of the Bottle ID

19. Failure to exploit the fact that the Bottle ID does not need to be co-located with the Bottle

20. Information about how to do the calling in is included with the product

Common Virtual Numeric Token Mistakes

21. No strategies for dealing with legal liabilities

22. Misrepresentation to manufacturers by 3rd-party providers of virtual numeric token services.

23. Pointless use (and hyping) of encryption

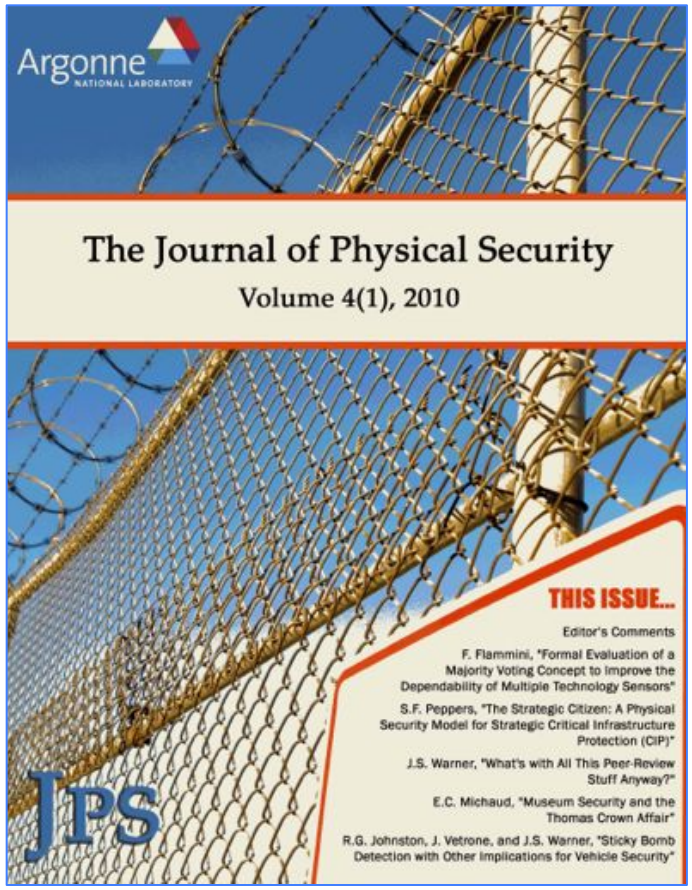
24. Confusion about the role of RFIDs and Track & Trace

25. Failure to understand the underlying complexity of CNT

26. Poor random number generation.
    - Should be done in hardware, not via PRNGs.
    - The assignment of Bottle IDs must not use any of these inputs: lot number, date, time, product, manufacturer, location, order off the factory line.

Anyone who attempts to generate random numbers by deterministic means is, of course, living in a state of sin. -- John von Neumann (1903-1957)

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)