Pharma Tampering, Counterfeiting, and Supply Chain Security

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

3 sq miles, ~3200 employees, $630+ million annual budget
R&D, consulting & technical assistance for government & industry

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**

Summary

There are many widespread mistakes & myths about cargo security and physical security that should be avoided.

Current tamper-indicating seals, tamper-indicating packaging, and product anti-counterfeiting tags aren't very effective.

There's little sophisticated R&D underway—mostly people and companies are pushing pet technologies, not trying to solve the problem holistically.

Product counterfeiting and (especially) product tampering are going to get a lot worse, including terrorist acts.

For many pharma manufacturers, there is a Due Diligence problem for tampering & counterfeiting.

Don't underestimate virtual numeric tokens!

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

-- Dan Philpott

Common Facility & Organizational Security Mistakes/Vulnerabilities

Blunder: Poor Insider Threat Countermeasures

- Employee disgruntlement is a risk factor for workplace violence, sabotage, theft, espionage, and employee turnover.
- While disgruntlement is certainly not the only insider threat motivator, it is an important one.

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

Blunder: Poor Insider Threat Countermeasures

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

Employee perceptions are the only reality!

The human-resources trade long ago proved itself, at best, a necessary evil—and at worst, a dark bureaucratic force that blindly enforces nonsensical rules, resists creativity, and impedes constructive change. -- Keith H. Hammonds

Blunder: Poor Insider Threat Countermeasures

- Not managing expectations
- Not being prepared for domestic violence coming into the workplace
- Not watching for the usual precursors to insider attacks due to disgruntlement, especially sudden changes in:
  - use of drugs or alcohol
  - signs of aggression or hostility
  - not getting along with co-workers
  - performance levels
  - being late for work or no show

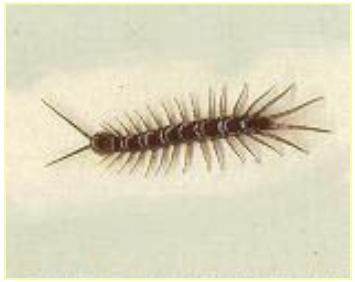
Blunder: Poor Insider Threat Countermeasures

- Not testing if your employees can be bribed
- Insufficient, non-periodic background checks
- Thinking that only your employees are insiders
- Thinking that low-level employees are not a major threat
- Polygraphs
- Not publicly prosecuting insider offenders

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

-- *Third Rock from the Sun*

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")

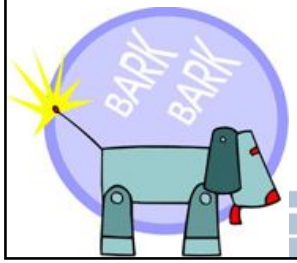
- Increases complexity.
- Multiple layers of bad security do not equal good security.
- It's unlikely the adversary has to defeat all the layers.
- Often mindlessly applied: the layers are not automatically backups for each other. They may have common failure modes, or even interfere with each other.
- Leads to complacency.
- Tends to be a cop-out to avoid improving any 1 layer or thinking critically about security.
- Often a knee-jerk response when security is poor or hasn't been thought through.

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

Cargo & Supply Chain Security

Realities of Cargo Security Technology 1

- High-technology is almost certainly not the answer to your security problems.
- If you can't respond in real-time (immediately), you don't need real-time monitoring or a real-time alarm.
- Most cargo real-time monitoring or hijack alarm devices are really about recovering the truck, not the cargo.
- Professional cargo thieves can empty a truck in 5 minutes and/or can block alarm signals.



If you think that technology can solve your security problems then (1) you don't understand your problems and (2) you don't understand the technology. -- Bruce Schneier

Realities of Cargo Security Technology 2

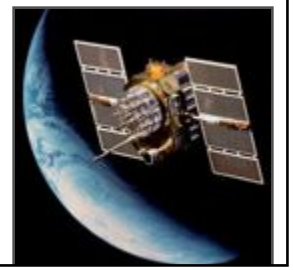
It's dumb to lock or seal the door handle, but that is what we usually do.

Locking Bars

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

You have to be careful if you don't know where you are going because you might not get there. -- Yogi Berra



GPS (and Other) Jamming

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.
- The risk: cargo theft, tampering with financial & security time stamps, crashing national networks (utilities, telecommunications, computer).

GPS Spoofing

GPS Spoofing

GPS Spoofing

(Spoofing can be detected for ~$15 of parts. But there is little interest.)

Tamper Indicating Seals

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.

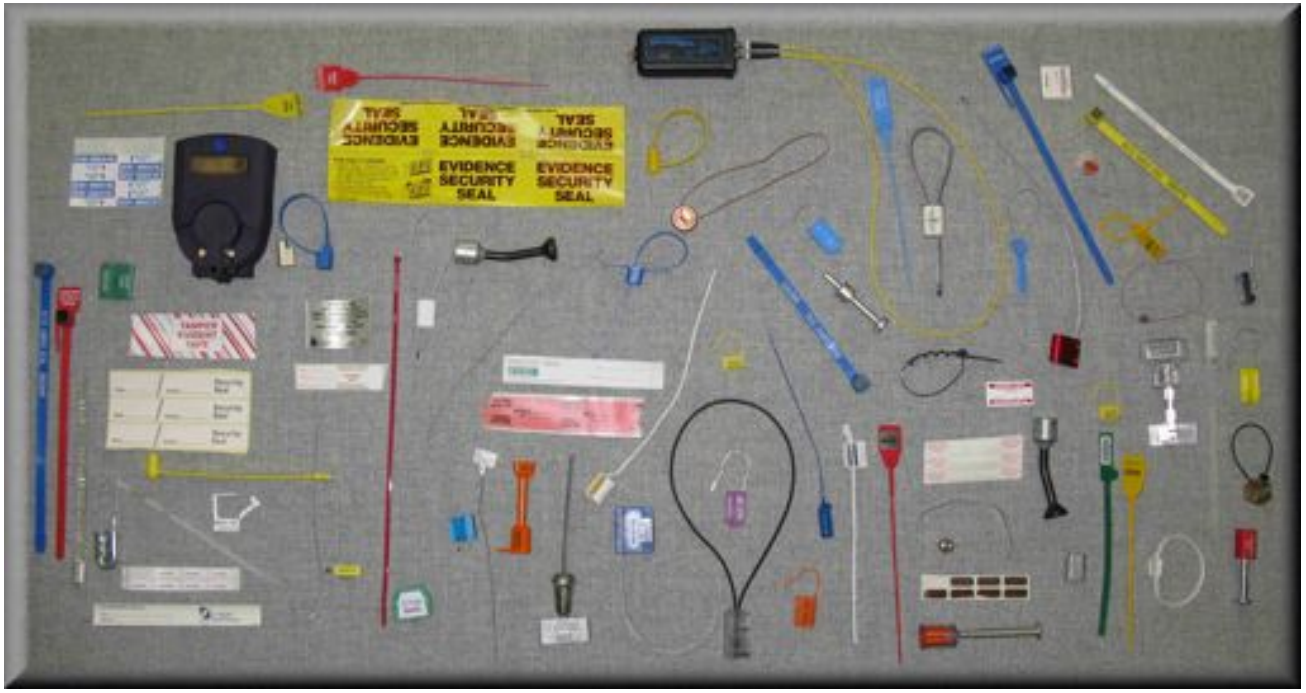
Terminology

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 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. No seal is “tamper-proof” or “tamper-resistant”. This is bad terminology.

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

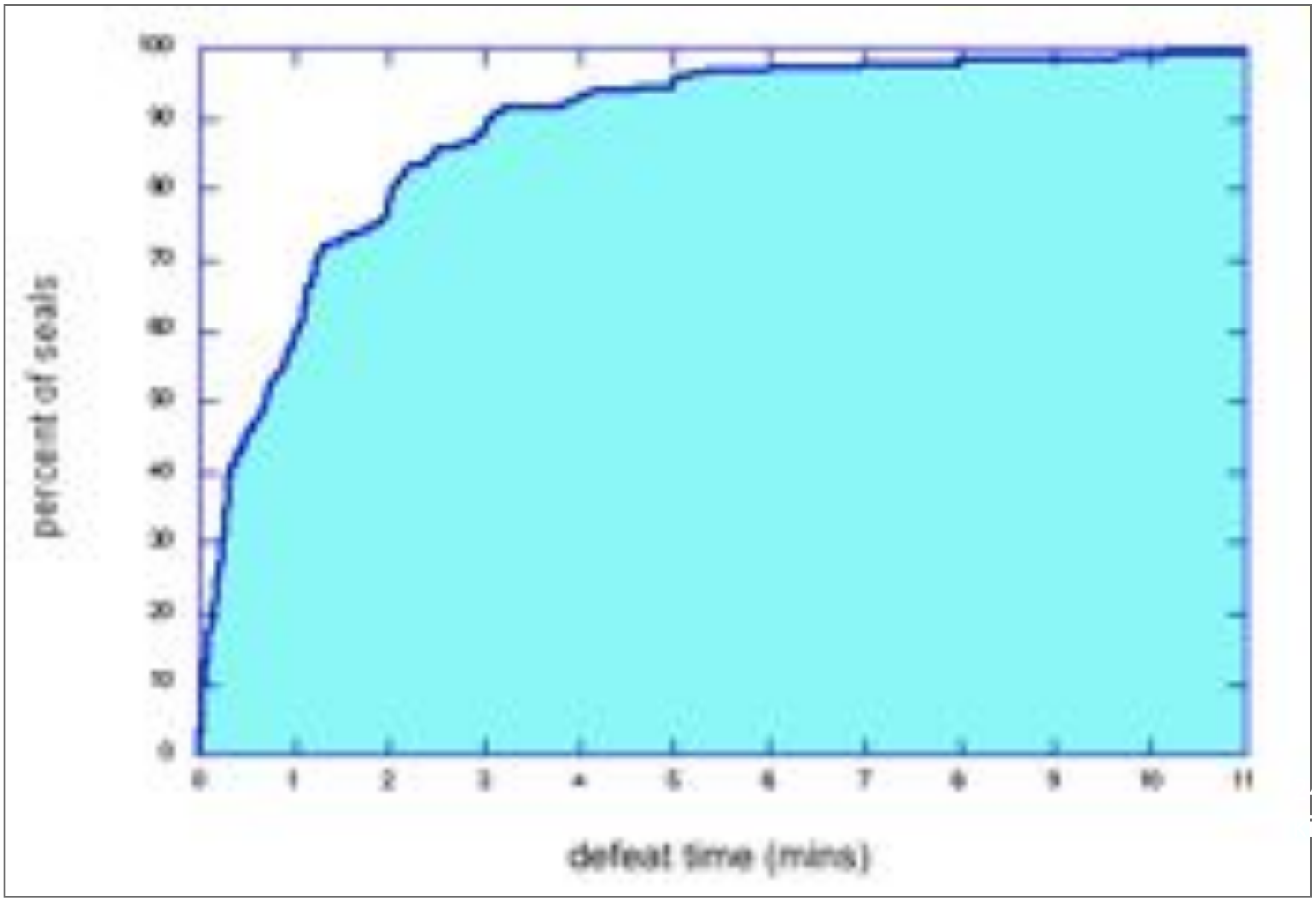
3. A seal must be inspected, either manually or with an automated reader, to learn anything about tampering or intrusion. The person doing this must know exactly what they are looking for.

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.

It’s better to be looked over than overlooked.
-- Mae West (1893-1980) in
Belle of the Nineties, 1934

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



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 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.

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.

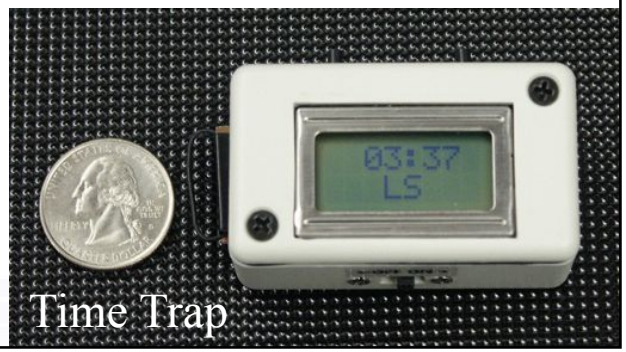
Don't play what's there, play what's not there.
-- Miles Davis (1926-1991)

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"

Tie Dye Seal

Chirping Tag/Seal



Time Trap

Talking Truck Cargo Seal:
A Password, Anti-Evidence, Audio Seal

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

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

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!

Tampering with Urine Drug Tests

It's easy to tamper with urine test kits.

Most urine testing programs (including for world class 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.

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

Tamper-Evident Packaging

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 a seal

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

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

Pharma Counterfeiting and Anti-Counterfeiting Tags

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.]

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 (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.

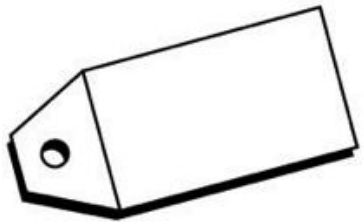
It is estimated that only 1% of “Louis Vuitton” designer handbags are authentic.

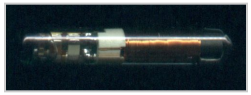
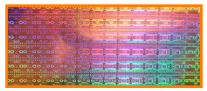
Blunder: Wrong Assumptions about Counterfeiting

- 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) counterfeit the apparent performance of the product or the security device, not the thing itself, or its real performance.

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

Common Anti-Counterfeiting Tags



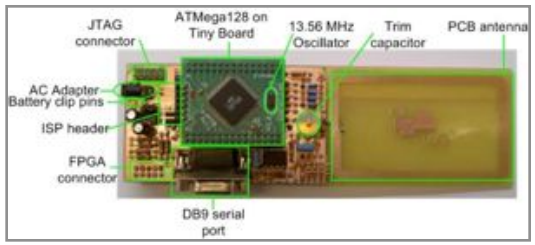
- RFIDs 
- holograms 
- color changing films 
- covert marks, inks, or micro-patterns (secret tags)
- taggants

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

A Sampling of RFID Hobbyist Attack Kits Available on the Internet

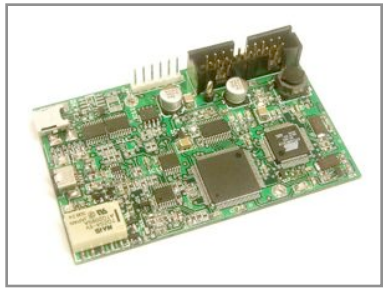
Commercial: $20 Car RFID Clone (Walmart)

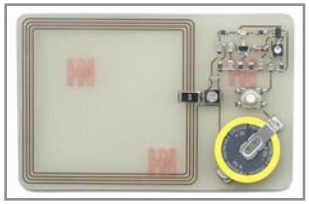
Commercial: Used for "faking RFID tags", "reader development."

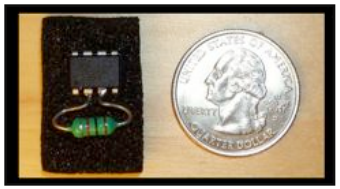


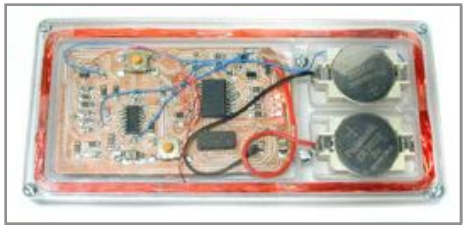
RFID Skimmers, Sniffers, Spoofers, and Cloners; oh my!

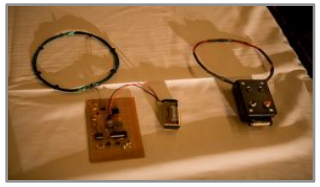
Documents, code, plans needed to build your own: free.

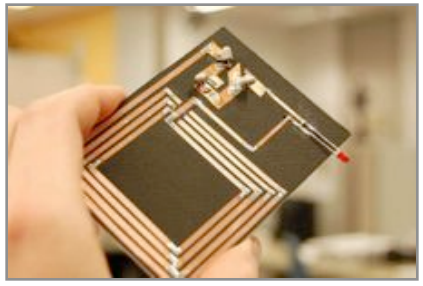


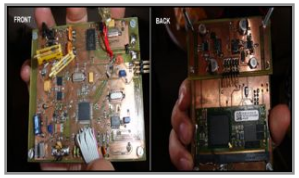










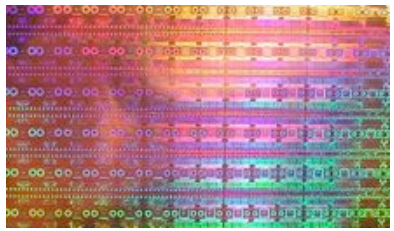


There is a huge danger to customers using this (RFID) technology, if they don't think about security.
-- Lukas Grunwald (creator of RFDump)

(Incidentally, Prox Cards are RFIDs!)

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

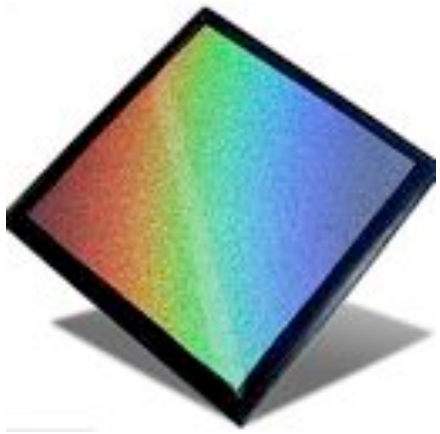
The Problems with Holograms



- easy to counterfeit (See, for example, http://www.nli-ltd.com/publications/hologram_counterfeiting.php)
- embossed (stamped) holograms are especially trivial to duplicate
- easy to fool consumers & harried pharmacy techs with flashy colors
- 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 & harried pharmacy technicians.



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

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

Everything secret degenerates…nothing is safe that does not show how it can bear discussion and publicity.
-- attributed to Lord Acton (1834-1902)

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.

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

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.
- 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.

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

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

Taggants

- 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

handheld X-ray
fluorescence

FTIR

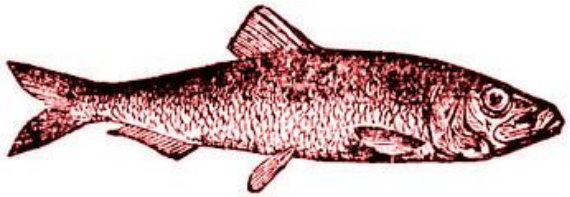
ultrafast GC

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

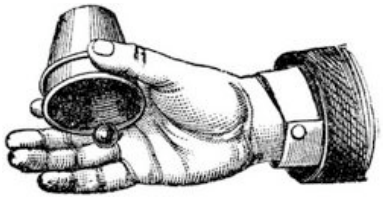
Warning: Encryption has little or no role to play in counterfeit detection!



It's a red herring.

It's snake oil.

It's smoke & mirrors.



It has nothing to do with the real problem.

It's often invoked in other kinds of security applications when good solutions & careful thinking are lacking.

Virtual Numeric Tokens

Imagine an Anti-Counterfeiting Tag That...

1. Is inexpensive & unobtrusive.
2. Is very difficult to counterfeit in large numbers.
3. Can be checked by pharmacies, hospitals, and wholesalers automatically (using an inexpensive reader).
4. Can be checked by consumers (without a reader).
5. Typically detects more than 98% of the fakes examined.
6. Does not become easier to defeat over time, or as technology advances.

The pursuit of perfection often impedes improvement.
-- George Will

"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

CONCEPT ARTICLE

Int J Pharm Med 2005; 19 (3): 163-171
1364-9027/05/0003-0163/$34.95/0

An Anticounterfeiting Strategy Using Numeric Tokens

Roger G. Johnston

Los Alamos National Laboratory, Vulnerability Assessment Team, Los Alamos, New Mexico, USA

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.

Radisson Welcomes
Emerging Infectious Diseases

-- Sign outside a Radisson Hotel

CNT Technique (con't)

- **"Calling-in":** Customers log into a web site, or call an automated phone line 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

Wine Authenticity:
Detects Tampering & Counterfeiting

Pharma Problems & Time Bombs

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
- Lessons of 1982 Tylenol poisonings (e.g., be above board) are forgotten (per J&J 2010)
- 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

I don't want any yes-men around me. I want everyone to tell me the truth—even if it costs him his job.

-- Samuel Goldwyn (1879-1974)

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).

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 (1985? – 1964)

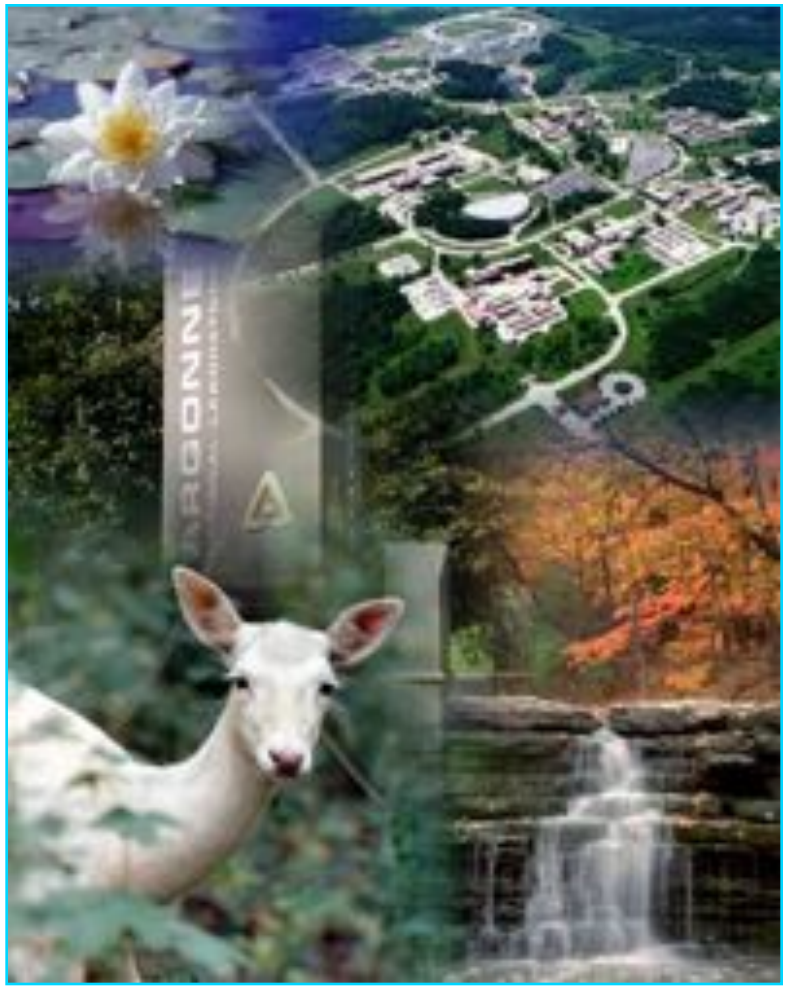
Other Pharma Security Problems

- ✓ 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?

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

For More Information...



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

Related papers, reports, and presentations are available today on CD or from rogerj@anl.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)

Supplemental material not part of the initial talk...

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, or 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)