Better Approaches to Physical Tamper Detection

Roger G. Johnston, Ph.D., CPP
Jon S. Warner, Ph.D.

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, ~3000 employees, $630 million annual budget
R&D and technical assistance for government & industry

Argonne
NATIONAL
LABORATORY

... for a brighter future

U.S. Department of Energy

UChicago ▸ Argonne LLC

A U.S. Department of Energy laboratory managed by UChicago Argonne, LLC

Vulnerability Assessment Team (VAT)

Sponsors

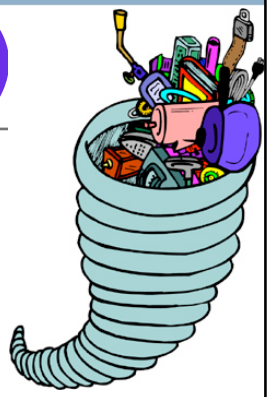
- DHS
- DoD
- DOS
- IAEA
- Euratom
- DOE/NNSA
- private companies
- intelligence agencies
- public interest organizations

A multi-disciplinary team of physicists, engineers, hackers, & social scientists.

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)

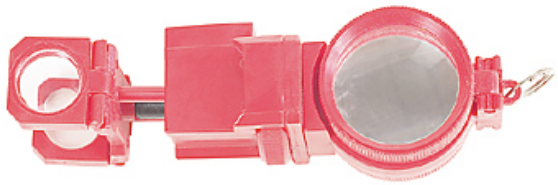
Our R&D and Other Projects (1)



- Seals & Tamper/Intrusion Detection
- Cargo security
- First to show how easy it is to spoof, not just jam GPS. First to suggest countermeasures.
- Defeats of a number of different biometric and other access control devices (many different ways).
- Attacks on RFIDs & contact memory buttons
- Sticky bomb detection
- Demonstrated attacks on an electronic voting machine from the voters' end.

Our R&D and Other Projects (2)

- Product authenticity (especially wine & pharmaceuticals)
- Questioning the security of urine drug tests
- Better ways to protect logged/monitoring/surveillance data
- Nuclear Safeguards
- Special Field Tools
- Vulnerability Assessments
- Consulting & Security Training
- Human Factors in Security / Security Culture & Climate



Terminology

-"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*

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

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

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

7,000+ years of sealing

early stamp seal, ~3500 BC

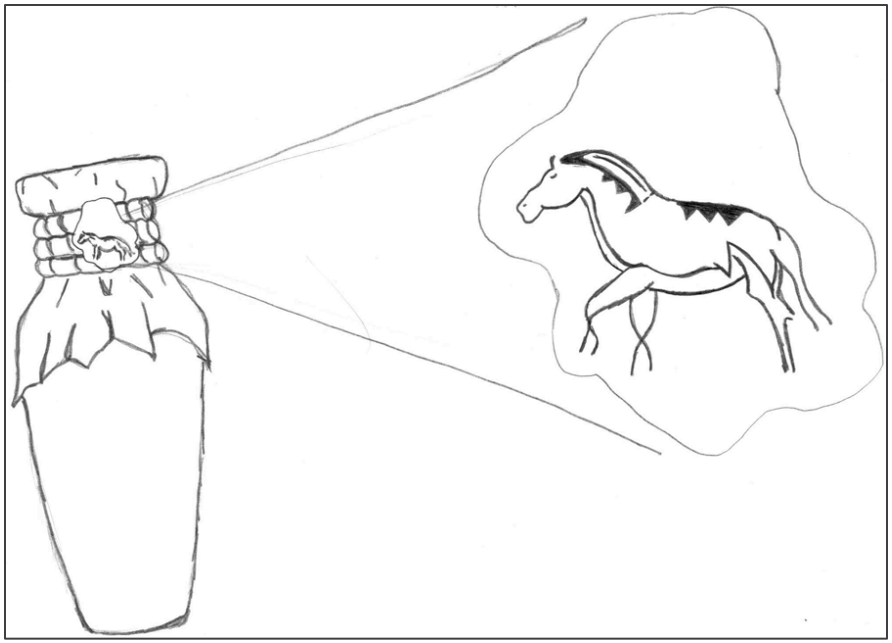
cylinder seal, Mesopotamia, ~2400 BC

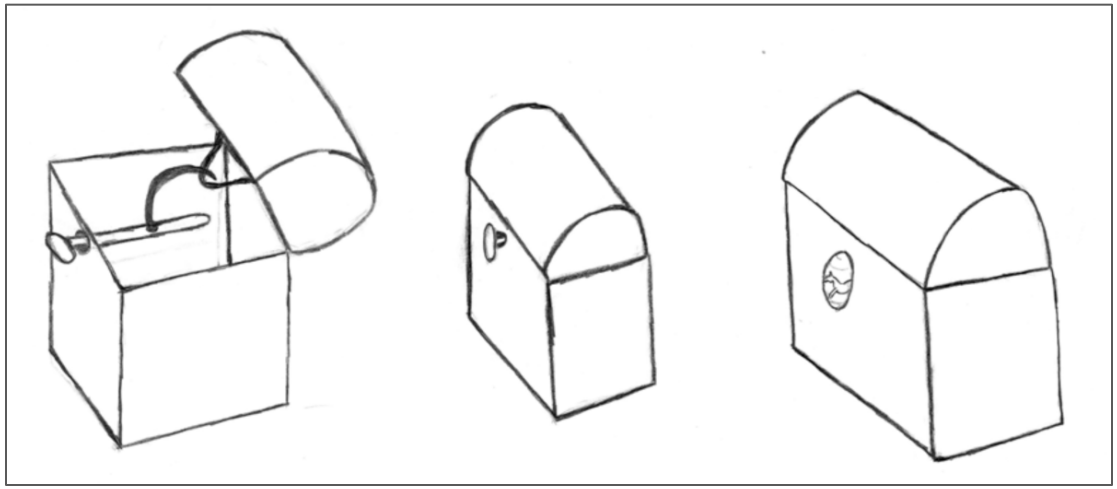
Minoan signet ring, ~1500 BC

papal lead seal, ~1100 AD

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

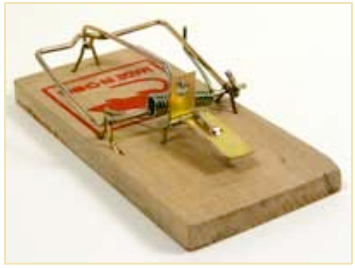
7,000+ years of sealing





Terminology (con't)

trap: a covert seal.



barrier seal: a lock and a seal in 1 device.

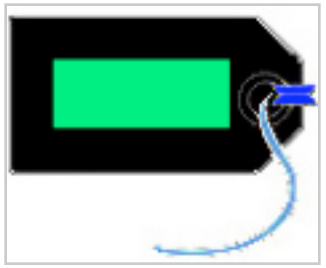
I think the inventor of the piñata may have had some unresolved donkey issues.

-- Dan Johnson

Terminology (con't)

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.

Factoid: Damn Yankees

A seal is not a lock. Yanking a seal off a container is not defeating it because the fact that the seal is missing or damaged will be noted at the time of inspection.

Factoid: Seal Minimum Requirements

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

2. You have to inspect a seal, either manually or with an automated reader to learn anything about tampering or intrusion.

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

Factoid: That Weird Human Factor

Defeating seals is mostly about fooling people, not defeating hardware.

(Unlike locks, safes, vaults, etc.)

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)

Factoid: The Recipe is Everything

A seal is no better than its “use protocol”...

...how the seal is:

- manufactured
- procured
- shipped
- stored
- installed
- inspected
- removed
- disposed of

- And how the seal data is protected and
- How the seal installers/inspectors are trained.

> All methodologies are based on fear.
> -- Kent Beck

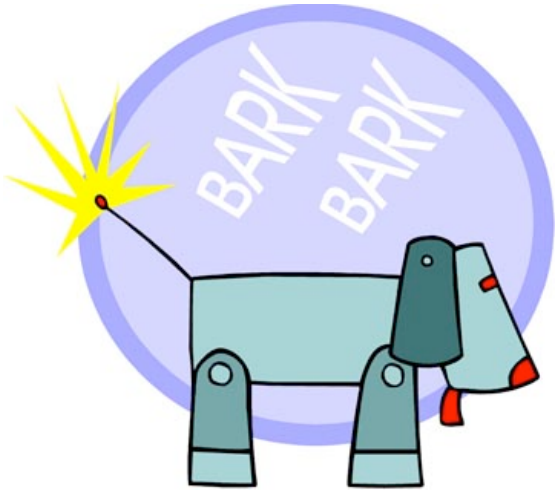
Terminology (con't)

real-time monitoring, intrusion detector, or "burglar alarm": an alarm sounds immediately when there is unauthorized entry or tampering.

> More warnings issued by all branches of the government today that another terrorist attack is imminent. We're not sure when, we're not sure where, just that it is coming. Who is attacking us now, the cable company?
>
> -- Jay Leno

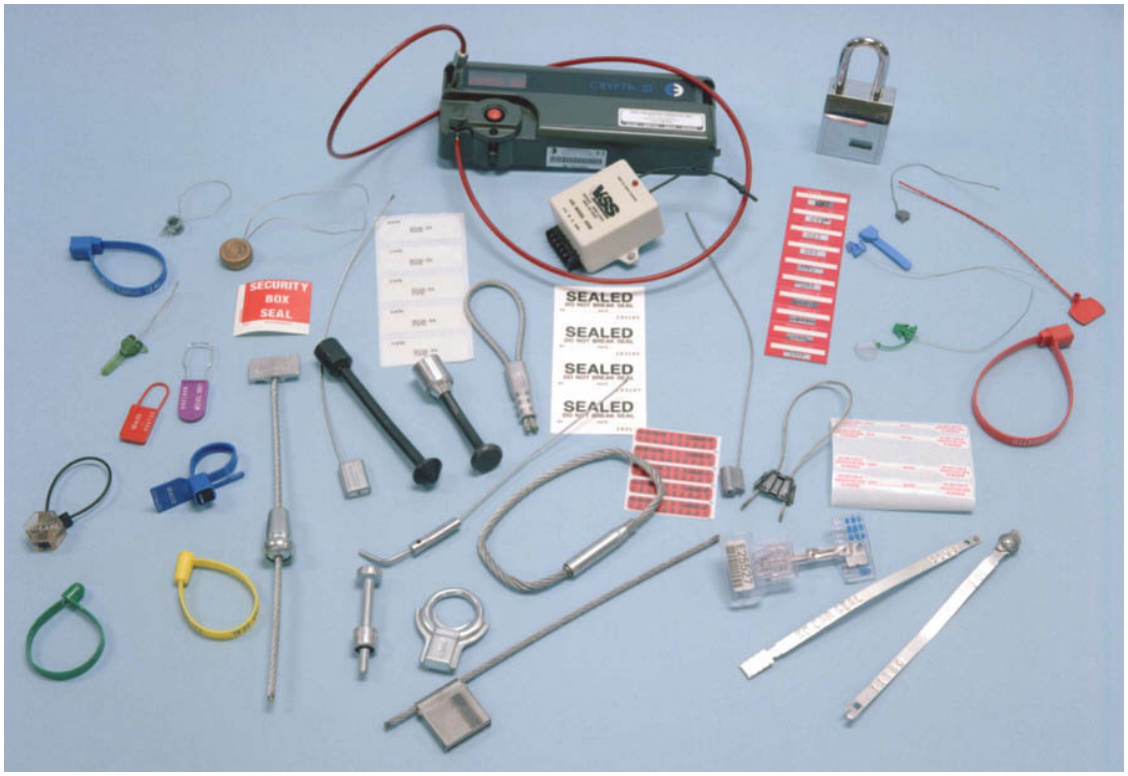
Factoid: What's Your Hurry?

If you can't respond immediately,
you don't need real-time monitoring or a real-time alarm.



If I had more time, I would write a shorter letter.
-- Blaise Pascal (1623-1662)

Seals



Some of the 5000+ commercial seals

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
- protecting medical sterilization
- protecting instrument calibration
- waste management & hazardous materials accountability

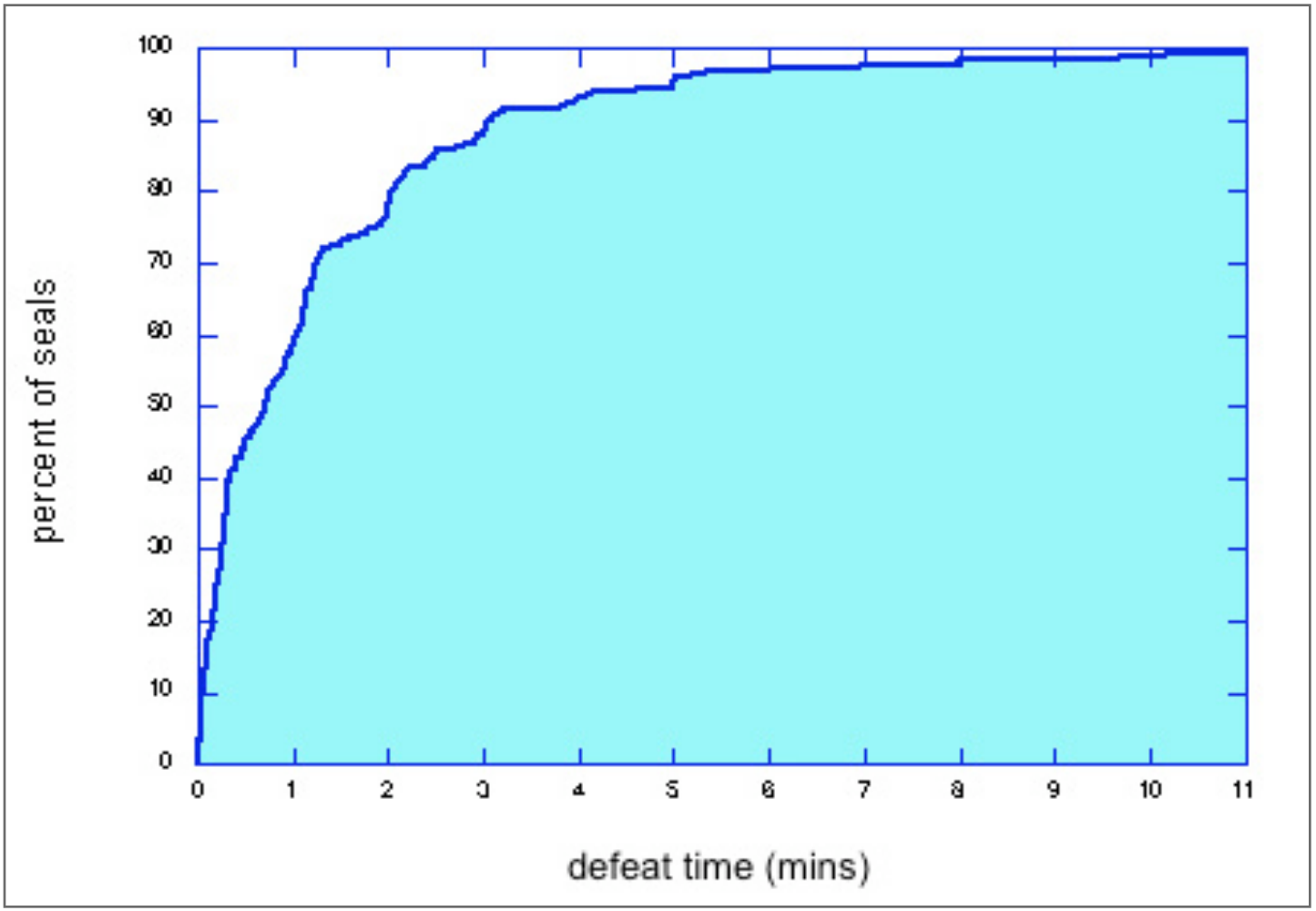
Seals Vulnerability Assessment

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.

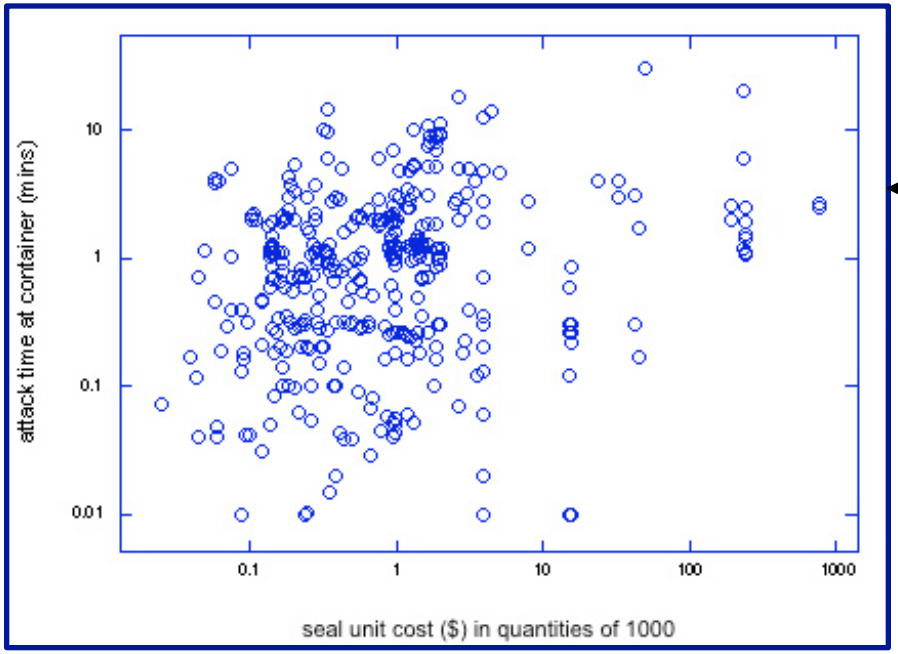
Seals are easy to defeat: Percent of seals that can be defeated in less than a given amount of time by 1 person using only low-tech methods



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

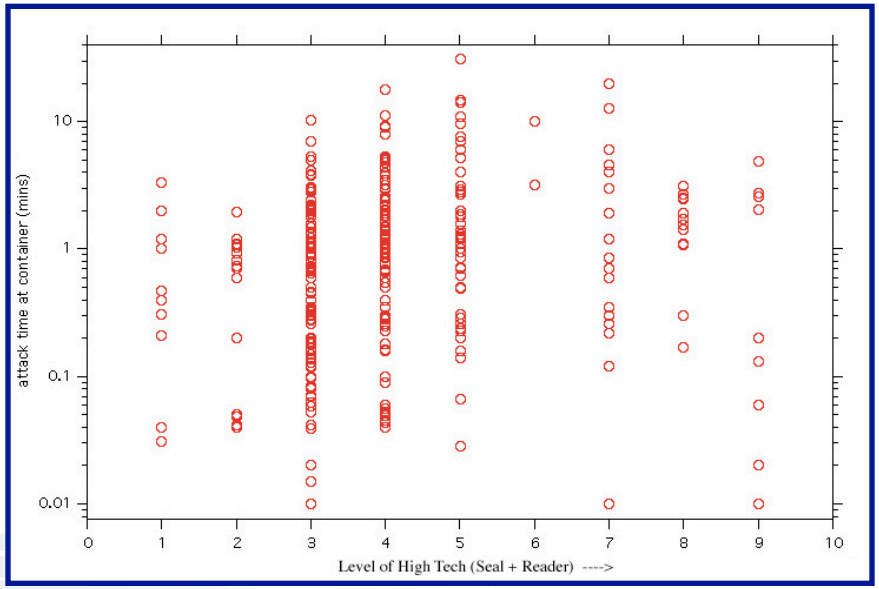
High Tech Isn't Automatically Better!



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

393 attacks

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



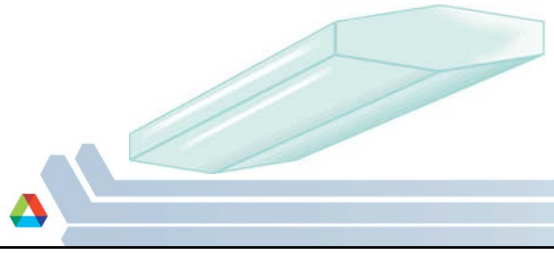
Some of the 105+ General Seal Attack Methods*

- "pick" open
- replicate (at or by the factory)
- counterfeit (whole or parts)
- repair the opened seal
- tamper with the seal data
- tamper with the seal reader
- deploy insider installers or inspectors
- backdoor attacks
- put on a different kind of seal with the correct original serial number

*RG Johnston & ARE Garcia, "An Annotated Taxonomy of Tag and Seal Vulnerabilities", *Journal of Nuclear Materials Management* **229**, 23-30 (2000)

For electronic seals, these attacks are also common:

- man-in-the-middle
- hijack the display (seal or reader)
- spoof the reader at a distance (especially when rf communication is involved)
- attack the power or quartz crystal



Game Show Host: What travels at three hundred million miles a second?
Contestant: A cheetah?

Factoid: Fake Counterfeits

Counterfeiting security devices is usually easier than developers, vendors, & manufacturers claim.

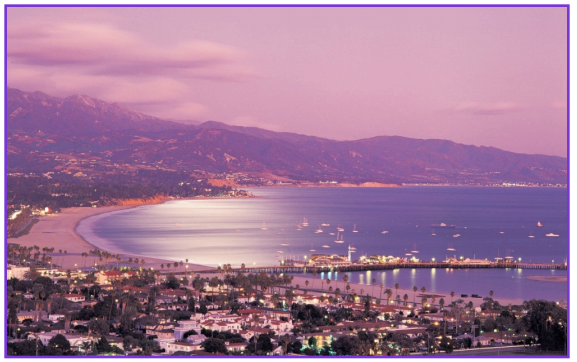
Often overlooked: The bad guys usually only needed to mimic the superficial appearance and *maybe* the apparent performance of the security device, not the device itself.

Sincerity is everything. If you can fake that, you've got it made.

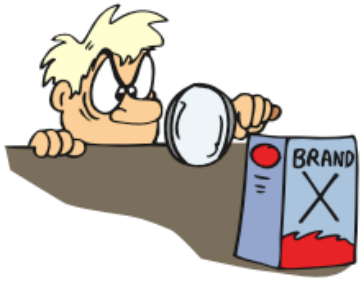
-- George Burns (1885-1996)

Tamper-Evident Packaging Test

7th Security Seals Symposium
Santa Barbara, CA
February 28 - March 2, 2006



- 71 tamper detection experts participated.
- A VAT college student (Sonia Trujillo) did the product tampering using only low-tech attacks.



"Do not eat if seal is missing."
-- actual printing on the seal

Results:

On a bag of Fritos:
"You could be a winner!
No purchase necessary.
Details inside."

statistically the same as random guessing!

Factoid: Find Another Hobby?

Sealsport: Defeating seals is probably not a very interesting hobby: currently too easy. (Maybe speed defeating?)

Plus, what use protocol do you test to?

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

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!

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

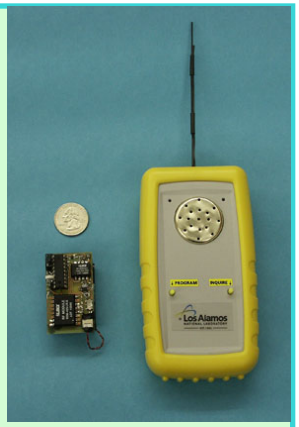
Conventional Seal: Stores the evidence of tampering until the seal can be inspected. But this 'alarm condition' is easy to erase or hide (or a fresh seal can be counterfeited).

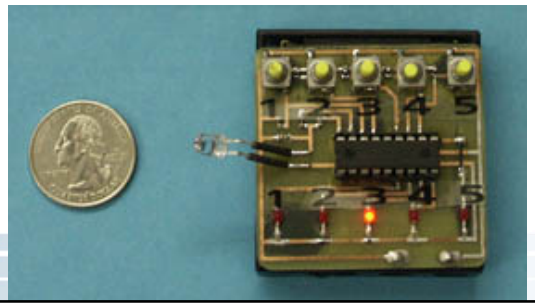
Anti-Evidence Seal: When the seal is first installed, we store secret information that tampering hasn't been detected. This is deleted when the seal is opened. There's nothing to erase, hide, or counterfeit.

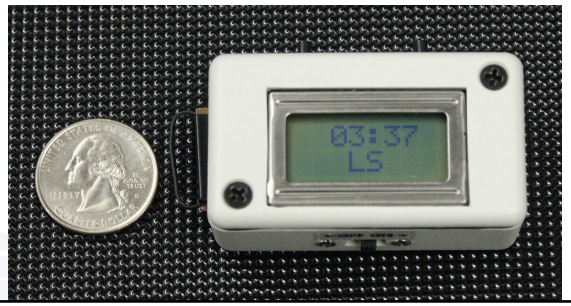
Don't play what's there, play what's not there.
-- Miles Davis (1926-1991)

20+ New “Anti-Evidence” Seals

- better security
- no hasp required
- no tools to install or remove seal
- no hardware outside the container
- 100% reusable, even if mechanical
- can monitor volumes or areas, not just portals
- “anti-gundecking”
- the bad guys can check the seal for you







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

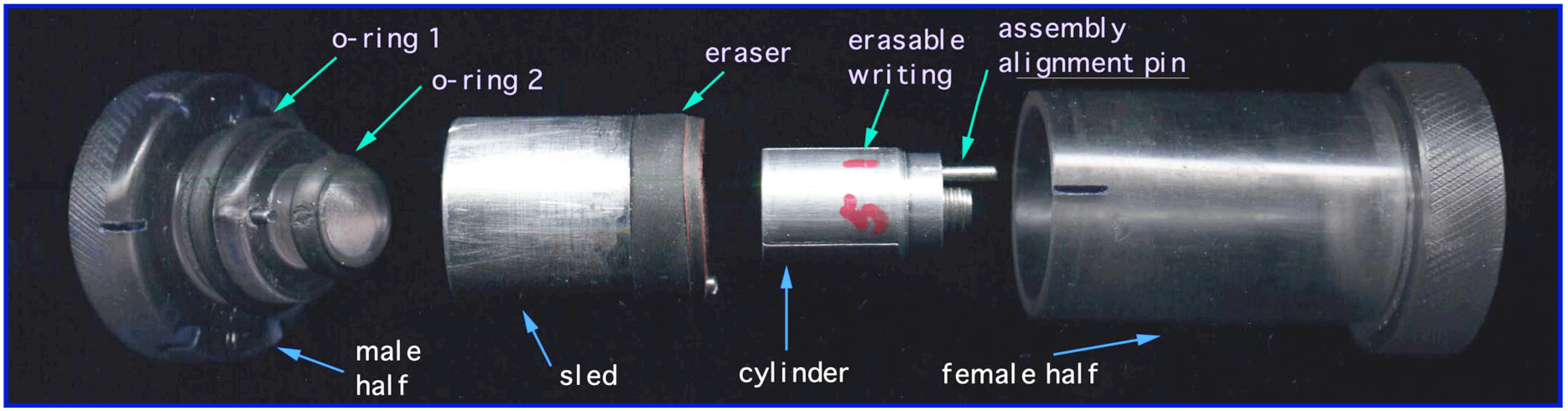
Seal: $15 of parts (retail)
Reader: $40 of parts (retail)

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

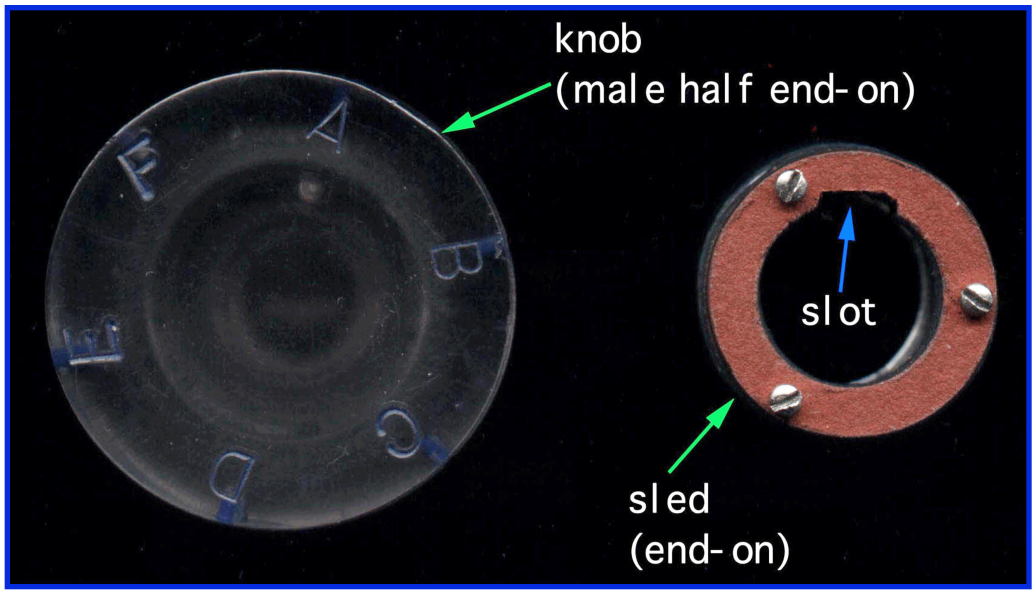
Talking Truck Cargo Seal: Sample Slogans

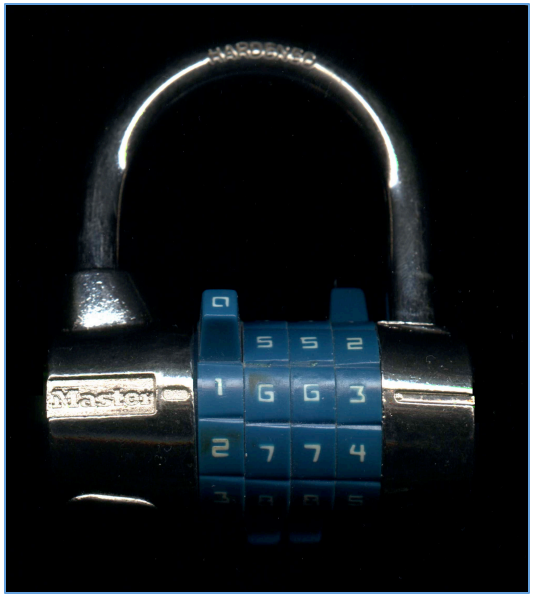
- At Least One Fire Extinguisher per Dozen Trucks
- The Best People You Can Hire for $8 an Hour
- The Center Lane Marker is Only a Suggestion
- Amphetamines Aren't for Amateurs
- We Break for Small, Furry Animals
- Not in Front of the Teamsters!
- Mad Max Works for Us
- We Eat Our Road Kill
- The "Go"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

Magic Slate Seal: A Mechanical Anti-Evidence Seal



side view





end view

Time Trap ("Xmucane Seal"): An Anti-Evidence Seal That Uses an Authentication Hash

- No reader.
- Check hash with a PDA, computer, or handheld unit.
- Or report time & hash via non-secure channels.
- ~$6 of parts (retail)
- can be both a seal & a tag

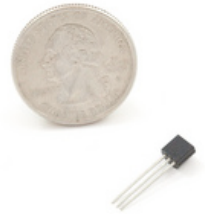
"You mean *now*?"
-- Yogi Berra when asked for the time of day

Wine Authentication:
Checks for Both Counterfeiting and Tampering

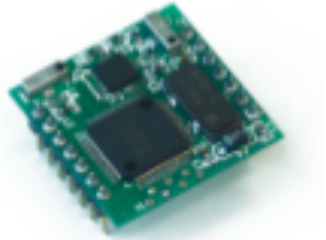
Some Low-Cost Commercial Sensors

Hall Effect magnetometer, ~$0.85

PIR motion, ~$8

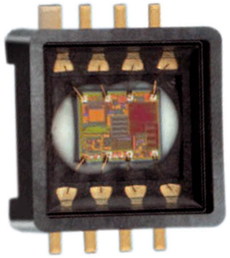


1-wire temperature, ~$4



high-resolution, 2-axis magnetometer, ~$60

color sensor, ~$9



barometric pressure, ~$4

thermistor, ~$0.80

temperature & humidity, ~$13

O2 sensor

force sensor, ~$4

gyro (angular rate sensor), ~$23

IR proximity, ~$13

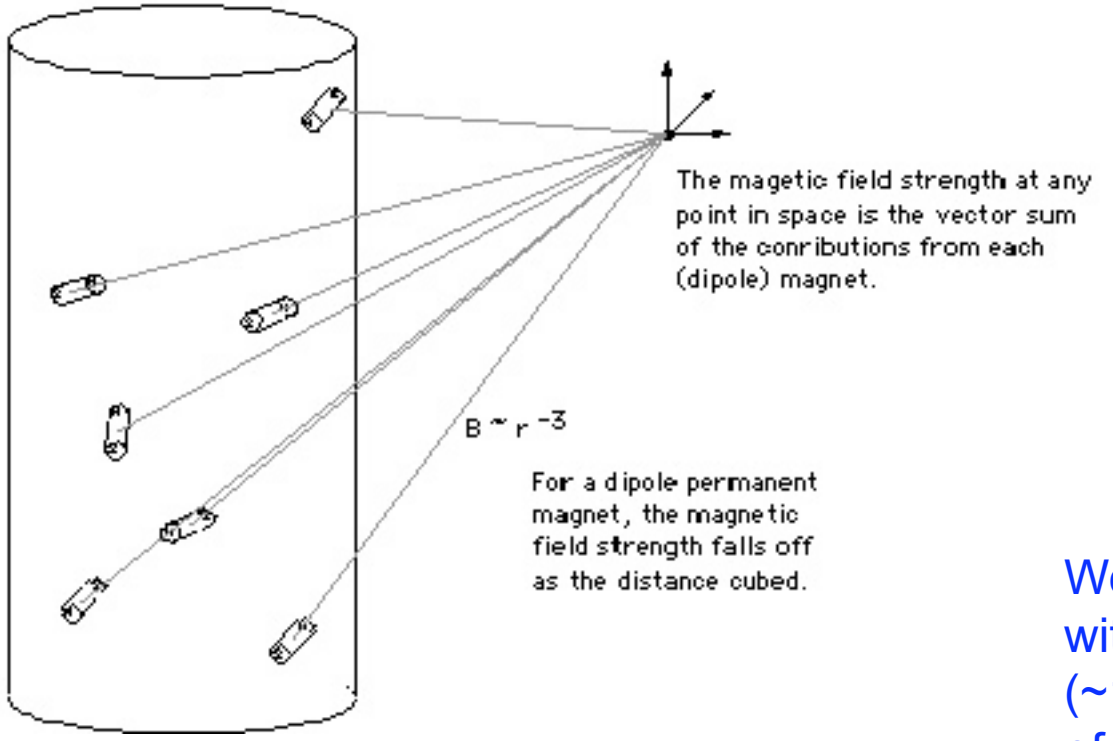
triple axis accelerometer, ~$8

vibration sensor, ~$2.50

MagTag

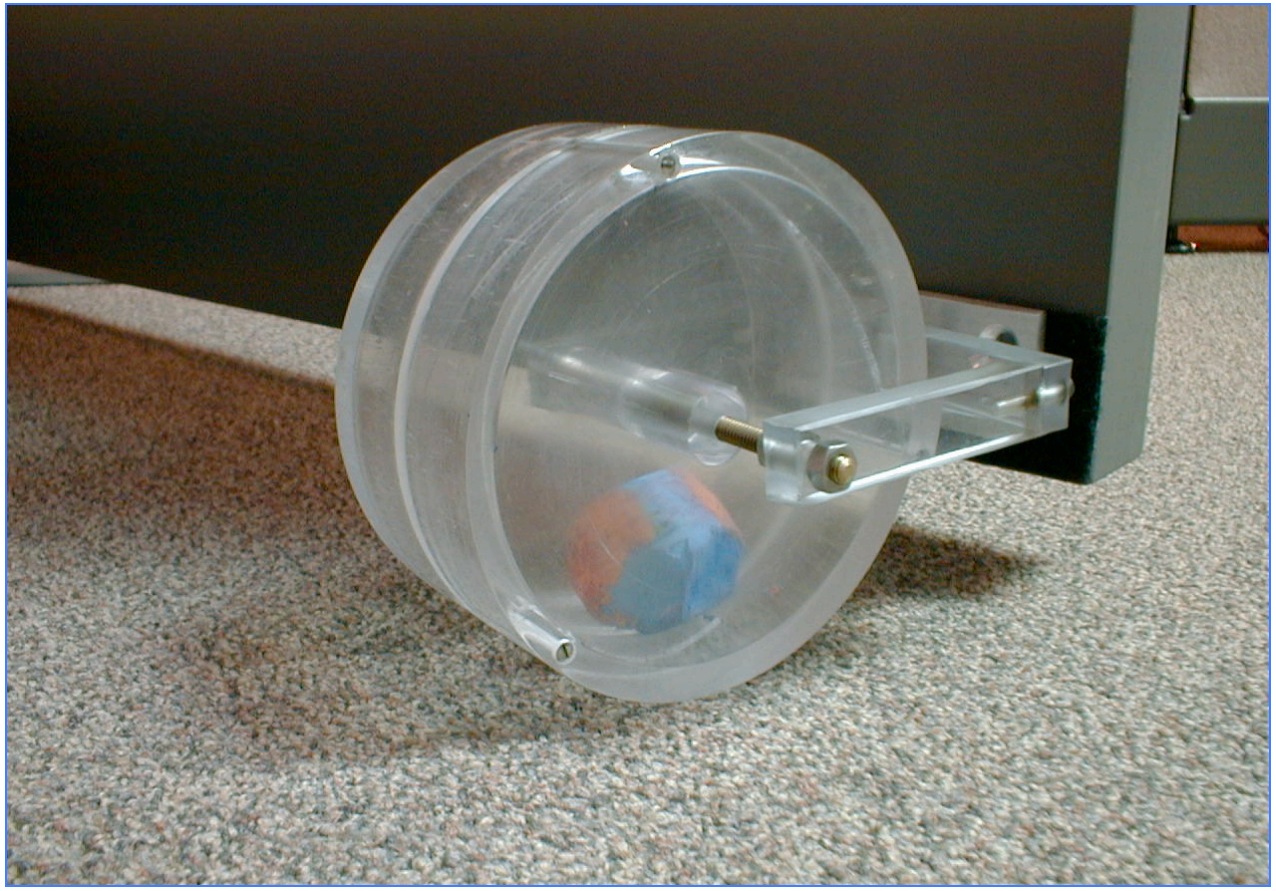
Place a number of magnets of various strengths in random locations and orientations inside a container. DC magnetic fields are virtually unattenuated by most materials, including most metals.

US patent 6,784,796

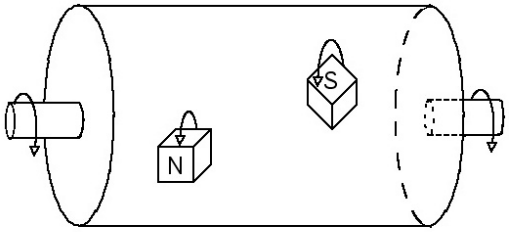


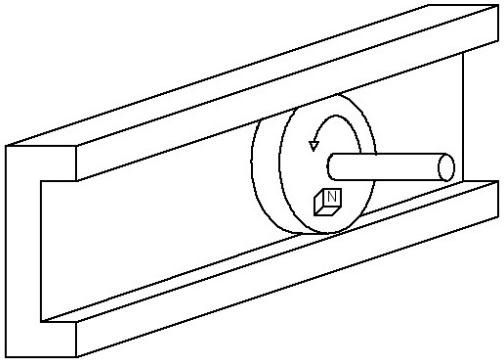
We read the DC magnetic fields with an inexpensive magnetometer (~15 nT resolution vs. Earth's field of 55,000 nT).

Hysteresis MagTag Designs



“hamster wheel”

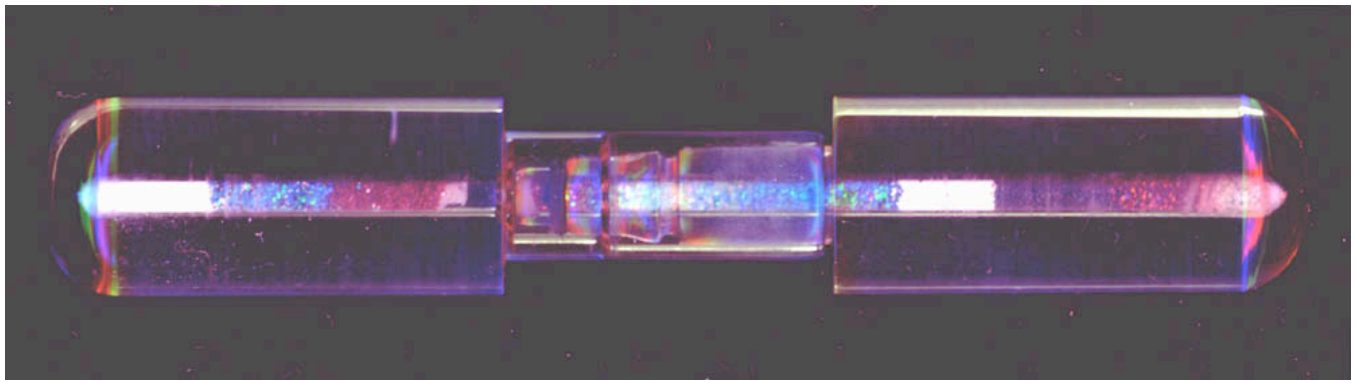




Beads-In-A-Box Volumetric Seal

- simple
- low cost
- fully reusable
- difficult to defeat
- volumetric tamper detection, not just portal
- exploits blink comparators

Glass & Powder Seal



- Strong, highly tempered glass.
- Disintegrates if anybody attempts to drill, saw, dissolve, or cut it.
- Uses the many advantages of glass: cheap, inert, corrosion resistant, transparent, strong, hard, brittle, tricky to repair, unique chemical fingerprints.

US patent 6,553,930

Problems with Anti-Evidence Seals

~ Nobody is interested in better seals.

Require more work than most seal users currently do.

Battery life.

There are secret key, hash, or password control and erasure issues.

Which sensors and how many?

Sneaking past the sensors.

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

Reliability & False alarm rates?

Our prototype designs may not be the best implementation of anti-evidence.

Town Crier Monitoring:
The Anti-Evidence Approach to Real-Time Monitoring

Don't sound an alarm (which can be easily blocked), send an occasional "All OK" bit or byte instead. Only the good guys know the correct value at any given time.

- Simple
- Low-cost
- Surreptitious
- High levels of security
- Ideal for moving cargo
- Very tolerant of communications noise
- Very low communications bandwidth (byte/sec to bit/min)

For More Information on Physical Security

Common and dangerous security mistakes (and their countermeasures):

RG Johnston & JS Warner,
Handbook of Security Blunders
(due out shortly)

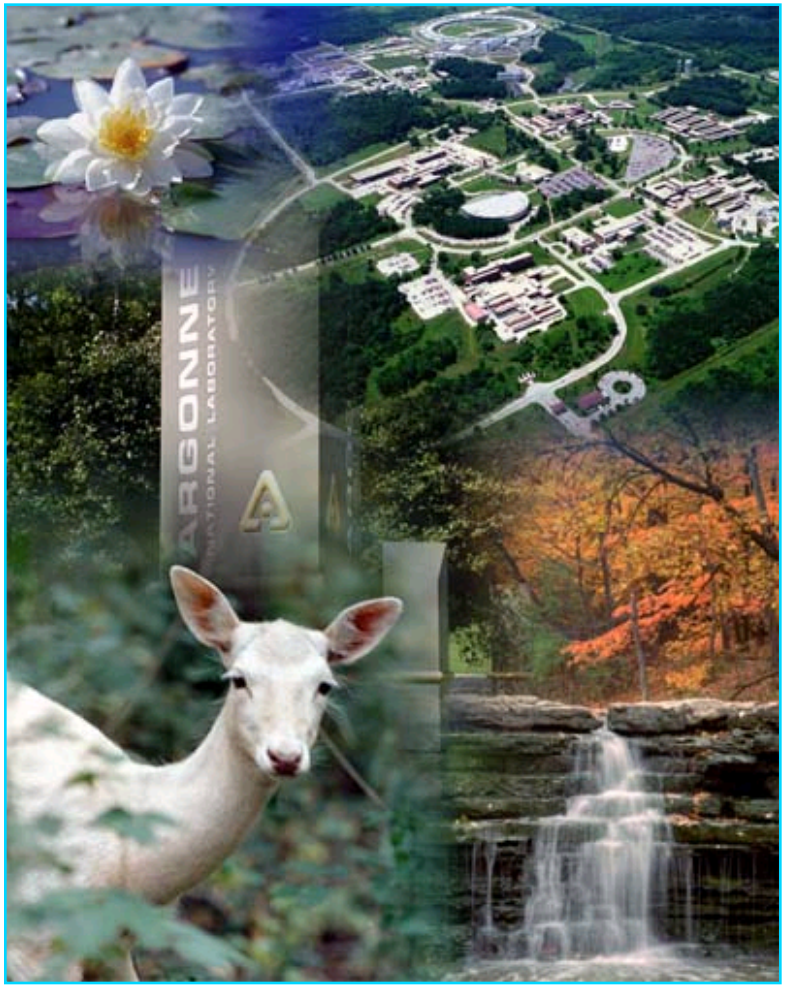
We made too many wrong mistakes.
-- Yogi Berra

The Journal of Physical Security

http://jps.anl.gov

(A free, online, peer-reviewed R&D journal)

Also...



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

Papers, reports, & presentations by the Argonne VAT are available for download at:

http://public.me.com/va_team

password = kevinkevin

Rat complaints have gone up, but we look at that as a positive thing, because more people know how to contact us now.
-- New York City pest control bureaucrat