Anti-Evidence Seals

Roger G. Johnston, Ph.D., CPP
Jon S. Warner, Ph.D.
Vulnerability Assessment Team
505-667-7414   rogerj@lanl.gov
http://pearl1.lanl.gov/seals

Los Alamos
NATIONAL LABORATORY

LANL Vulnerability Assessment Team

✓ seals, traps & tamper detection
✓ biometrics & access control
✓ computer physical security
✓ RFID & CMB vulnerabilities
✓ tamper-evident packaging
✓ GPS spoofing countermeasures
✓ tags & product anti-counterfeiting
✓ educational & security culture issues
✓ hosting *Journal of Physical Security*
✓ Adversarial Vulnerability Assessments
✓ rapid container sampling tools (3 patents)

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)

Summary

- Current tamper-indicating seals are WAY too easy to spoof.

- That's bad because they are protecting important stuff.

- There are workarounds.

- But much better seals are both needed and possible: Anti-Evidence Seals.

Definitions

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

- seal: a tamper-indicating device (TID) designed to leave evidence of unauthorized access. Seals do not resist entry (like locks), nor do they report trespassing in real-time (like intrusion detectors).

- barrier seal: part lock, part seal; a compromise.
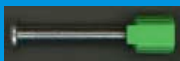
Definitions

➢ <u>trap</u>: a covert seal (such as a seal that is placed inside the container).

➢ <u>tag</u>: a unique identifier of an object or container. There are 4 kinds:
- identification
- security
- anti-counterfeiting
- buddy or token

Definitions

➢ <u>defeating a seal</u>: opening a seal, then resealing (using the original seal or a counterfeit) **without being detected**.

➢ <u>attacking a seal</u>: undertaking a sequence of actions intended to defeat it.

Terminology to Avoid

- ⊗ "tamper-proof" seal

- ⊗ "tamper-resistant" seal

- ⊗ "tamper-deterrent" seal

- ⊗ anti-pilferage seal

- ⊗ security seal vs. indicative seal

Seals Vulnerability Assessments

- ❖ We studied 244 different seals in detail:
  - government & commercial
  - mechanical and electronic
  - low-tech through high-tech
  - cost varies by a factor of 10,000

- ❖ Half are in use for critical applications.

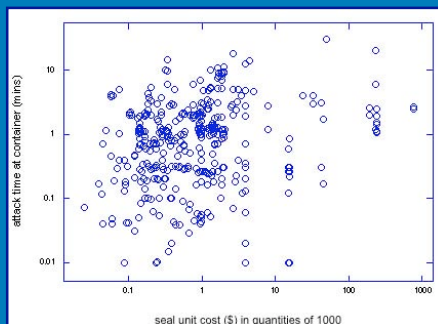- ❖ ~ 19% are used in nuclear security & safeguards.

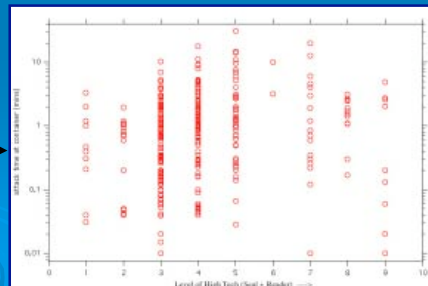**Percent of Seals That Can Be Defeated
in Less Than a Given Amount of Time**
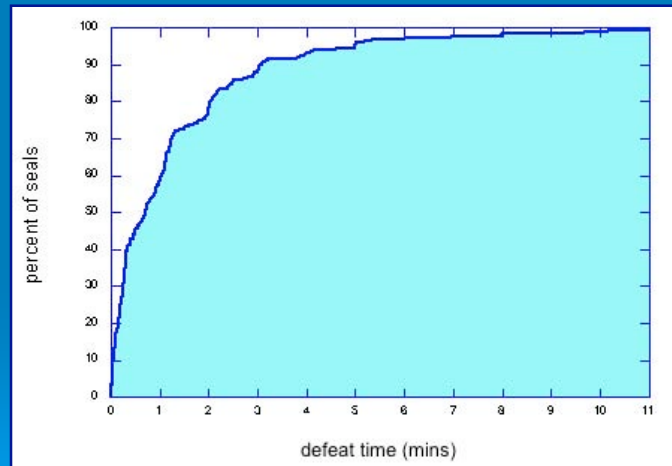
High Tech Isn't Better

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

Countermeasures

27%   13%

60%

cheap & easy
not so cheap & easy
none apparent

393 attacks
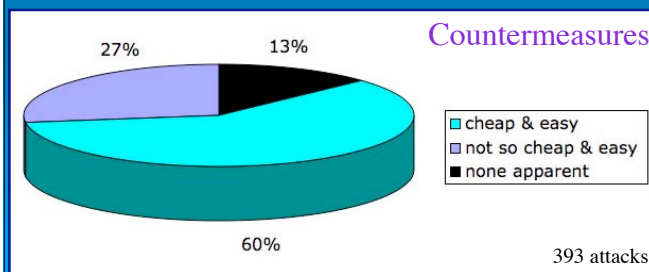
The Good News (con't)

➢ Better seals are 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!

Talking Truck Cargo Seal
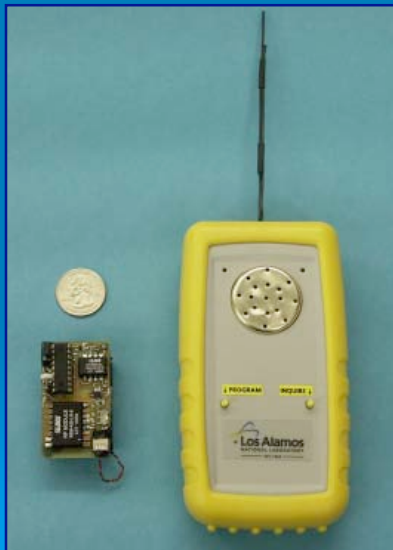
Seal: $20 of parts (retail)
Reader: $45 of parts (retail)

Talking Truck Cargo Seal

- Goes inside the truck or container.
- The reader communicates with the seal through the truck (or container) wall via short-range rf.
- 120-4000 spoken slogans are stored.
- The slogans are not secret, just which one (the "anti-evidence") that was chosen randomly by the electronics for a given cargo shipment.

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 Brake 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!

Near Miss Trucking

Time Trap

- Goes inside the container, or outside on a hasp (with different sensors).

- Exploits 2 facts:
  - The bad guys must enter the container before the good guys inspect the seal.
  - Time travels forward.

- $8 of parts (retail):
  - a clock
  - a microprocessor
  - a battery
  - intrusion sensor

Time Trap

- The seal chooses a random key, K.
- After a countdown (allowing the seal to be placed in the container), monitoring starts.
- The display is blank during monitoring.
- A new hash (value) is computed each minute using K & the current time.

Hash or Hash Value

➢ A fixed length "number" computed from a larger number using a hash algorithm.

➢ Typically, many different numbers yield the same hash value.

➢ For the Time Trap, the hash is 2 letters, computed from the time & K.

Time Trap

➢ Once the opening of the container (by the good guys or the bad guys) is detected:
  • K & the hash algorithm are erased in micro-seconds.
  • The time the container was opened is permanently displayed, along with its corresponding hash value.

➢ Either elapsed shipment time or absolute time can be shown.

➢ The wrong time or hash indicates tampering.

Time Trap

- If the bad guys opened the container first, they don't know:
  - When the good guys will later open the container
  - What the correct hash value is for that time
  - What the K value was--at least 400 different K values produce the same hash for a given time
  - What the hash algorithm was

- The bad guys gain nothing by reverse engineering the microprocessor program and/or counterfeiting the seal hardware.

- To re-use the Time Trap, turn it off, then back on. A new (unpredictable) K value will be chosen by the seal based on the user's µsec response time.

Time Trap

- No reader.
- Check hash with PDA, computer, or handheld unit.
- Or report time & hash via non-secure channels.

LANL Time Trap Hash (Oct 05)

K = 01024

- clock time
- baseline 0 (elapsed time)

max K = 65535

anti-evidence
2 letters, English

Elapsed: Days Hours Minutes
Time: 0 : 3 : 10

Hash: RF

Reset Time to 0:00:00
Reset Time to: 0:00:00

Serial Number 14512
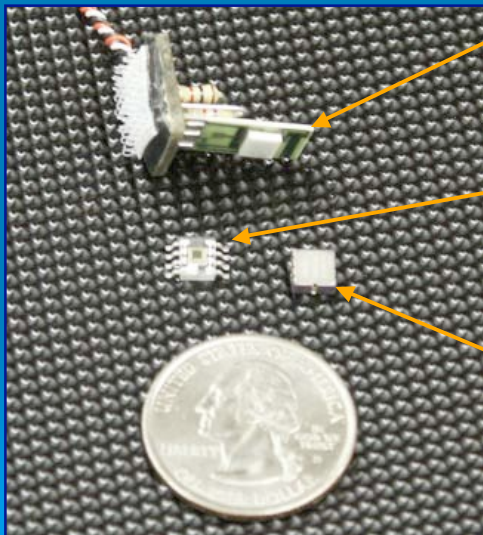Model Number 53022

Update Time/Hash each min

Time Trap

1. Power on.
2. Note the random key (K=36047 in this case).
3. Start countdown & place inside container.
4. For tamper inquiry: Remove the seal from the container. Then check the time & hash (for the correct K value).

Some New Low-Cost, Low-Power Solid State Commercial Sensors

Hall Effect Magnetometer

Honeywell SS94; ~50 nT sensitivity vs 55,000 nT for Earth's field; $13 each in quantities of 1

Color Sensor

TAOS TCS230; remarkable color sensitivity (color is difficult to counterfeit); $3-6 each in quantities of 1

Accelerometer/Tilt Sensor

Memsic MXD2020GL; ~0.001g sensitivity; $9 each in quantities of 1

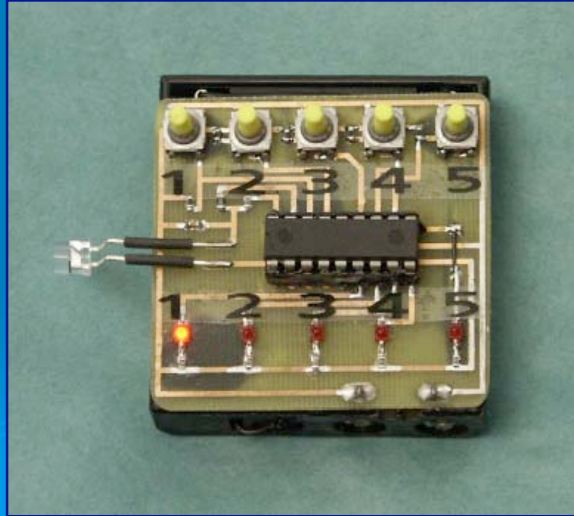Also: light, PIR, sound, ultrasound…

Tie-Dye Bolt Seal

Tie-Dye Door Knob Seal

Blinking Lights Seal

- ➢ $5 of parts (retail)
  - 5 LEDs & 5 buttons
  - microprocessor
  - sensor(s)

- ➢ The seal randomly chooses, then flashes, a 2-digit password & 2-digits of anti-evidence

- ➢ Reuse by turning the seal off, then on.
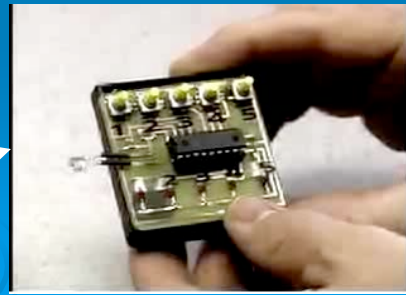

Blinking Lights Seal

- ➢ When the container is opened, the good guys have 1 minute to enter the correct password, or else the anti-evidence is erased.

- ➢ If the correct 2-digit password is entered (within 1 min), and no previous intrusion has occurred, the seal flashes the 2-digit anti-evidence for 1 minute. Then the anti-evidence is erased and the seal goes "offline".*

- ➢ At inspection time, if the seal is offline or the anti-evidence is wrong, then the good guys know tampering has occurred.

Blinking Lights Seal

➢ The bad guys only have a 4% chance of guessing the correct password, but they receive no clue as to whether they guessed correctly or not.

➢ If they guess wrong, the anti-evidence is erased, and the seal goes offline in 1 minute.

1. View password & anti-evidence
2. Tamper inquiry:
    a. enter password (3-3)
    b. check anti-evidence (5-4)
3. Seal goes "offline"

Another Blinking Lights Seal
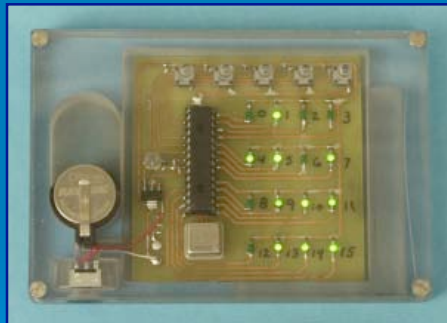
Advantages of Anti-Evidence Seals

+ better security
+ simple, low cost
+ fully reusable (even if mechanical)
+ no tools to install or remove the seal
+ some don't require a reader
+ can often be used inside the container
+ may not require a hasp
+ some monitor a wall or volume, not just a portal

Advantages of Anti-Evidence Seals

+ It's often possible to open the container <u>before</u> checking or removing the seal.

+ You can check the seal multiple times without opening the container (even if the seal is inside the container).

+ Anti-Gundecking: We can automatically verify that the seal inspector actually checked the seal, rather than just saying he did.

Some of the Other 20+ New VAT Seals

◆ **Magic Slate Seal** - mechanical AE seal

◆ **Flashing LED Seal** - infrared AE seal

◆ **Theodolite Seal** - remotely read

◆ **Beads-in-a-Box** - passive volumetric seal

◆ **Plug Seal** - for containers with no hasp

◆ **MagTag** - US Patent 6,784,796

◆ **Enhanced Seal Insert** - US Patent 6,588,812

◆ **Tempered Glass Seal** - US Patent 6,553,930

◆ **Triboluminescent Seal** - US Patent 6,394,022

Real-Time Cargo Monitoring

The anti-evidence approach is, we believe, also the correct way to do real-time monitoring & "smart containers".

(Called "Town Crier" Monitoring.)

- Simple
- Low-cost
- Fast setup
- High levels of security
- Quickly transferable to other containers
- Very low communications bandwidth (byte/sec to bit/min)

LANL Vulnerability Assessment Team

Roger Johnston, Ph.D., CPP, Ron Martinez, Leon Lopez,
Sonia Trujillo, Adam Pacheco, Anthony Garcia,
Jon Warner, Ph.D., Alicia Herrera, Eddie Bitzer, M.A.

http://pearl1.lanl.gov/seals

A copy of this CD
can be obtained from:

rogerj@lanl.gov

Ring the bells that still can ring.
Forget your perfect offering.
There is a crack in everything.
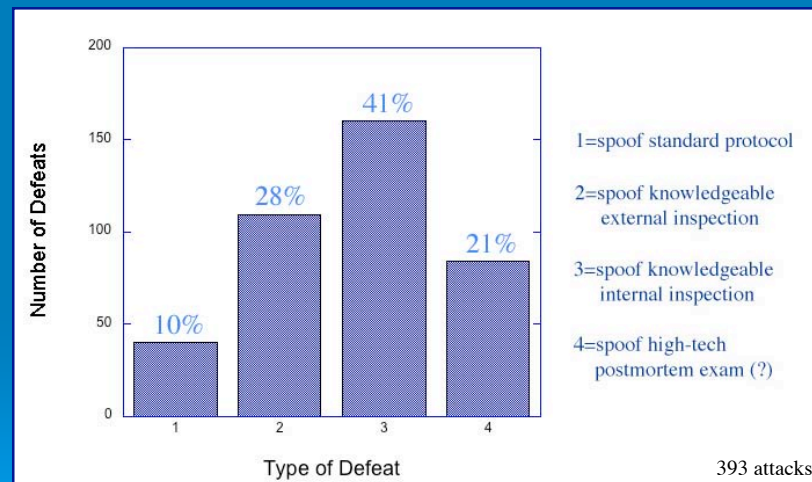That's how the light gets in.
                        -- Anonymous

Next slides are additional handout material

Types of Anti-Evidence Seals

type	examples
Complexity	Cobra, RPT, MagTag, Beads-in-a-Box Seal
Password	Talking Truck Cargo Seal, Magic Slate Seal, (5) Blinking Lights Seal
Hash/One-Time Pad	Time Trap, Town Crier, Flashing LED Seal
Saturated Response	(16) Blinking Lights Seal
Challenge/Response	?

Types of Attacks

Number of Defeats

10% 28% 41% 21%

Type of Defeat

1=spoof standard protocol

2=spoof knowledgeable external inspection

3=spoof knowledgeable internal inspection

4=spoof high-tech postmortem exam (?)

393 attacks

Magic Slate Seal