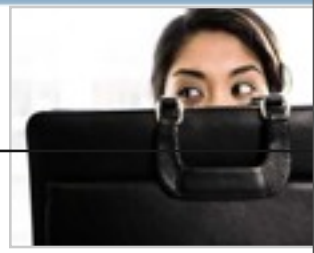
Chirping Tag and Seal

9th Security Seals Symposium
Houston, TX, Sept. 2, 2010

Jon S. Warner, PhD. and Roger G. Johnston, Ph.D., CPP
Vulnerability Assessment Team
Argonne National Laboratory
jwarner@anl.gov

The VAT works in the following areas

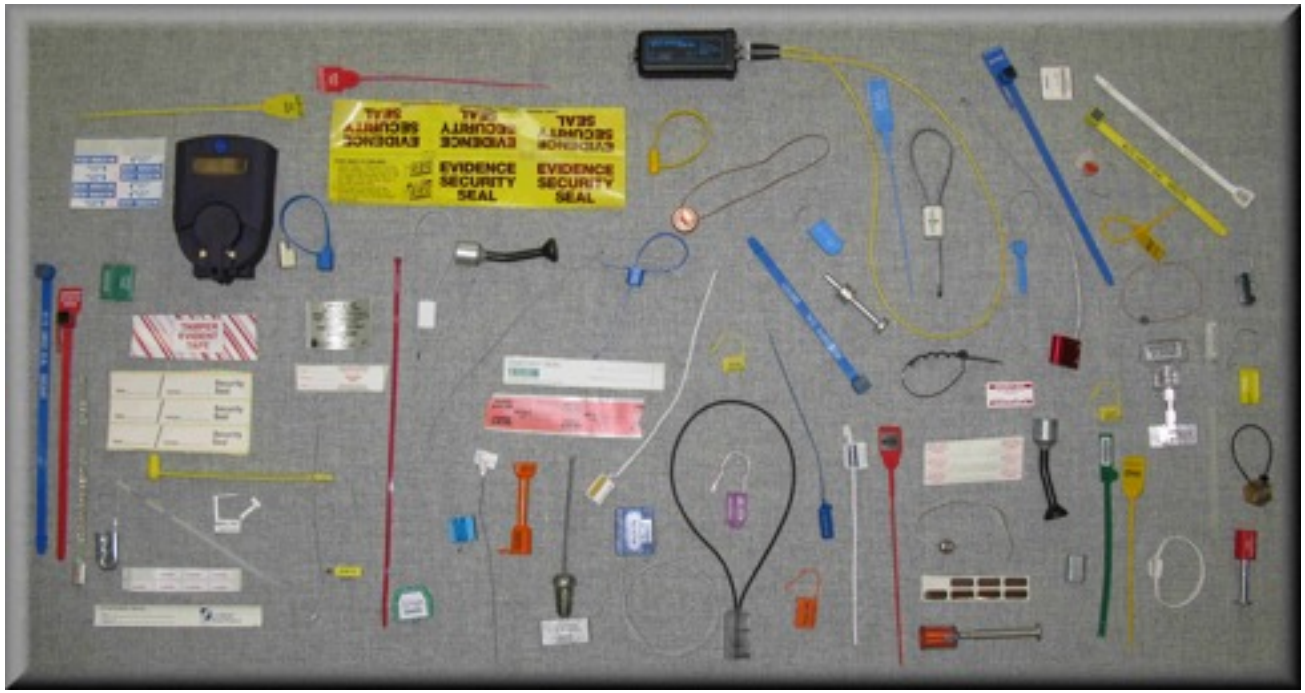


- specialty field tools
- consulting & training
- physical security R&D
- insider threat mitigation
- vulnerability assessments
- access control & biometrics
- microprocessor applications
- tamper & intrusion detection
- novel security devices/strategies
- tags & seals
- counter intelligence
- reverse engineering
- drug testing security
- electronic vote tampering
- security countermeasures
- cargo & transportation security
- security culture & human factors
- product tampering & counterfeiting
- nuclear safeguards/nonproliferation

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

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

Terminology

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.

-"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*

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.

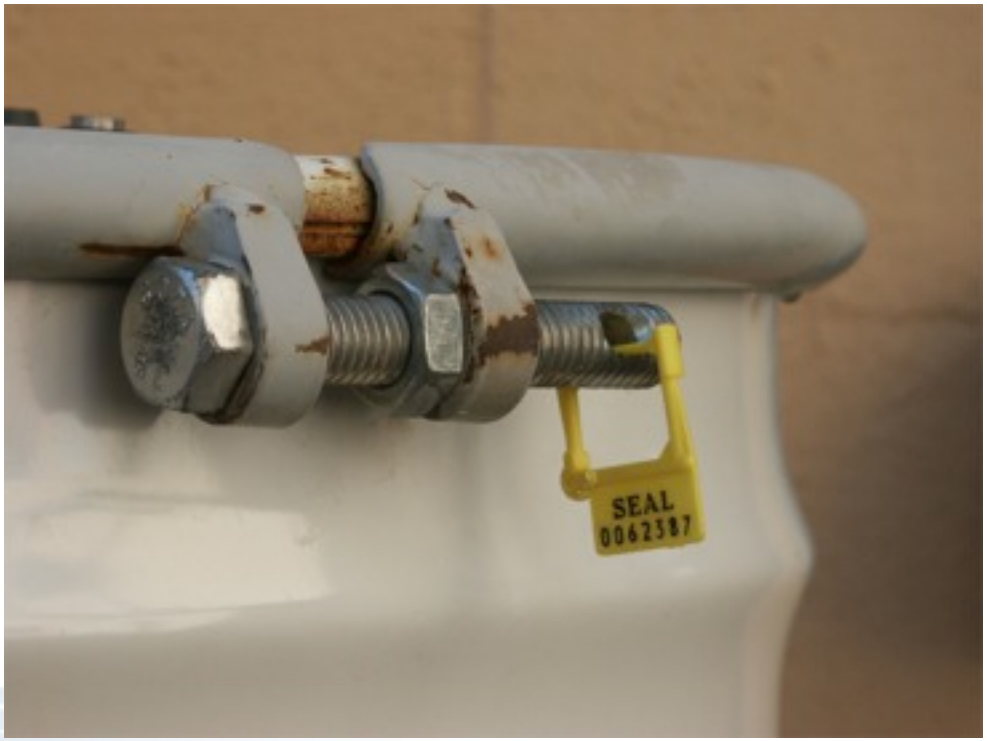
Radisson Welcomes
Emerging Infectious Diseases

-- Sign outside a Radisson Hotel

Factoid: Damn Yankees

A seal is not a lock.

Yanking a seal off a container is not defeating it!



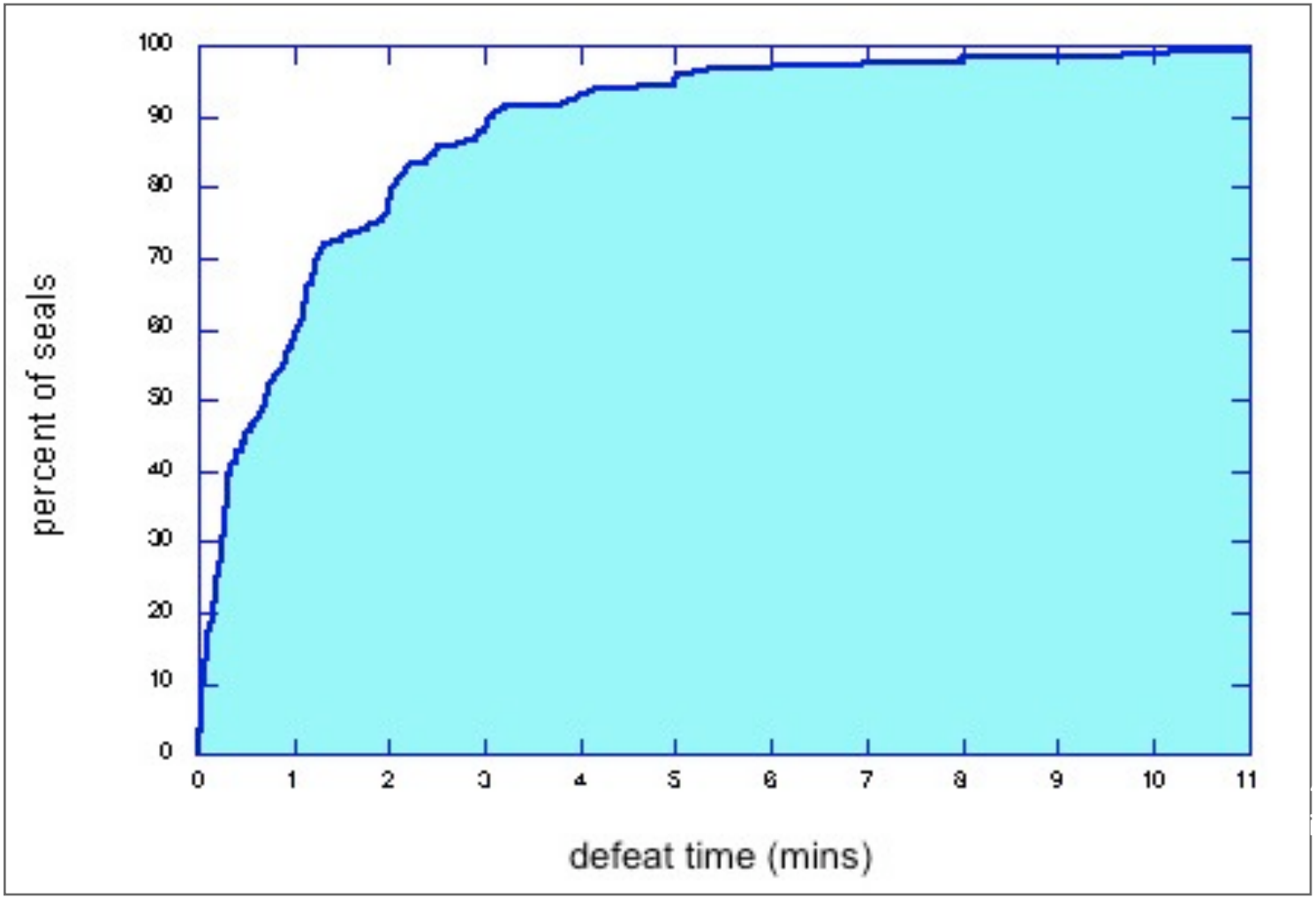
Seals Vulnerability Assessment

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.

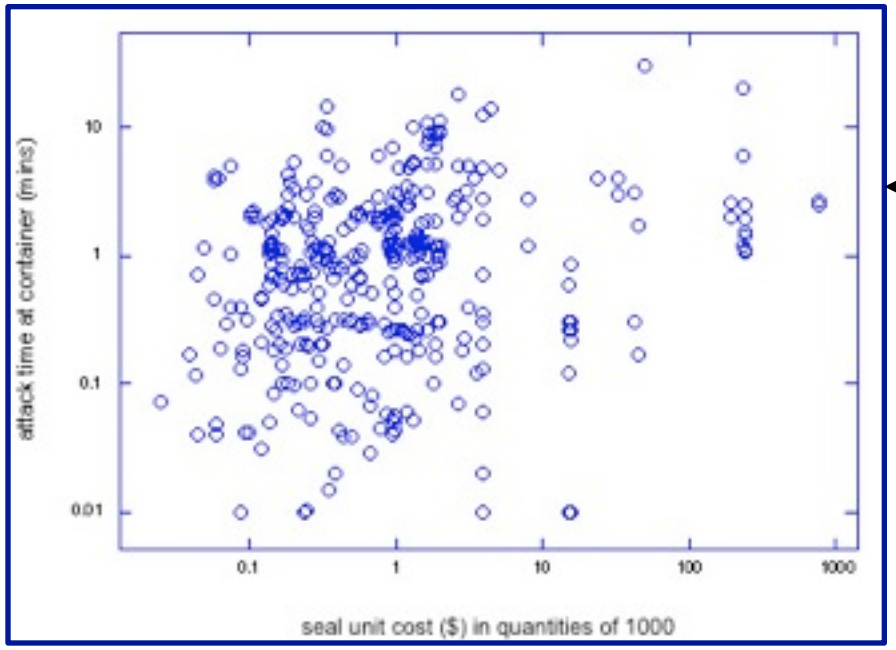
Seals are easy to defeat: Percent of seals that can be defeated in less than a given amount of time by 1 person using only low-tech methods



Results for 244 Different Seal Designs

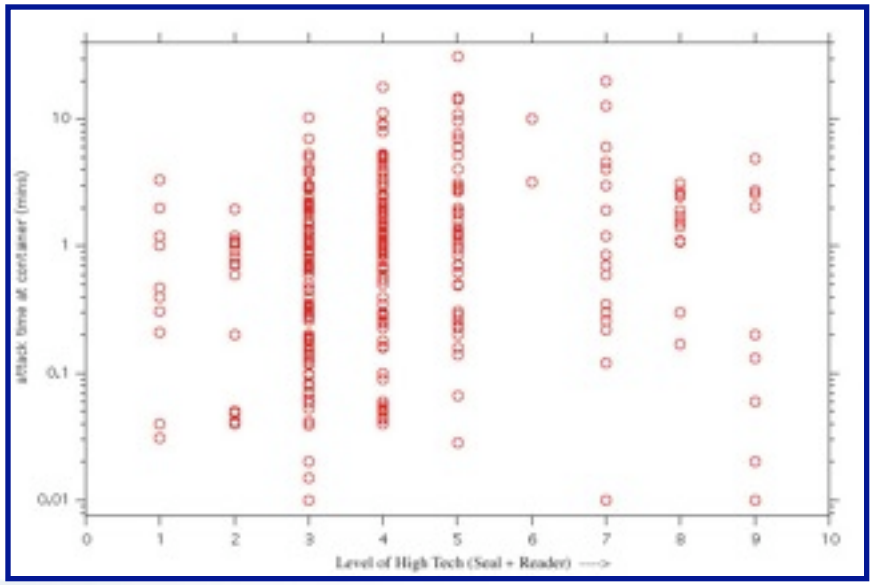
parameter	mean	median
attack time	1.4 mins	43 secs
cost of tools & supplies	$78	$5
marginal cost of attack	62¢	9¢
time to devise successful attack	2.3 hrs	12 mins

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*

- shim
- “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

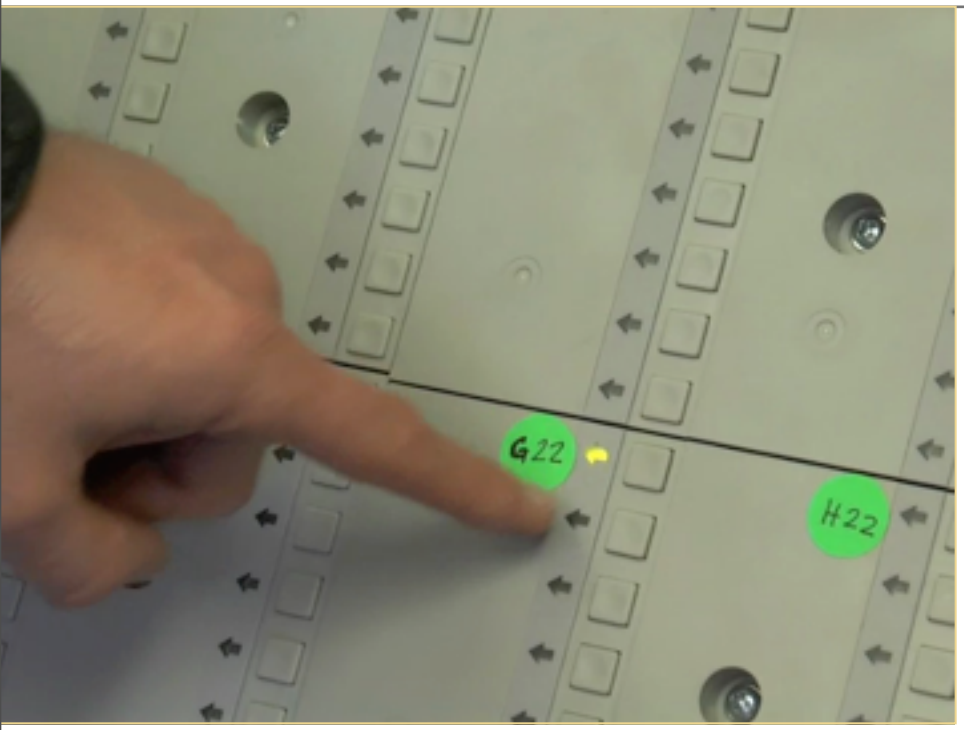
*RG Johnston & ARE Garcia, "An Annotated Taxonomy of Tag and Seal Vulnerabilities", *Journal of Nuclear Materials Management* **229**, 23-30 (2000)

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
- read encryption keys from memory

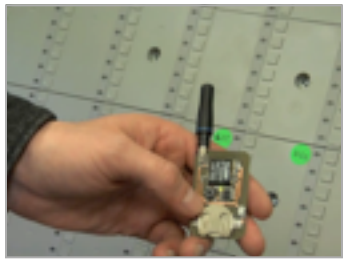
Game Show Host: What travels at three hundred million miles a second?
Contestant: A cheetah?

Man In The Middle example - Vote Switching



Tools needed (minimum):

- ✓ Screwdriver
- ✓ Razor Blade
- ✓ Wire
- ✓ Portable soldering iron



Turn vote cheating on or off up to 3000 feet away

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)

Better Seals - Rethinking the fundamentals

It’s easy to detect tampering!

But what do we do with the information that tampering has occurred?

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. When the seal is opened this "Anti-Evidence" is quickly erased. There's nothing left 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
- ✓ can go inside the container
- ✓ no tools to install or remove seal
- ✓ no hardware outside the container
- ✓ 100% reusable, even if mechanical
- ✓ monitor volumes or areas, not just portals
- ✓ only 1-2 bytes needs to be erased (fast; fewer data remanence problems)
- ✓ can automatically verify that the seal was checked (“anti-gundecking”)

Anti-Evidence Unresolved Issues

Relatively little interest in better seals.

- Battery life.
- Sneaking past the sensors.
- Which sensors and how many?
- Reliability & False alarm rates?
- Require more work than most seal users currently do.
- There are secret key, hash, or password control issues.
- There are still some speed and data remanence issues.
- No independent, external Vulnerability Assessments have been done

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

A wide variety of sensors can be used with the Anti-Evidence seals to detect tampering and intrusion

Hall Effect magnetometer, ~$0.85

PIR motion, ~$8

1-wire temperature, ~$4

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

color sensor, ~$2

barometric pressure, ~$4

thermistor, ~$0.80

temperature & humidity, ~$13

O_2 sensor

CO_2 Sensor ~$19

force sensor, ~$4

gyro (angular rate sensor), ~$23

IR proximity, ~$13

triple axis accelerometer, ~$8

vibration sensor, ~$2.50

An “Anti-Evidence” seal example

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

Seal: $15 of parts (retail)
Reader: $30 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!

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

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

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

“Town Crier” Monitoring - Version 1

(Version 1 ~ $1600)

Parameters

Total truck monitoring time: 193 hrs

“ALL OK” signal frequency: once/second

Early results

Missing “All OK” signals: 1 out of 697197

Wrong “All OK” signals: 0 out of 697197

Intrusions detected: 36 of 36

Town Crier Monitoring - Version 2

Town Crier Seal Module

Headquarters Module

Version 2 ~ $58 ($16 without voice playback)

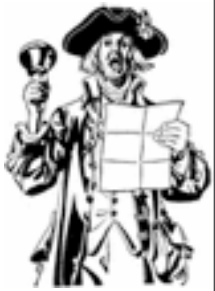
Simplifying the Town Crier

The Town Crier can be simplified by eliminating:

1. Speaking (though it's nice for demonstrations)
2. LCD (again, nice for demonstrations)
3. RF communications (alternatives such as infrared or acoustics are simpler, cheaper, less power-hungry, and potentially more secure)
4. Data modulation (The Bingo Number isn't necessary!)

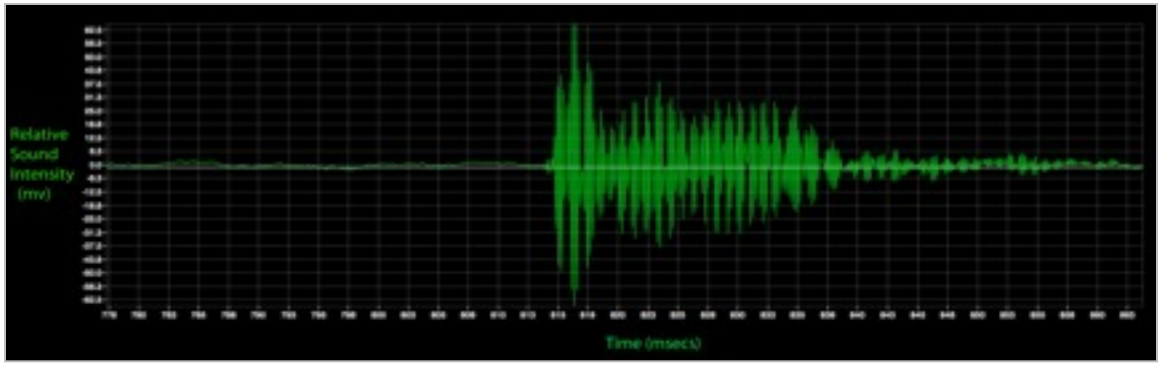
Instead of a "Bingo" number, we send an acoustic chirp at specific, pre-determined times known only to the good guys.

The Anti-Evidence is the arrival of a chirp at the correct time (unpredictable for the bad guys).



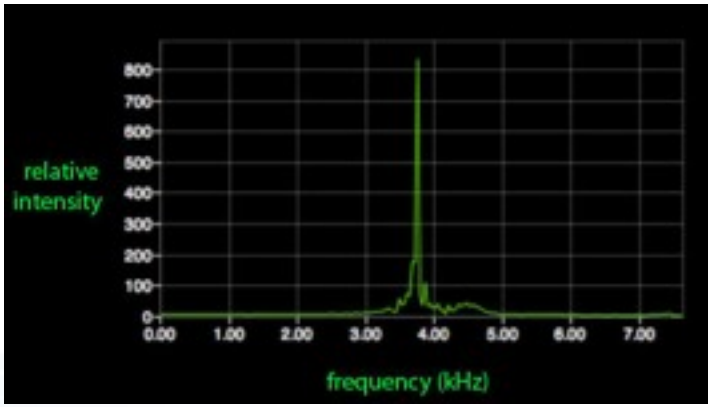
Chirping “Tag and Seal”
(a greatly simplified Town Crier System)

(~$11 retail quantities)



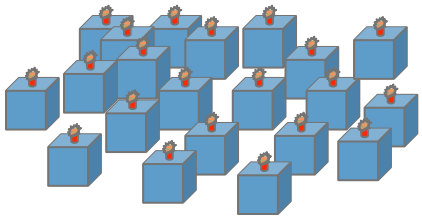
23 msec pulse

3.8 kHz



Cargo Container (or vault)

Many Chirping Tag/Seals in one volume



- ✓ Many chirping tags/seals can be enclosed in the same volume, all chirping in a unique time sequence.
- ✓ Each seal has a unique chirp timing algorithm.
- ✓ A microphone system listens for the chirps.
- ✓ A microcontroller (connected to the microphone) analyzes the chirps and compares the actual arrival time with the expected arrival time.

Cargo Container (or vault)

Many Chirping Tag/Seals in one volume

- ✓ The chirps are so short that they rarely overlap, but the good guys already know when to expect overlap anyway.
- ✓ Only the time to the next chirp is important, not absolute time.
- ✓ The chirping from one tag/seal stops if the asset being monitored is missing, opened, or tampered with.
- ✓ Tampering with the asset or the tag/seal causes erasure (< 1 μsec) of the information needed to generate future chirps at the correct times.

Chirping “Tag and Seal”

- *It’s a…*
  - ✓ tag (for theft detection)
  - ✓ tamper indicating seal (for tampering)
  - ✓ real-time monitor (for immediate detection)!
- Ideal for securing sealed radiological sources.
- In most applications, only 1 chirp every minute or so is needed on average (vs. every 3 secs for our prototypes)

Chirping Tag & Seal Variations

- Switch to ultrasonic chirps to annoy workers less (ultrasonic yields a shorter range)
- Change the acoustical chirp frequency (currently 3.8 kHz)
- Change the chirp duration (currently 23 ms)
- Change the average duration to the next chirp (for our demo, we average one chirp every 4 seconds)
- Change the PRNG chirp timing algorithm or use a one-time pad for better security (the algorithm will change for each seal in use, this provides it's uniqueness)

Example Applications

1) Asset in vault – Chirper system alerts guards to intrusion into the asset

- In real time (Real Time Monitor)
- At a later time, after interrogation of the system (Seal)

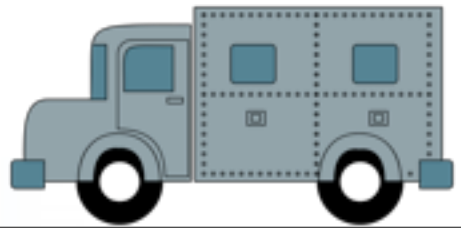
2) Asset in vault – Multiple Chirpers chirp at the microphone system and alerts the guards to theft (Security Tag)

Example Applications (con't)

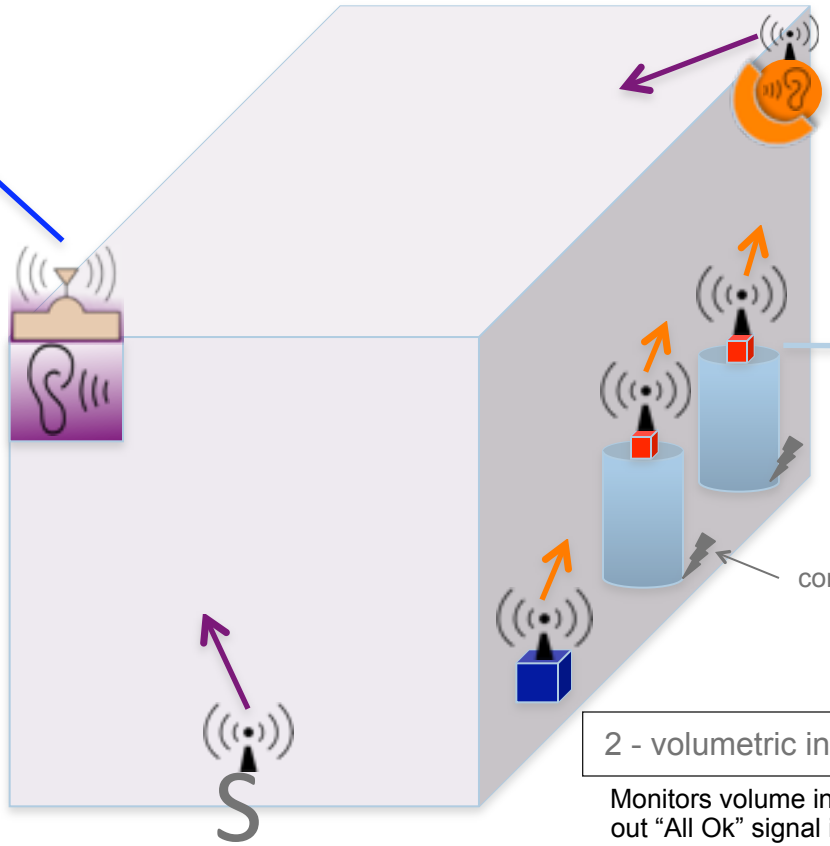
3) Cargo truck – Chirpers chirp at the microphone system. The truck takes the results and reports to headquarters (using Anti-Evidence or not) (Real Time Monitor)

4) Cargo truck – When the truck arrives at it's destination the microphone system is interrogated. The microphone system can report on tampering and when it occurred. (the microphone system is a Seal).

Alternatively, the good guys can open the cargo door and listen to the chirps for evidence of tampering or theft (Seal, Security Tag).



Nested Chirping*



4 - internal Town Crier listener

Collects data from devices inside container. Sends “All ok” signal to outside of container.

5 - Truck Town Crier
APRS/spoof-resistant GPS

Collects data from inside/outside container. Sends “All Ok” signal to HQ.

3 – Anti-Evidence tamper detection in/on containers

Monitors containers for tampering and theft. Sends “All Ok” signal inside cargo container.

container & vehicle removal delay measures

2 - volumetric intrusion detection

Monitors volume inside container. Sends out “All Ok” signal inside cargo container.

1 – Anti-Evidence seal

Monitors access into container. Sends Out “All Ok” signal to the external collection system

*Note: Chirping can be in the form of acoustic, ultrasonic, light (LED), RF, etc.

Advantages of acoustic chirps

- simple & cheap
- low power requirements
- >> 300 foot detection range
- 3.8 kHz is a relative quiet part of the acoustic spectrum
- works to some extent through walls or from inside containers
- ultrasonic chirps can replace acoustical chirps to avoid annoying workers (but range is less)

Advantages of acoustic chirps (con't)

- Unlike RF…
  - EM interference not an issue with acoustic chirps
  - works well near metals, liquids, & around corner
  - the user can tell if the chirper is working
  - no perceived safety issues
  - device can't sneak out sensitive info (the data isn't even modulated)
  - no International Frequency Spectrum regulations to comply with
  - Unlike RFID, the chirper doesn't use static identification

Questions?