LA-UR- 02-6946

Approved for public release;
distribution is unlimited.

Title: Towards Better Tamper & Intrusion Detection

Author(s): Roger G. Johnston
Anthony R.E. Garcia
Adam N. Pacheco

Submitted to: 6th Security Seals Symposium
Santa Barbara, CA
February 18-21, 2003

Los Alamos
NATIONAL LABORATORY

Title: Towards Better Tamper and Intrusion Detection

Author: Roger Johnston, Anthony R.E. Garcia, and Adam N. Pacheco

Abstract:

This presentation discusses in generic terms some of the work of the Vulnerability Assessment Team at Los Alamos National Laboratory in the area of tamper and intrusion detection. Novel security approaches are discussed. We also present preliminary results for a crude prototype of a high security ("Town Crier") monitoring system for securing moving cargo or stationary assets.


DENVER BRONCOS

Towards Better Tamper & Intrusion Detection

Roger G. Johnston, Ph.D., CPP
Vulnerability Assessment Team
Los Alamos National Laboratory

505-667-7414
rogerj@lanl.gov
http://pearl1.lanl.gov/seals

Types of Traps

type 1: the adversary is unaware of the trap until after he trips it, when it is (ideally) too late to do anything about it.

type 2 : the adversary is unaware of the trap, both before and after tripping it.

type 3: the adversary knows you are using a trap, but can't find it. (Future micro- and nano-traps.)

Definitions

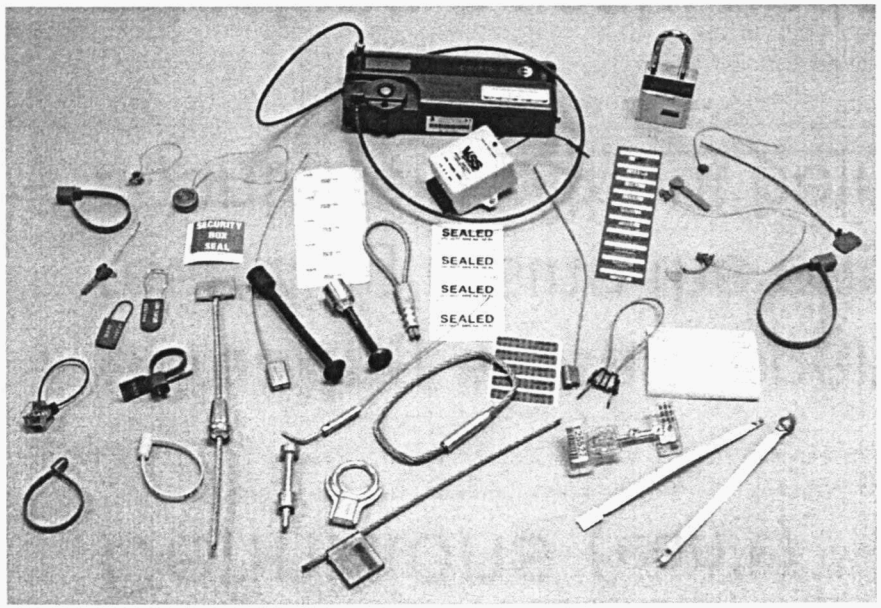
lock: a device to delay, complicate, and/or discourage unauthorized entry.

seal : a tamper-indicating device (TID) designed to leave non-erasable, unambiguous evidence of unauthorized entry or tampering. Unlike locks, seals are not necessarily meant to resist access, just record that it took place.

trap: a covert seal.

Tamper-Indicating Seals

Seals: Detect tampering or unauthorized access



Some of the 5000+ commercial seals

Applications

- customs
- cargo security
- non-proliferation
- treaty verification
- counter-terrorism
- counter-espionage
- consumer protection
- records & ballot integrity
- evidence chain of custody
- weapons & ammo security
- protecting instrument calibration
- waste management & hazardous materials accountability

Definitions (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.

Defeating seals is thus mostly about fooling people, not beating hardware (unlike defeating locks, safes, or vaults)!

Definitions (con't)

tamper detection: delayed (after the fact) detection of unauthorized access.

intrusion detection: immediate (real-time) detection of unauthorized access.

Cargo Container Vulnerabilities

Each year at the 361 U.S. ports:

6 million truck-size cargo containers
(2% inspected)

7,500 foreign ships

200,000 foreign sailors

Cargo Container Vulnerabilities

Millions of people live within a few miles of U.S. ports

The ports are surrounded by fuel tanks, chemical plants, and vital bridges.

Overall port security is poor.

Cargo containers are an ideal vector for terrorists!

Cargo Container Vulnerabilities

There are additional cargo vulnerabilities through truck and rail shipments into the U.S.

Drug and other types of smuggling using cargo containers is also a serious problem.

Security for large-scale shipment of highly radioactive waste is an unsolved problem.

Cargo Container Security

National Cargo Security Council: 2% of all U.S. international and domestic cargo is stolen (about $15 billion/year).

Existing cargo container security devices and monitoring systems are inadequate, especially for moving containers.

Increasingly, insurance companies, Fortune 500 companies, and JIT manufacturing techniques demand better security.

Cargo Container Security

After 10 years of study, we think we know how to do high-security tamper & intrusion detection correctly, using a fundamentally unconventional approach.

A prototype has been built, and this “Town Crier” concept has been demonstrated for both stationary and moving assets.

Definitions (con't)

vulnerability assessment: discovering and demonstrating ways to defeat a security device, system, or program. May include suggesting counter-measures and security improvements.

The 2% Rule

Typically, about 2% of inspected seals are problematic: tampering or no tampering? (Range: 0.1% to 5%)

Reasons

- manufacturing defects
- installation errors
- inspection errors
- problems with seal data
- electronics or battery failure (for active seals)
- aging or environmental wear
- seal damage (inadvertent or deliberate)
- borderline cases
- actual tampering

The 2% Rule (con't)

It is necessary to have a policy in place **in advance** to deal with these problematic seals.

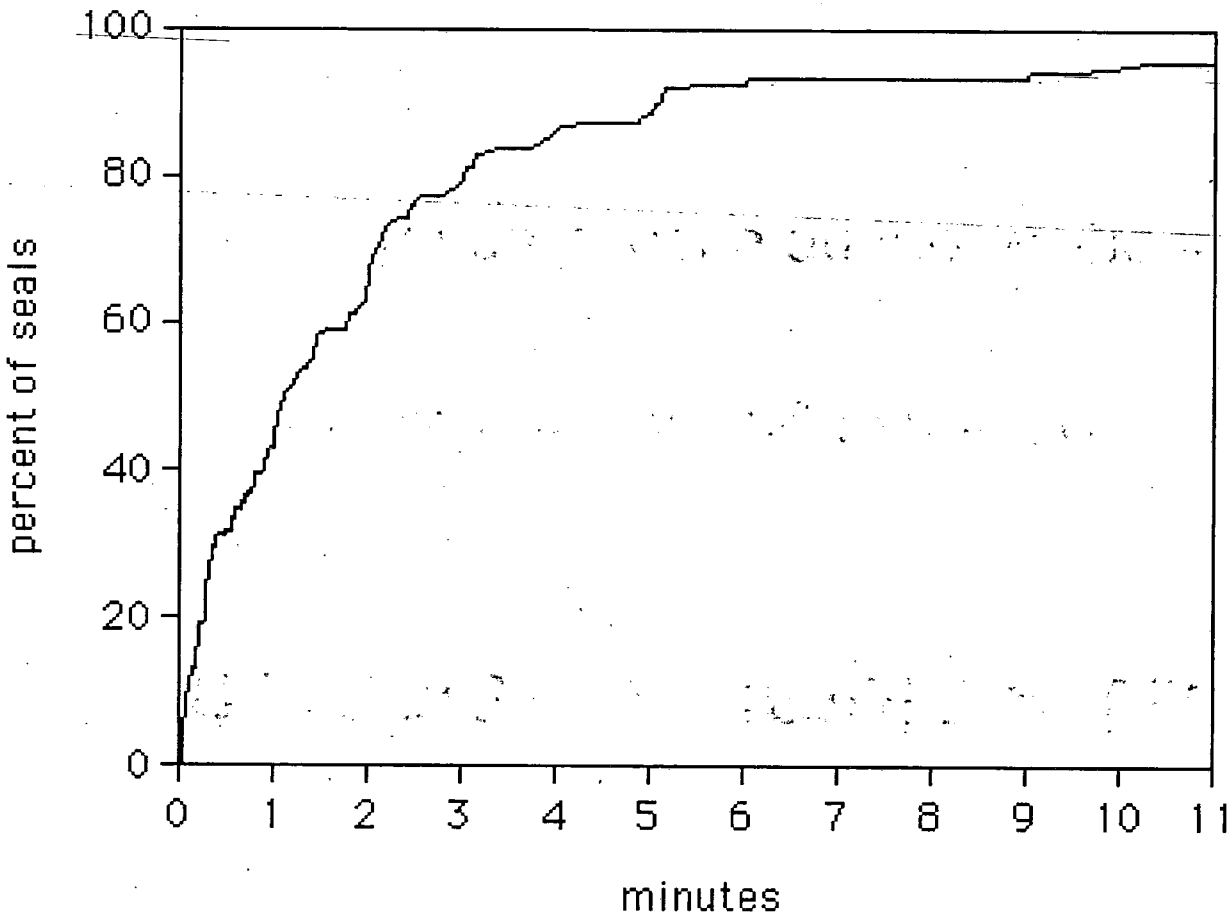
Why Complex, High-Tech Tags & Seals Are Vulnerable To Simple Attacks

- Still must be physically coupled to the real world
- Still depend on the loyalty & effectiveness of user's personnel
- More legs to attack
- Users don't understand the device

Why Complex, High-Tech Tags & Seals Are Vulnerable To Simple Attacks (con't)

- Developers have the wrong expertise
- Developers & users focus on the wrong issues
- The arrogance of high technology (the "Titanic effect")

Cumulative Defeat Time Graph



Categorizing Defeats

We fool the seal inspector, even with...

Type 1 - nominal, usual, or recommended inspection

Type 2 - careful visual inspection of exterior

Type 3 - careful visual inspection of seal interior & exterior

Type 4 - any kind of inspection/analysis?

Seal Vulnerability Assessments

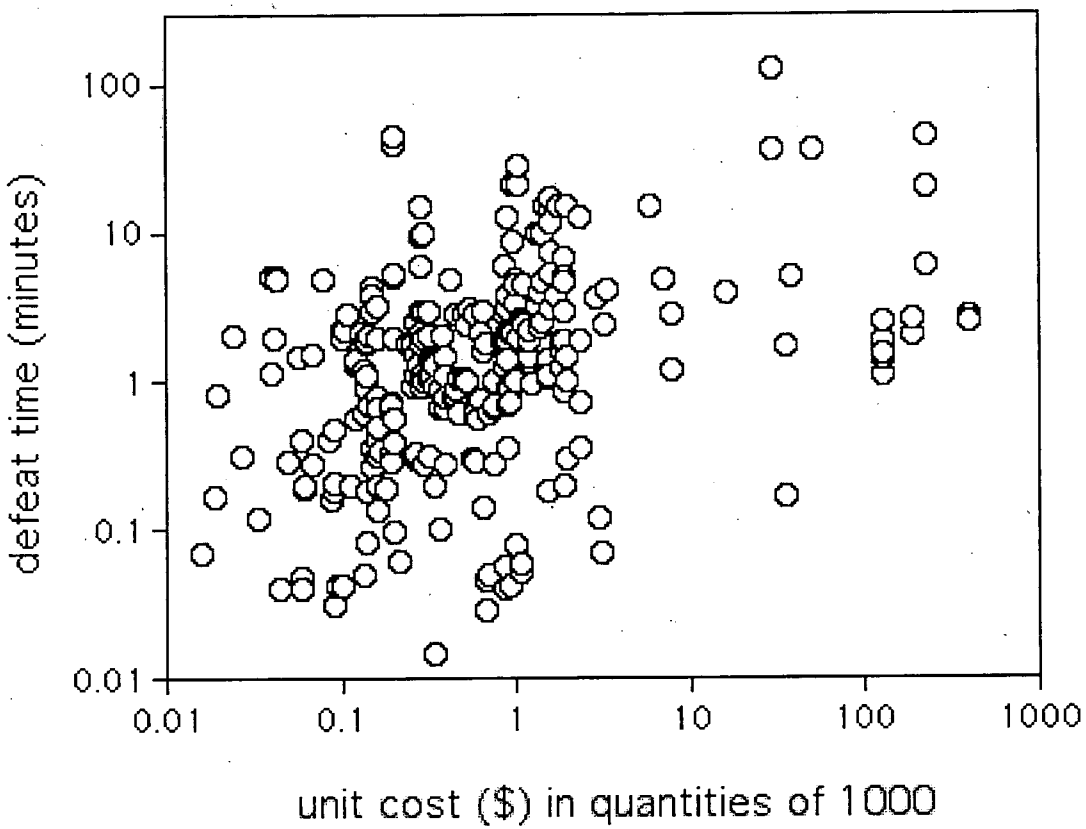
We studied 198 different seals:

government & commercial

passive & active

low-tech through high-tech

Defeat Time vs. Seal Cost

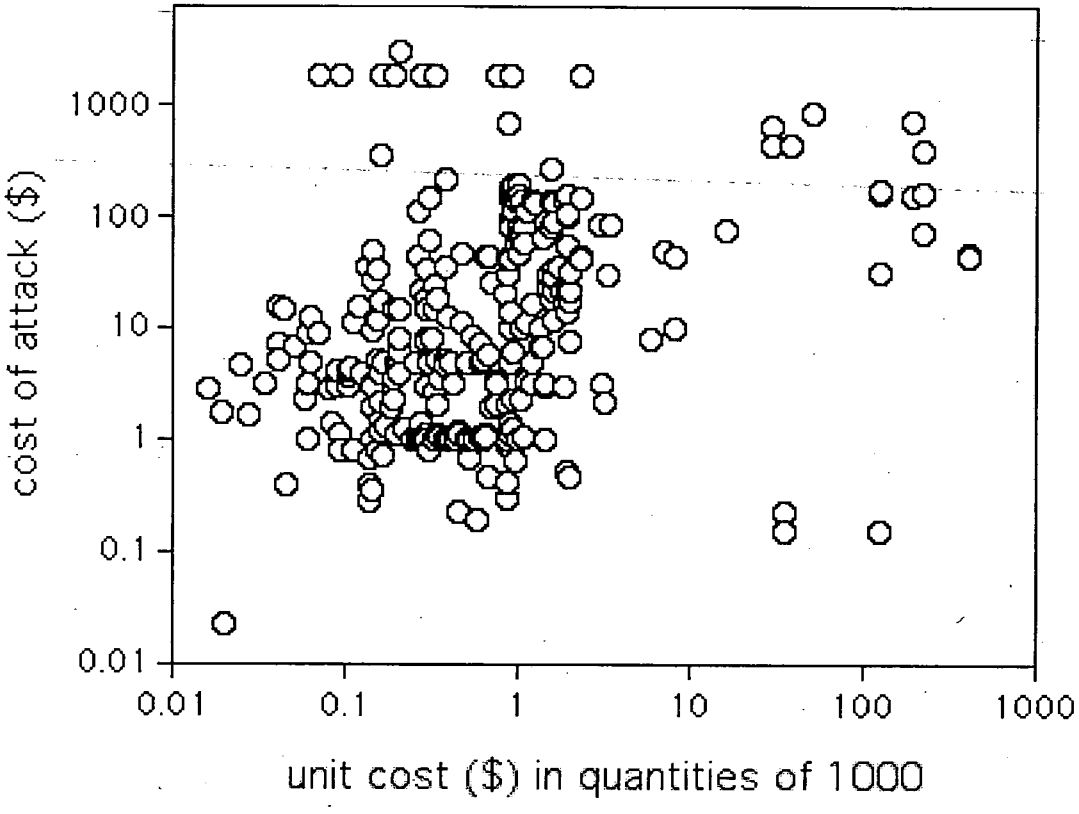


linear LS fit

r = 0.12

slope: 1.5 sec/$

You Can't Outspend the Adversary!



linear LS fit

r = 0.03

slope: 27¢/$

Seals Summary

- At least 56% of these seals are currently in use for "critical" applications.

- At least 16% of the seals are in use (or under serious consideration) for nuclear safeguards.

Vulnerability Assessments (con't)

We developed and demonstrated 289 different defeats on the 198 seals

(1-6 defeats per seal)

The Good News: Countermeasures

- 58% of the attacks have simple & inexpensive countermeasures

- Another 30% of the attacks have workable countermeasures (though not as cheap or simple)

Passive vs. Active Seals

6 of 198 seals (3%) are active seals

(We've tentatively identified low-tech attacks on 4 other active seals, but haven't yet demonstrated them.)

Mean Values for 289 Attacks on 198 Different Seals

(One well-practiced attacker, working alone, using only low-tech tools and methods)

defeat time: 3.9 mins

cost of tools/supplies: $126

marginal cost of tools/supplies: 40¢

time to devise attack: 6.1 hrs

Median Values for 289 Attacks on 198 Different Seals

(One well-practiced attacker, working alone, using only low-tech tools and methods)

defeat time: 1.4 mins

cost of tools/supplies: $8

marginal cost of tools/supplies: 10¢

time to devise attack: 36 mins

Range of Values for 289 Attacks on 198 Different Seals

(One well-practiced attacker, working alone, using only low-tech tools and methods)

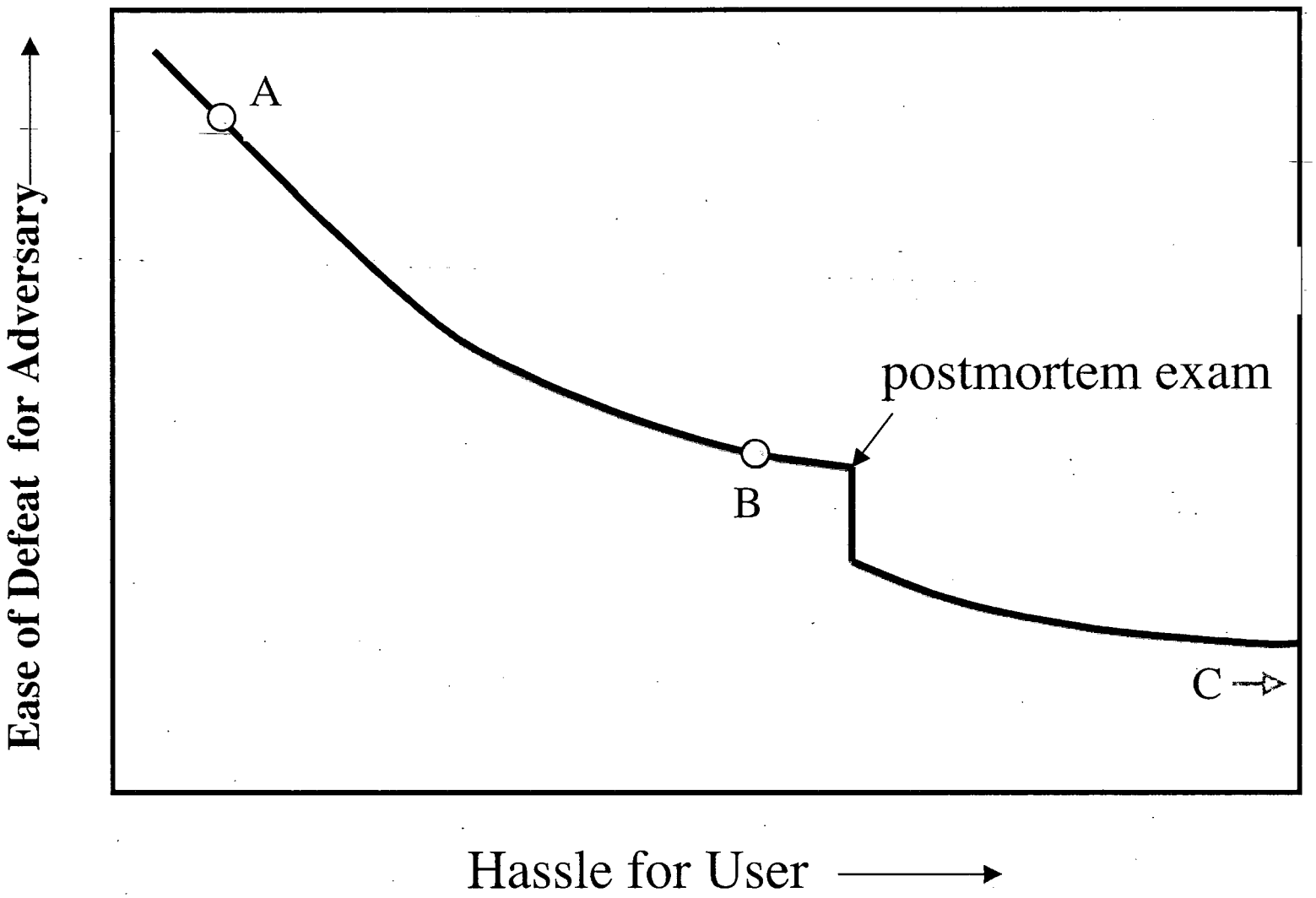
defeat time: 3 secs - 2 hrs

cost of tools/supplies: 2¢ - $3000

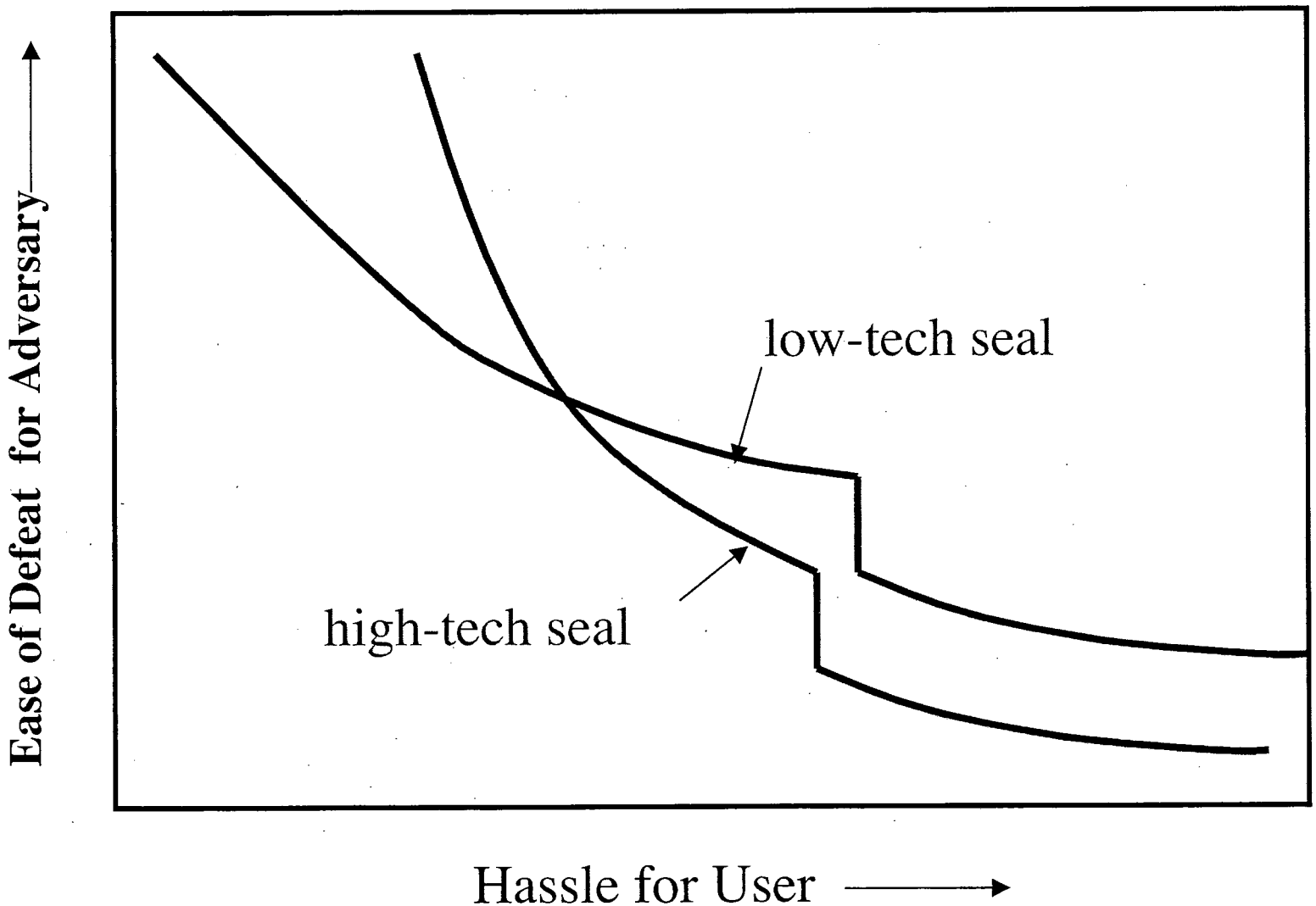
marginal cost of tools/supplies: 1¢ - $40

time to devise attack: 5 secs - 10 days

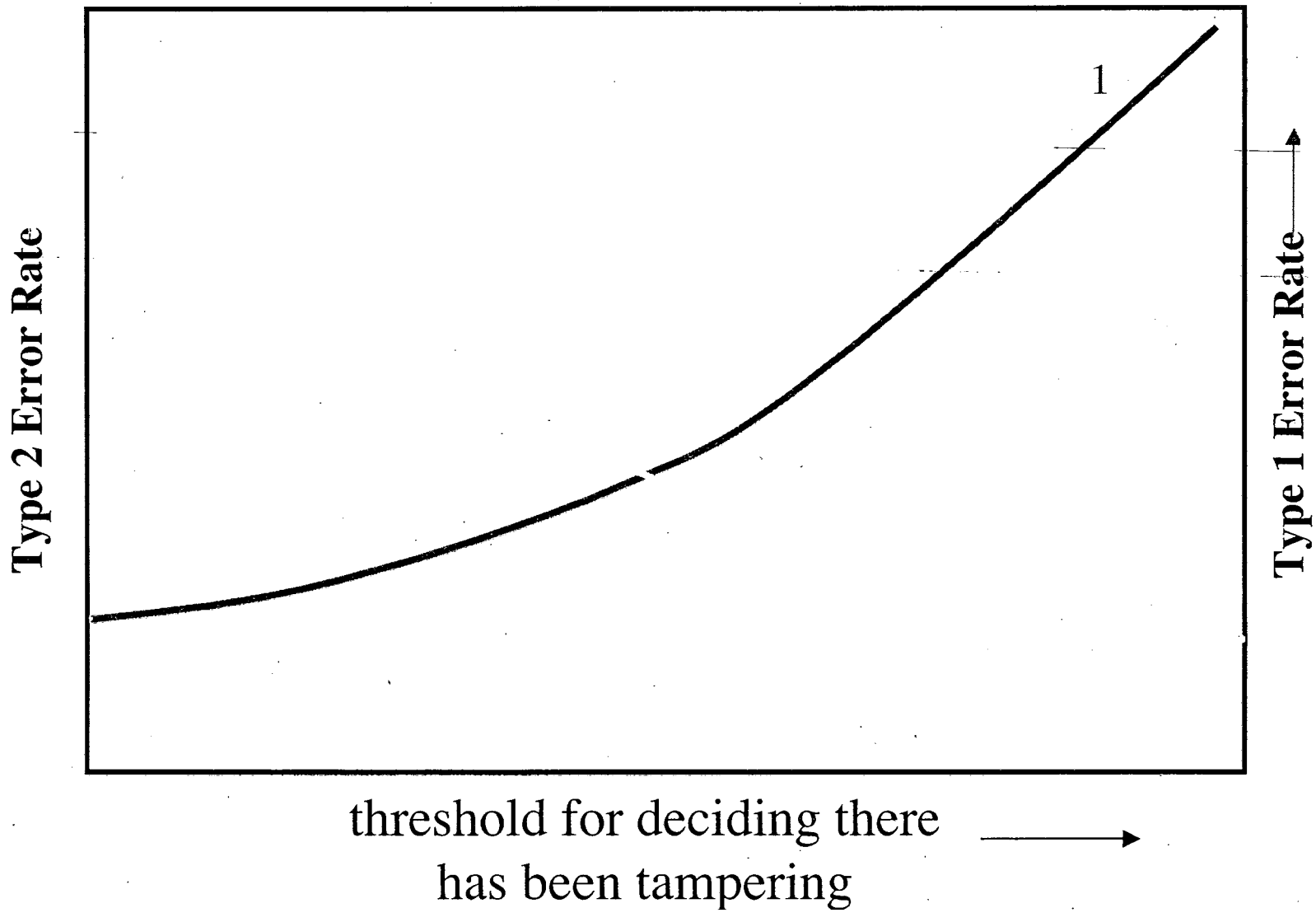
Generic Seal Curve



Low- vs. High-Tech Seals



Type 2 (false accept) vs. Type 1 (false reject) Errors



Problems with Conventional Tamper Detection

It's easy to detect tampering!

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

Problems with Conventional Tamper Detection (con't)

Conventional seals store the 'alarm condition' until it is time to inspect the seal.

But many attacks on seals involve simply erasing this stored information!

Anti-Evidence Approach to Tamper Detection

- Store secret information, such as a random number.
- Erase the number when tampering is detected.
- The 'good guys' can check the number by using a password or PIN.

Anti-Evidence Approach to Tamper Detection (con't)

- Any attempt by the 'bad guys' to enter the wrong password or PIN erases the number.
- Any attempt by the 'bad guys' to access the number (so they can counterfeit it) causes the number to be instantly erased in the process.

Anti-Evidence Approach to Tamper Detection

Surprisingly, this approach can be implemented in a simple passive seal!

(No before & after photos.)

Problems with Conventional Intrusion Detection

It's easy to detect intrusion!

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

Problems with Conventional Intrusion Detection (con't)

Simple conventional intrusion detectors send an alarm once intrusion is detected.

But it is easy to block an alarm.

Problems with Conventional Intrusion Detection (con't)

More sophisticated, conventional intrusion detectors rely on encryption/authentication and/or two-way communication or polling of sensors

This is complicated, and not very practical, especially for monitoring moving cargo.

Anti-Evidence ("Town Crier") Approach to Intrusion Detection

- Send a periodic "All OK" signal if no intrusion is detected.
- Encrypt using a one-time keypad. This is the only unbreakable cipher, and has no export control or proprietary issues.
- Allows for great simplicity.

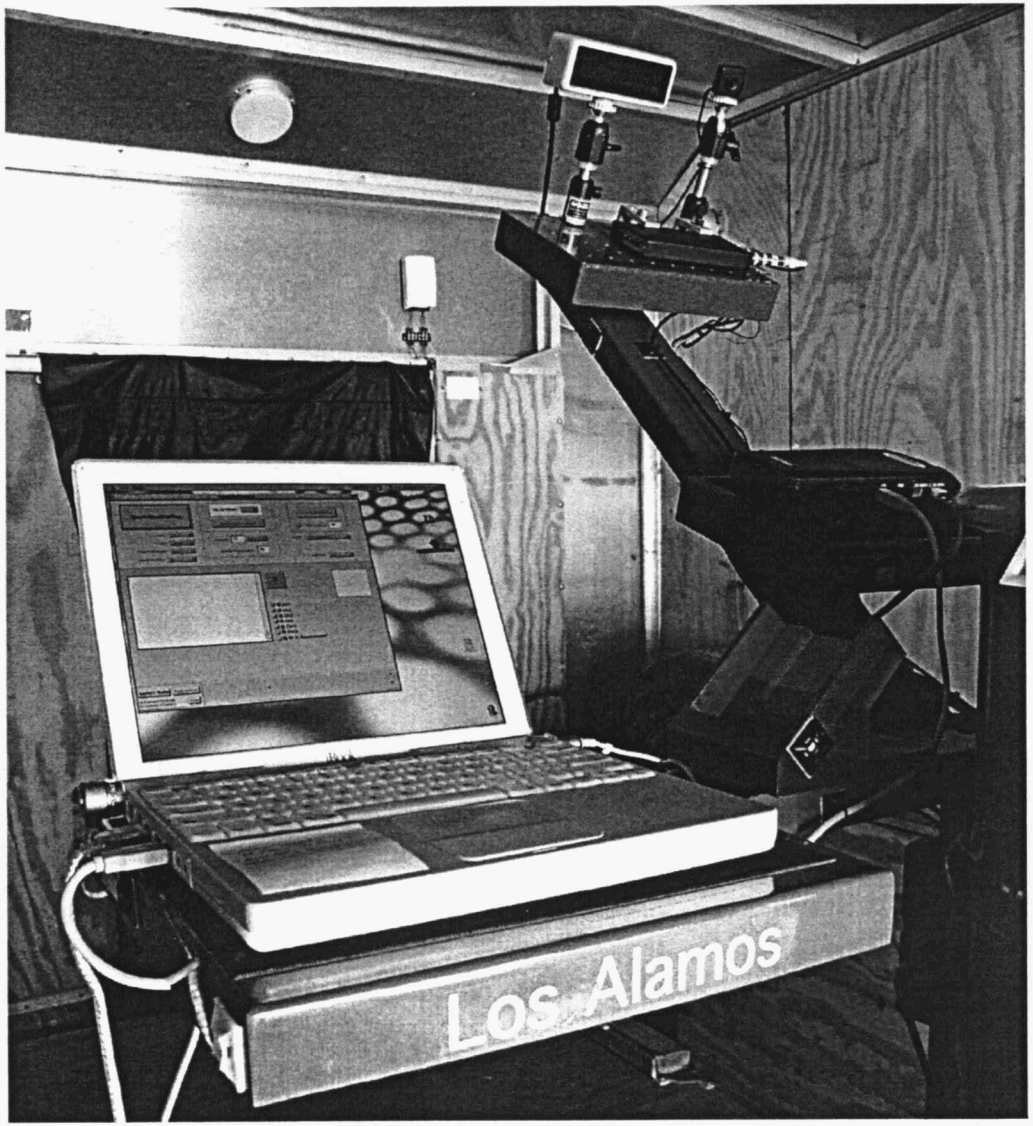
Anti-Evidence ("Town Crier") Approach to Intrusion Detection (con't)

- Requires only one-way, extremely low bandwidth communication.
- Can be used to simultaneously monitor many moving vehicles or containers.

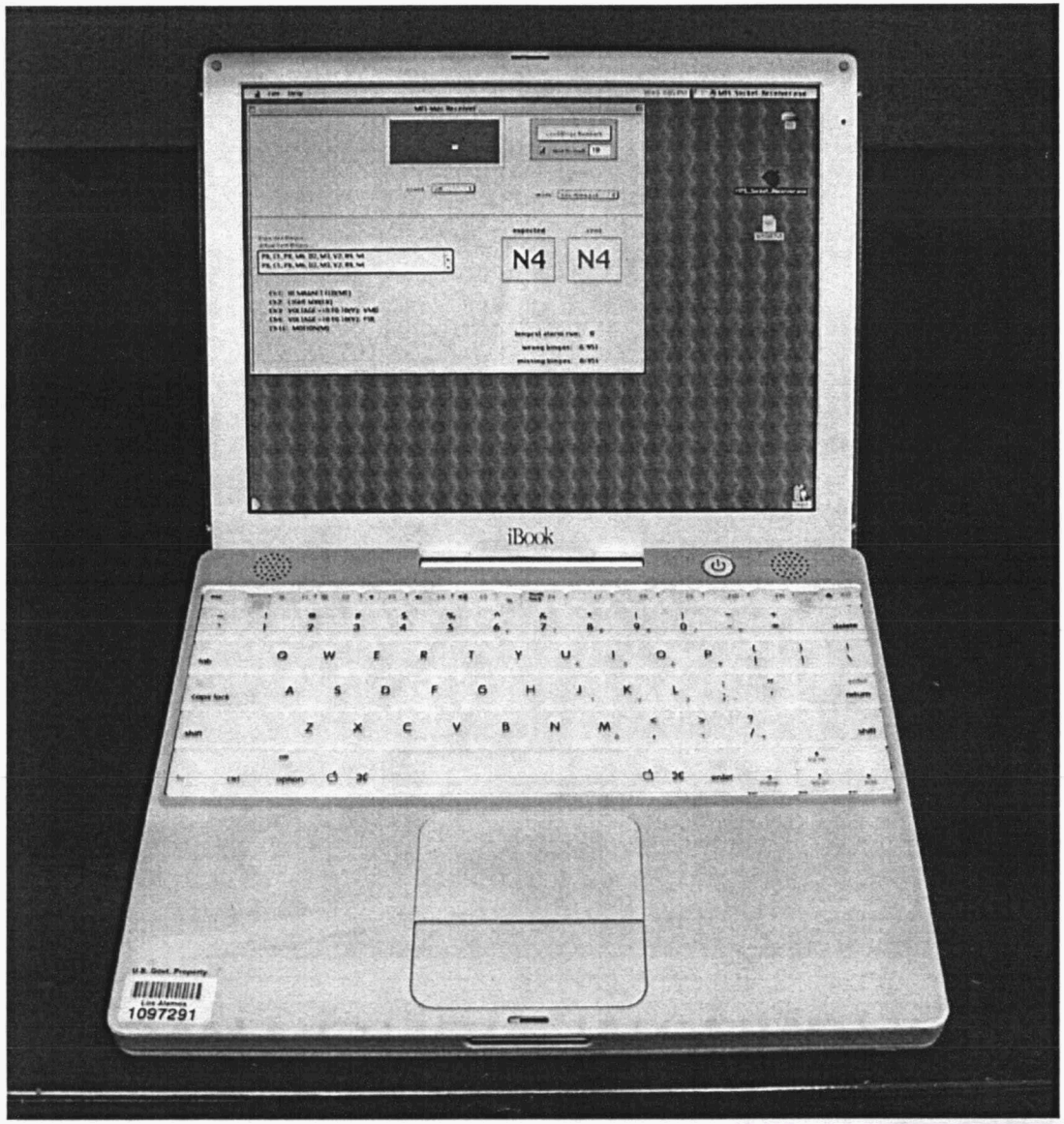
“Town Crier” Monitoring

“Town Crier” Monitoring

“Town Crier” Monitoring



“Town Crier” Monitoring



"Town Crier" Monitoring: Novel Tamper & Intrusion Detection

Continuous, real-time monitoring using simple, low-cost hardware and an anti-alarm/anti-evidence strategy that avoids many of the vulnerabilities of conventional tamper & intrusion detection devices and approaches.

Attributes

- unprecedented high-levels of security
- relatively low cost
- mostly COTS hardware
- easy to set-up and run
- can be rapidly deployed
- quickly adapts to new/different sensors

Attributes (con't)

- easy to scale up or down
- can be operated covertly (Type 1 trap)
- monitors many moving containers, transportainers, or vehicles simultaneously
- frees up security guards, escorts, & couriers
- ultra-low bandwidth, one-way communications encrypted via a one-time keypad (intrusion detection mode)
- attractive for treaty monitoring