LAUR-05-3658

Talk for ICEM'05 Glasgow, Scotland, Sept 4-8, 2005

Nuclear Safeguards & Security: We Can Do Better

Roger G. Johnston, Ph.D., CPP, Jon S. Warner, Ph.D., Anthony R.E. Garcia, Ron K. Martinez, Leon N. Lopez, Adam N. Pacheco, Sonia J. Trujillo, Alicia M. Herrera, and Eddie G. Bitzer, M.A.

Vulnerability Assessment Team
Los Alamos National Laboratory

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

Los Alamos NATIONAL LABORATORY

Vulnerability Assessment Team

Physical Security
- consulting
- cargo security
- tamper detection
- training & curricula
- nuclear safeguards
- vulnerability assessments
- novel security approaches
- new tags & seals (patents)
- unique vuln. assessment lab

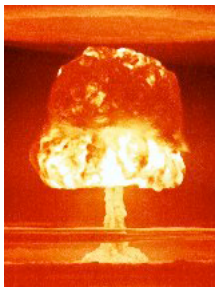
The VAT has done detailed vulnerability assessments on hundreds of different security devices, systems, & programs.

The greatest of faults, I should say, is to be conscious of none.
-- Thomas Carlyle (1795-1881)

Domestic vs. International Nuclear Safeguards

The differences are so extreme, we must be suspicious when similar hardware, strategies, expertise, and personnel are used.

These differences are widely recognized in theory…but not in practice.



Examples of Highly Dual Use

- calorimetry
- intrusion detectors
- safeguards experts
- gamma spectroscopy
- video monitoring systems
- auditing sampling statistics
- encryption/data verification
- passive & active neutron NDA
- certain tamper-indicating seals
- advanced semiconductor sensors

Domestic Nuclear Safeguards

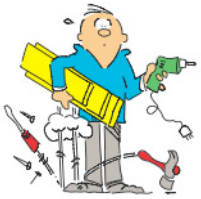
- is MPC&A
- is a traditional security application:
  - ✓ the "good guys" own the assets & facilities
  - ✓ the (unknown) adversaries have limited resources & personnel to try to break in
  - ✓ secrecy is allowed
  - ✓ the "good guys" can use the facility infrastructure, personnel, & training to counter the adversary

International Nuclear Safeguards

- is treaty monitoring, not MPC&A
- not a traditional security application, everything is backwards:
  - ✓ the adversary owns the assets & facilities
  - ✓ the (known) adversary can deploy massive resources to defeat the safeguards
  - ✓ the "good guys" aren't present most of the time
  - ✓ no secrecy--details must be negotiated & transparent
  - ✓ the adversary can use the facility infrastructure, personnel, & training to help defeat the safeguards

Major Tools for Improving Security

- Security Survey
- Risk Management
- Design Basis Threat



- **(Adversarial) Vulnerability Assessment**

Problems with Conventional Methods

- binary
- close ended
- unimaginative
- often used to justify the status quo
- dominated by groupthink & bureaucrats
- tend to let the good guys define the problem
- not done from the perspective of the adversaries
- do not usually lead to major security improvements

The bad guys do adversarial vulnerability assessments, not security surveys, risk management, or DBT--so the good guys should, too!

The Insider Threat: Usually ignored or underestimated

Examples

- Russian safeguards programs
- IAEA
  - lack of security & counter-intelligence culture
  - no background checks on employees & nuclear inspectors
- organizations with disgruntlement problems
  - mistreatment of employees, retirees, & terminated personnel
  - no fair & effective complaint resolution process
  - no fair & effective whistleblower program

Disgruntlement

- Disgruntled employees are known to be a risk for workplace violence, espionage, theft, & sabotage.
- Research shows that employee disgruntlement is associated with perceptions of unfairness & inequity, not necessarily objective conditions.
- Disgruntlement is probably increasing world-wide for general employees.

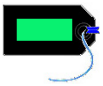
$\neq$

Terminology

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.

tag: a unique identifier of an object or container.



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.

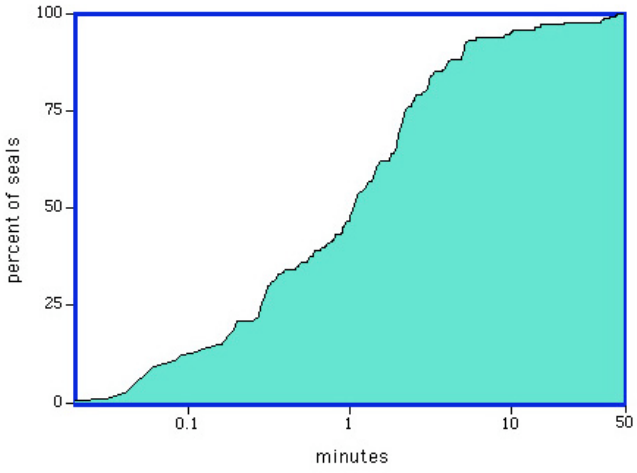
Seals Vulnerability Assessment

We studied 213 different seals in detail:

- government & commercial
- mechanical & electronic
- low-tech through high-tech
- cost varies by a factor of 10,000

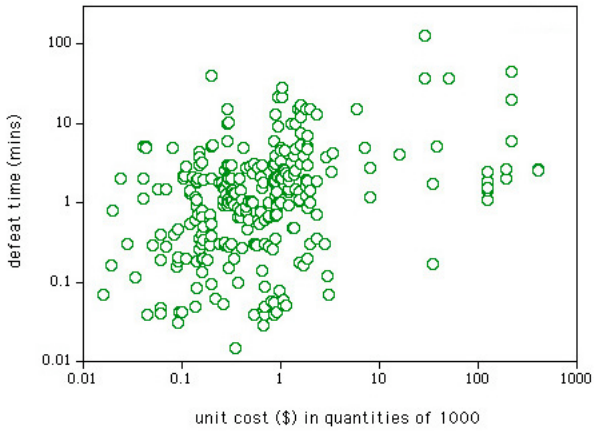
Over half are in use for critical applications, and 16% play a role in nuclear safeguards.

Percent of seals that can be defeated in less than a given amount of time by 1 person using only low-tech methods



213 seals

Defeat Time vs. Seal Cost (213 seals)



linear LS fit

r = 0.14

slope: 1.6 sec/$

307 attacks

Results for 213 Seals

parameter	mean	median
defeat time for 1 person	2.7 mins	1 min
cost of tools & supplies	$144	$5
margin cost of attack	42¢	9¢
time to devise successful attack	5 hrs	12 mins

The Good News: Countermeasures

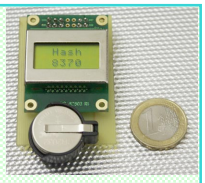
- Most of the attacks have simple and inexpensive countermeasures, but the seal installers & inspectors must:
  - + understand the seal vulnerabilities
  - + look for likely attacks
  - + have seen examples of attacked seals
- Also: better seals are possible!

Anti-Evidence Seals

conventional seals: 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, then erase this 'anti-evidence' when tampering is detected. There is then nothing for an adversary to hide, erase, or counterfeit.

20+ New Anti-Evidence Seals



- inexpensive
- better security
- no tools to install or remove seal
- can be inside or outside container
- 100% reusable, even if mechanical
- can monitor volumes or areas, not just portals
- can automatically verify the seal inspector actually checked the seal

MagTag, Tie-Dye Seal, Magic Slate Seal, Glass & Powder Seal, Triboluminescence Seal, Plug Seal, Talking Truck Cargo Seal, Blinking Lights Seal, Time Trap…

"Town Crier" Monitoring: real-time intrusion detection using anti-evidence

- ideal for transport monitoring
- avoids many of the problems associated with treaty monitoring
- simple, low-cost, robust, high-security
- ultra-low bandwidth (bit/sec to bit/min)

Problem: Lack of Effective Security Features & Tamper Detection

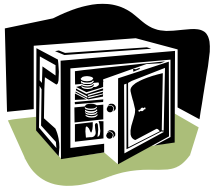
- MC&A hardware
- intrusion detectors
- GPS tracking systems
- access control devices (including biometrics)
- radiological instruments
- video monitoring systems
- instrumentation enclosures

Inventory

- Counting and locating our stuff.
- No nefarious adversary.
- Will detect innocent errors by insiders, but not surreptitious attacks by insiders or outsiders.

Security

- Meant to counter nefarious adversaries, typically both insiders & outsiders.
- Includes Material Control & Accounting (MC&A)
  - looks like inventory but is not
  - often confused with inventory
  - often drifts into inventory



Tags: an example of confusing inventory with security (and high-tech with high-security)

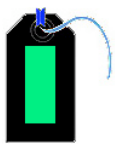
- bar codes

- rf transponders (RFIDs)

- contact memory buttons

Usually easy to:

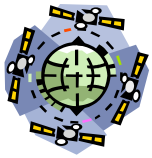
* lift
* counterfeit
* spoof the reader



There are two kinds of fool. One says, "This is old, and therefore good." And one says, "This is new, and therefore better."
-- John Brunner (1934-1995)

GPS: Another classic example of confusing Inventory & Security, High-Tech & High-Security

- The private sector, foreigners, and 90+% of the U.S. government must use the civilian GPS satellite signals.
- These are unencrypted and unauthenticated.
- Civilian GPS was never meant for security applications, yet it is being used that way (e.g., transport security).



Attacking Civilian GPS Receivers

Blocking: just break off the antenna, or shield it with metal; not surreptitious.

Jamming: easy to build a noisy rf transmitter from plans on the Internet; not surreptitious.

Spoofing: surreptitious & (as we've demonstrated) surprisingly easy for even unsophisticated adversaries. *There are simple countermeasures.*

Physical attacks: appear to be easy, too.

GPS Cargo Tracking

GPS Satellite

Tracking Information
Sent to HQ
(perhaps encrypted/authenticated)

GPS
Signal

(vulnerable here)

GPS is great for navigation, but it does not provide high security.

The 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/default.htm

We have a CD containing related papers & reports.

Available today or request a copy at rogerj@lanl.gov

The problem is not that there are problems. The problem is expecting otherwise and thinking that having problems is a problem.
-- Theodore Rubin