LA-UR-05-3658
Approved for public release;
distribution is unlimited.

Title: **Nuclear safeguards and security: we can do better**

Author(s):
Roger G. Johnston
Jon S. Warner
Anthony R. E. Garcia
Ron K. Martinez
Leon N. Lopez
Adam N. Pacheco
Sonia J. Trujillo
Alicia M. Herrera
Eddie G. Bitzer

Submitted to:
Tenth International Conference on Environmental Remediation and Radioactive Waste Management (ICEM'05)
September 4-8, 2005
Glasgow, Scotland

Los Alamos
NATIONAL LABORATORY

LAUR-05-3658

NUCLEAR SAFEGUARDS AND 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
MS J565, Los Alamos, NM 87545 USA

ABSTRACT

There are a number of practical ways to significantly improve nuclear safeguards and security. These include recognizing and minimizing the insider threat; using adversarial vulnerability assessments to find vulnerabilities and countermeasures; fully appreciating the disparate nature of domestic and international nuclear safeguards; improving tamper detection and tamper-indicating seals; not confusing the inventory and security functions; and recognizing the limitations of GPS tracking, contact memory buttons, and RFID tags.

INTRODUCTION

The efficacy of nuclear safeguards depends critically on employing sophisticated security strategies and effective monitoring hardware. The Vulnerability Assessment Team (VAT) at Los Alamos National Laboratory has extensively researched issues associated with nuclear safeguards, especially in the areas of tamper/intrusion detection, transport security, and vulnerability assessments.[1-5] This paper discusses some of our findings, recommendations, and warnings.

THE INSIDER THREAT

The "Insider threat" is the security risk to an organization due to its employees. As a general rule of thumb, most organizations underestimate or even ignore the insider threat.[6-9] This certainly appears to be the case for a number of nuclear safeguard programs.

For example, it is widely recognized that Russia's nuclear safeguards programs typically fail to adequately deal with the insider threat [10,11], largely for historical reasons.[12]

Another example involves the design of material control and accounting (MC&A) equipment used for domestic and international nuclear safeguards. This includes radiological and calorimetric instruments, access control devices, monitoring equipment, and surveillance hardware. In our experience, MC&A equipment is rarely designed with any significant level of tamper detection. It is far too easy for insiders (and potentially even outsiders) to tamper with these devices. The need for better tamper detection is discussed below.

One particularly troublesome insider risk involves the International Atomic Energy Agency (IAEA). The IAEA has been criticized in the past for a lack of security culture and counter-intelligence emphasis.[13] Particularly worrisome is the fact that the IAEA does little or no background checking on employees, either before or after hiring.[13-16] This includes nuclear inspectors, as well as IAEA personnel who coordinate, process, and interpret inspection data.

The absence of substantial background checks is unfortunate from the standpoint of security, counter-espionage, and counter-terrorism. In our view, it is imprudent (especially post 9/11) to allow inspectors extensive access to critical nuclear facilities when basic facts concerning their character, as well as criminal, financial, and drug use histories are largely unknown. It is also inconsistent with the IAEA's call to member states to improve nuclear security and safeguards practices.

The lack of background screening is also troublesome because the IAEA (and the world) must trust the

judgment of the inspectors and their supervisors about whether treaty violations may be occurring. The lack of employee screening places the reliability of inspections (and the IAEA's reputation) at risk. This has the potential of undermining nonproliferation efforts.

It is worth noting that IAEA inspectors (quite appropriately) are granted diplomatic privileges. This is advertised in IAEA job ads.[17] There is a possibility that the position might attract nefarious individuals who are interested in exploiting diplomatic status and frequent foreign travel for criminal or terrorist activities.

In our view, the following arguments do not mitigate the need for background checks on nuclear inspectors and other IAEA employees:

1. IAEA inspectors are usually escorted within an inspected nuclear facility.

2. The professional "reputation" of an IAEA employee is considered in hiring decisions.

3. International differences in attitudes about individual privacy can complicate background checks.

4. Local and European Union regulations may discourage background checks.

5. Background checks are expensive, and will not eliminate the insider threat.

6. Judging the loyalty, veracity, and reliability of people is far from being an exact science.

On the other hand, it must be admitted that having security background checks is no guarantee that they will be implemented effectively.[18] For example, a number of United States government agencies make extensive use of polygraphs for screening employees even though they are highly dubious tools.[19,20] These same agencies often seem to be obsessed with issues of mental health [21], and tend to look askance at employees who have had counseling from psychologists or social workers (thus discouraging the practice), even though there is ample evidence that such professional counseling can improve mental health.[22] An important fact often overlooked is that most of the spies who have been caught in the past were not mentally ill when apprehended.[23,24]

Probably the most powerful tool for countering the insider threat is to treat employees well in order to minimize disgruntlement. (Retirees and terminated employees should also be treated respectfully.) Disgruntlement is known to increase the risk of organizational conflict, workplace aggression and violence, theft, espionage, and sabotage.[25] Unfortunately, the large bureaucratic government organizations that typically control nuclear applications are rarely noted for fairness and empathy in their treatment of people.

ADVERSARIAL VULNERABILITY ASSESSMENTS

In our experience, the traditional tools for improving security—security surveys, risk management techniques, and design basis threat—are inadequate for optimal security.[5] To often, they result in no significant improvements in security, or are simply used to justify the status quo. Moreover, these techniques usually fail to be sufficiently imaginative or proactive in foreseeing threats.

We believe the most powerful tool for uncovering vulnerabilities and devising countermeasures is the adversarial vulnerability assessment (AVA). Unlike the other techniques, AVAs require a major mental coordinate transformation.[5] The vulnerability assessors need to quit thinking like the "good guys" and instead try to get into the heads of the "bad guys" and think like they do. The goal is to *eagerly* look for security weaknesses and vulnerabilities to exploit, rather than trying to reassure ourselves that everything is fine—which is too often the case with security surveys, risk management, and design basis threat.

The prerequisite for an effective AVA is to minimize groupthink and the use of bureaucrats, and instead involve clever, creative, hands-on, non-conformist individuals.[26] The kinds of people that tend to be best at adversarial vulnerability assessments are the very people who are rarely allowed to substantially participate in nuclear safeguards or risk management: smart alecks, trouble makers, schemers, organizational critics, loophole finders, questioners of tradition and authority, outside-the-box thinkers, artists, hackers, tinkerers, problem solvers, and "techno-nerds". The vulnerability assessors must be allowed free reign to consider vulnerabilities and countermeasures. It is also essential for the organization to scrupulously avoid any denial or retaliation when vulnerabilities are inevitably discovered.[5]

DOMESTIC VS. INTERNATIONAL SAFEGUARDS

Traditionally, international nuclear safeguards have been viewed as an extension of domestic nuclear safeguards. Very similar technologies, expertise, personnel, strategies, and funding sources are often employed.[27] This is unfortunate because the two applications couldn't be more disparate.[28]

Domestic nuclear safeguards is very much a traditional security application: the "good guys" own the assets of interest and the facilities where they are stored, and the "bad guys" may attempt to gain access (using insiders

and/or outsiders). Typically, the bad guys will be relatively limited in number of personnel and their capabilities.

International nuclear safeguards, i.e., treaty monitoring is quite different. The adversary is the nation that signed the treaty, and is being monitored for evidence of cheating. This adversary, unlike in domestic safeguards, has enormous (national- or world-class) resources and expertise that could be applied to defeating the safeguards. Moreover, with international safeguards, the "bad guys" now own the assets and facilities of interest, and the "good guys" (inspectors) are not allowed inside the facility much of the time. This kind of backwards security problem has been less than thoroughly analyzed in its proper context.

TAMPER-INDICATING SEALS

Tamper-indicating seals—which detect unauthorized access—play a crucial role in both domestic and international nuclear safeguards.[29] They are important for transport security, nuclear material control and accounting, long-term storage, waste management, quality control, treaty inspections, disarmament, counter-espionage, protecting records, and protecting monitoring and inspection equipment.

We have studied hundreds of different tamper-indicating seals in detail. This includes at least 20 different seals that are currently in use for nuclear applications somewhere in the world, and others that are under consideration. We have demonstrated how all these seals can be defeated quickly, using low-tech tools, methods, and supplies available to almost anyone.[3,30] Often, high-tech electronic seals are easier to defeat than many inexpensive, low-tech mechanical seals.

We have also found the tamper detection capabilities of many other security and monitoring devices to be absent or remarkably unsophisticated. As a result, we believe a wide variety of access control systems, intrusion detectors, radiological/calorimetric monitors, and surveillance hardware are highly vulnerable to spoofing by both insiders and outsiders.

As a result of our work, we have come to the conclusion that conventional tamper detection methods are fundamentally flawed.[30] When a conventional tamper-indicating seal (or tamper-evidence enclosure) is opened, it must store this information (the "alarm condition") until such time as the seal can be inspected. It is, however, far too easy to erase (or hide) the alarm condition, or make a counterfeit fresh seal.[3,30,31]

There is a much better approach to tamper detection, which we call the "anti-evidence" method.[30] Instead of storing the (vulnerable) alarm condition until inspection time, we instead store information at the very start, when the seal is first installed, that tampering has NOT yet occurred. This "anti-evidence" gets instantly erased when tampering is detected. At inspection time, the inspector looks for the anti-evidence. If it is absent or incorrect, she can conclude that tampering has occurred. If, on the other hand, the anti-evidence is intact, then the seal was not opened.

With this anti-evidence approach, an adversary gains nothing by counterfeiting the tamper detection hardware, because he does not know what anti-evidence to store in the seal. (The anti-evidence information is known only to the good guys, is different for every seal, and changes if a given anti-evidence seal is re-used.) Any attempt by the adversary to gain access to the secret anti-evidence causes it to be instantly erases. Moreover, having opened a seal, an adversary does not know how to erase or hide the alarm condition, because the anti-evidence is long gone.

We have devised and demonstrated a number of different anti-evidence seals, mechanical as well as electronic. Figure 1 shows one example, called a "Time Trap". This seal can be placed on the hasp of a container or door. Alternatively (using different sensors), it can be placed inside a container, room, or transport vehicle.

When the Time Trap determines that entry has occurred (it doesn't care whether by good guys or bad guys) it turns on its liquid crystal display. The display then alternates between showing the time that entry occurred (left in figure 1), and the hash (or secret number) for that time (right). There is a different hash for each minute.

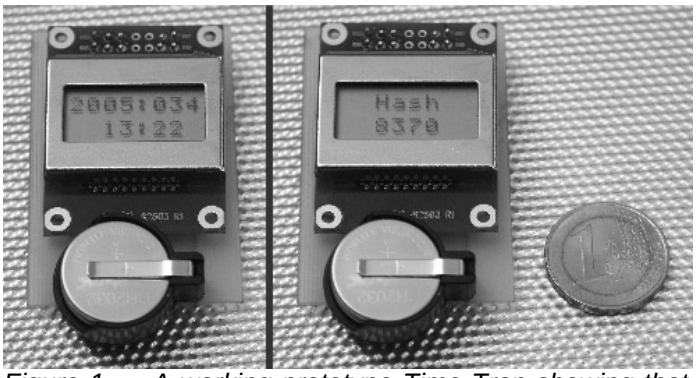

Figure 1 - A working prototype Time Trap showing that entry occurred on February 3, 2005 at 1:22 P.M. The display alternates between the time when intrusion was detected (left) and the hash value for that time (right). If the time is off by more than a few minutes and/or the hash value is wrong or missing, then we must conclude that tampering has previously occurred. This anti-evidence seal is controlled by an onboard programmable microprocessor. The entire device was constructed from less than $8 of parts (retail quantities of 1).

Only the good guys know the correct hash for future times, but the future hash values (and/or algorithm) were instantly erased when the seal detected entry. Thus, the bad guys gain nothing by counterfeiting the seal hardware, nor do they know what the display should read when the good guys eventually open the container, door, or vehicle at a later time.

Some of the interesting attributes of the Time Trap (and other anti-evidence seals include) [30]:

- No tools are needed to install or remove the seal.
- The seal is fully reusable (though, for the best security, a different secret hash key and/or hash algorithm should be used each time).
- "Anti-gundecking": The seal automatically verifies that the seal inspector actually checked the seal for tampering. If the seal inspector is not told the correct hash value for the given displayed time, the act of reporting the time and hash value back to headquarters (using unsecured communications channels) is verification that she actually did check the seal, not just falsely claim to have done so.

Another problem in international nuclear safeguards is that few, if any tamper-indicating seals are currently designed with the idea that the seal installer (or remover) may have a hidden agenda. In many situations (especially for treaty monitoring), inspectors may not be allowed to personally handle containers, nuclear material, or weapons. They may be limited to merely observing while facility personnel (the potential "bad guys") install or remove the seals.

This is a serious problem because with conventional seals, it is all too easy to surreptitiously fail to fully close the seal, or to palm the original seal and actually install or remove a different one. This problem of inspectors not being able to personally install or remove the seal can be substantially overcome through the use of anti-evidence seals. Other approaches can also be helpful for detecting seal subterfuge. These include employing effective seal use protocols [32], and using techniques such as challenge inspections, or "choose or keep", and "keep the used parts" protocols.[33]

REAL-TIME INTRUSION DETECTION

An anti-evidence approach is also attractive for real-time intrusion monitoring of nuclear material, including during transport. It offers the possibility of simplicity and low cost, yet provides very high levels of security. We call such an approach the "Town Crier" method.[4]

Instead of sending an alarm when intrusion is detected—which can be easily blocked—Town Crier monitoring involves sending out a periodic, extremely low bandwidth "All OK" signal (typically less than a few bits/minute) as long as no intrusion has been detected. Only the good guys know what the "All OK" signal looks like at any given time. This approach avoids complex two-way communication, potentially troublesome encryption or authentication methods, and complicated state-of-health checks on the sensors. It has many advantages for transport security, including minimizing power requirements, and avoiding the need to broadcast high bandwidth data from the transport vehicle which advertises to the world the importance of the cargo.

GPS TRANSPORT TRACKING

The Global Positioning System (GPS) is often used or considered for tracking radioactive material, vehicles, or containers during transport. Unfortunately, most if not all nuclear applications (including those done outside the United States) must use the civilian GPS signals, rather than the military signals. The civilian GPS signals were never meant for security applications. They are unencrypted and unauthenticated, and thus not secure.

We have demonstrated how easy it is to spoof (not just jam) GPS receivers using widely available commercial GPS satellite simulators.[34] These simulators can be readily purchased, rented, or stolen. They are not export controlled. An adversary needs little knowledge of GPS, computers, electronics, or even radio frequency (rf) communications to generate fake time and position data. There are simple countermeasures to detect spoofing from commercial GPS satellite simulators [35], but these are not currently in use and will not be fully effective against a more sophisticated spoofing attack.

Another worrisome problem with GPS is that many facilities, organizations, and networks use it for critical time synchronization. This creates a number of serious security vulnerabilities [34,35] that could compromise a nuclear safeguards program (domestic or international).

CONTACT MEMORY BUTTONS & RFID TAGS

Like GPS, contact memory buttons [36,37] and radio frequency identification (RFID) tags [38] are fundamentally inventory technologies that are highly problematic for use in security applications. Inventory involves counting and locating assets, but it does not intrinsically deal with nefarious adversaries. That is the role of security.

Existing contact memory buttons and RFIDs are very useful for inventory purposes, but have typically been designed with little or no thought to attacks from

adversaries. We have, for example, demonstrated that both contact memory buttons and RFIDs are easy to lift or counterfeit, and that it is easy to spoof their readers even without counterfeiting the devices themselves. (To "lift" a tag means to remove it from one object or container and reattach it to another, without being detected.)

Unfortunately, it is very common for inventory devices and systems to undergo a kind of "mission creep".[32] When first employed, they are viewed as inventory tools, but quickly come to (incorrectly) be thought of as providing security. We believe such mission creep is presently occurring for contact memory buttons in nuclear applications, and will occur for RFIDs in the future. Contact memory buttons, for example, have been employed as part of a nuclear "material inventory process". [36] This process, however, eventually gets presented as a technique for "surveillance", inventory "control", "continuous monitoring", and sounding of alarms with anomalous conditions.[37] These are clearly characteristics of security, not inventory.

It is critical to avoid confusing the inventory and security functions because doing so usually leads to very poor security.

CONCLUSION

This paper has briefly discussed a number of aspects of nuclear security and safeguards that can and should be significantly improved. To do so requires critical and creative thinking, the intelligent use of the appropriate tools and technologies, a realistic understanding of problems and vulnerabilities, and avoidance of common fallacies and misconceptions.

DISCLAIMER

The views expressed in this paper are those of the authors and should not necessarily be ascribed to Los Alamos National Laboratory or the United States Department of Energy.

REFERENCES

1. Vulnerability Assessment Team, <http://pearl1.lanl.gov/seals/default.htm>.
2. R.G. Johnston, "Assessing the Vulnerability of Tamper-Indicting Seals", *Port Technology International* 25(1), 155-157 (2005).
3. R.G. Johnston, A.R.E. Garcia, and A.N. Pacheco, "Efficacy of Tamper-Indicating Devices", *Journal of Homeland Security*, April 16, 2002, <http://www.homelandsecurity.org/journal/Articles/displayarticle.asp?article=50>.
4. R.G. Johnston, A.R.E. Garcia, and A.N. Pacheco, "The 'Town Crier' Approach to Monitoring", *International Journal of Radioactive Materials Transport* 13(2), 117-126 (2002).
5. R.G. Johnston, "Effective Vulnerability Assessments", Proceedings of the Contingency Planning & Management Conference, CPM West 2004, Las Vegas, NV, May 25-27, 2004.
6. "Treason101", <http://www.totse.com/en/politics/federal_bureau_of_investigation/163723.html>.
7. S.D. Sagan, "The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Nuclear Security", *Risk Analysis*, 24(4), 935-946 (2004), <http://iisdb.stanford.edu/pubs/20274/Redundancy_Risk_Analysis.pdf>.
8. K. Poulsen, "U.N. Warns of Cyber Attack Risk", *SecurityFocus*, September 27, 2004, <http://www.securityfocus.com/news/9592>.
9. M. Bunn and G. Bunn, "Nuclear Theft and Sabotage: Priorities for Reducing New Threats", I*AEA Bulletin* 43/4/2001, <http://www.iaea.org/Publications/Magazines/Bulletin/Bull434/article5.pdf>.
10. S. Saradzhyan, "Russia: Grasping Reality of Nuclear Terror", BCSIA Discussion Paper 2003-02, Kennedy School of Government, Harvard University, <http://bcsia.ksg.harvard.edu/BCSIA_content/documents/saradzhyan_2003_02.pdf>.
11. Center for International Trade and Security, "Nuclear Security Culture: The Case of Russia", University of Georgia, December, 2004, <http://www.uga.edu/cits/documents/pdf/Security%20Culture%20Report%20041118.pdf>.
12. M. Bunn, "The Threat in Russia and the Newly Independent States", October 28, 2002, <http://www.nti.org/e_research/cnwm/threat/russia.asp>.
13. D. Kay, "The IAEA", in A. Lathan, editor, *Multilateral Approaches to Non-Proliferation*, Proceedings of the 4th Canadian Non-Proliferation Workshop, 1995, pp. 319-332.
14. E.G. Bitzer and R.G. Johnston, "Inspecting the Inspectors: The case for background investigations of IAEA inspectors", Los Alamos National Laboratory report (in preparation).
15. R.G. Johnston, "Tamper Detection for Safeguards and Treaty Monitoring: Fantasies, Realities, and Potentials", *Nonproliferation Review* 8(1),102-115 (2001), <http://www.princeton.edu/~globsec/publications/pdf/9_2johnston.pdf>.
16. James V. Grimaldi, "Weapons Inspectors' Experience Questioned", *Washington Post*, November 28, 2002, Page A01, <http://www.washingtonpost.com/ac2/wp-dyn/A48596-2002Nov27?language=printer>.
17. International Atomic Energy Agency (IAEA), "Jobs at the IAEA", <http://www.iaea.org/About/Jobs/>.
18. E.T. Pound, "How Felons Gain Access to the Nation's Secrets And Why the Government Says it's all Right", *USA Today*; December 29, 1999.

19. A.P. Zelicoff, “Polygraphs and the National Labs: Dangerous Ruse Undermines National Security”, *Skeptical Inquirer*, July 1, 2001.
20. Board on Behavioral, Cognitive, and Sensory Sciences and Education (BCSSE), “The Polygraph and Lie Detection”, The National Academy Press, Washington, D.C. (2003).
21. Defense Security Service, “Relevance to Security”, <http://www.dss.mil/nf/adr/emotion/emoteT1.htm#Behavior%20Patterns%20Associated%20with%20Espionage>.
22. W. McDermut, I.W. Miller and R.A. Brown, “The Efficacy of Group Psychotherapy for Depression: A Meta-analysis and Review of the Empirical Research”, *Clinical Psychology: Science and Practice* 8(1), 98-116 (2001).
23. L.A. Stone, “I Spy a Myth”, *Security Management*, October 1, 1991.
24. L.A. Stone, “MMPI Scorings from Two Major Traitorous U.S. Citizen Spies”, *Psychology of Espionage Reports*, April 2003, <http://www.home.earthlink.net/~lastone2/espionage.html>.
25. R.G. Johnston and M. Bremer Maerli, “The Negative Consequences of Ambiguous ‘Safeguards’ Terminology”, INMM Proceedings, July 13-17, 2003, Phoenix, AZ.
26. M. Caloyannides, “Enhancing Security: Not for the Conformist”, *Security & Privacy* 2(6), 86-88, November-December 2004.
27. M. Bremer Maerli and R.G. Johnston, “Safeguarding This and Verifying That: Fuzzy Concepts, Confusing Terminology, and Their Detrimental Effects on Nuclear Husbandry”, *Nonproliferation Review* 9(2), 54-82 (2002), <cns.miis.edu/pubs/npr/vol09/91/91maerli.pdf>.
28. R.G. Johnston and M .Bremer Maerli, “International vs. Domestic Nuclear Safeguards: The Need for Clarity in the Debate Over Effectiveness”, *Disarmament Diplomacy*, issue 69, February-March 2003, <http://www.acronym.org.uk/dd/dd69/69op01.htm>.
29. R.G. Johnston, "Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management", *Science and Global Security* 9(3), 93-112 (2001), <http://lib-www.lanl.gov/la-pubs/00818333.pdf>.
30. R.G. Johnston, “The ‘Anti-Evidence’ Approach to Tamper Detection”, *Packaging, Transport, Storage and Security of Radioactive Material* (in press).
31. R.G. Johnston and A.R.E. Garcia, "An Annotated Taxonomy of Tag and Seal Vulnerabilities", *Journal of Nuclear Materials Management* 28(3), 23-30 (2000).
32. R.G. Johnston, “How to be a Better Seal User”, Los Alamos National Laboratory Report LAUR-03-6179 September, 2003.
33. E.R. Gerdes, R.G. Johnston, and J.E. Doyle, "A Proposed Approach for Monitoring Nuclear Warhead Dismantlement", *Science and Global Security* 9(1), 113-141 (2001), <www.princeton.edu/~globsec/publications/pdf/9_2gerdes.pdf>.
34. J.S. Warner and R.G. Johnston, “A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing”, *Journal of Security Administration* 25(2), 19-27 (2002).
35. J.S. Warner and R.G. Johnston, “GPS Spoofing Countermeasures”, *Homeland Security Journal*, December 12, 2003, <http://www.homelandsecurity.org/bulletin/Dual%20Benefit/warner_gps_spoofing.html>.
36. C.A. Pickett, “Active Tag and Seal Technologies Designed for the Unattended Monitoring of Stored Nuclear Materials”, Proceedings of the Fourth Security Seals Symposium, June 15-16, 1999, Oxnard, CA, pp. 69-74, <http://locks.nfesc.navy.mil/pdf_files/8057sp.pdf>.
37. Oak Ridge National Laboratory, “Precision Inventory Control and Accountability: SmartShelf Technology”, <http://www.y12.doe.gov/orsens/smrtshlf.htm>.
38. M. Bhuptani and S. Moradpour, *RFID Field Guide: Deploying Radio Frequency Identification*, Prentice Hall, 2005.