Tamper Detection for Safeguards and Treaty Monitoring: Fantasies, Realities, and Potentials

Tamper detection has an important role to play in domestic nuclear security and safeguards, as well as in international verification and treaty monitoring. Unfortunately, ideas about tamper detection often seem to be based on misconceptions, fuzzy goals, and wishful thinking. Current tamper detection programs are hampered by these problems, as well as by poor training, limited analysis, vague (or nonexistent) standards, “see-no-evil” mentality, “one-size-fits-all” thinking, and unmitigated vulnerabilities. Better approaches, more sophistication, improved hardware, and greater understanding are sorely needed for both current and future applications.

In this essay, I review tamper detection devices, particularly tags and seals, and then discuss the erroneous beliefs held by many nuclear security practitioners about the effectiveness of these devices. Next, I explore the general problems that plague the use of seals and other tamper devices in the United States and worldwide, and then look at specific problems in U.S. and Russian material protection, control, and accounting programs (MPC&A) and in the International Atomic Energy Agency’s (IAEA’s) tags and seal program. I conclude with a survey of new tamper detection applications and recommendations for improving tamper detection both for domestic security and international transparency and treaty monitoring. Throughout, I argue for a more realistic assessment of the possibilities and vulnerabilities of tamper detection devices.

TAMPER DETECTION MEASURES

Tamper detection often involves the use of tags and/or seals. Tags are applied or intrinsic features or devices used to identify an object or container. Familiar examples of tags from everyday life include car license plates and the holographic design found on many credit cards. Seals are tamper-indicating devices (TIDs) meant to detect unauthorized access to a door, container, or package.6 Familiar examples of seals include the tamper-indicating packaging required on all U.S. over-the-counter pharmaceuticals, and the inexpensive plastic or wire seals often installed on home or commercial utility meters in the United States to detect pilferage.

Thousands of different seals are currently available, including both passive and active devices. Passive seals include irreversible mechanical assemblies, frangible
foils or films, epoxies, adhesive labels, wires or cables, optical fibers, and other devices and materials that become damaged or show changes when cut or manipulated. There are currently two types of active seals: electronic and fiber optic. Electronic seals continuously monitor for some kind of change indicative of tampering. Active fiber optic seals periodically or randomly send light pulses down a fiber optic bundle (or single fiber) to check continuity.

It is important to realize that seals—unlike locks—are not intended to resist unauthorized access or entry. Instead, they are meant to indelibly record that such access took place. Indeed, some seals are made of paper or plastic and can be easily torn by hand; however, this does not inherently make them ineffective for tamper detection. Another issue that sometimes causes confusion is the partial interchangeability of tags and seals. A secure seal must have tag-like attributes, and vice versa. As a consequence, a device that is primarily being used as a seal may have secondary uses as a tag, while a tag may also be useful for detecting tampering.

One of the critical issues in tamper detection and verification is whether a given tag or seal can be “defeated,” and if so, how easily. “Defeating” a seal means to spoof it. Though there are other kinds of attacks, defeating a seal typically involves opening it, then resealing without being detected, using either the original seal or a counterfeit. If the original seal is used, the seal might be opened without damage or evidence of opening, or else the damage and/or evidence must be erased or hidden. In a similar manner, defeating a tag means counterfeiting the tag without being detected, or else lifting the tag and reapplying it to another object or container without being detected. To “attack” a tag or seal means to undertake a sequence of actions intended to defeat it.

Any given tag or seal is potentially susceptible to hundreds of different kinds of attacks. In the case of seals, the wide variety of possible attacks can be grouped into the following categories:

- tampering with the seal or seal design prior to use, in order to install a backdoor;
- opening and then closing the seal without damaging it or creating evidence of entry;
- hiding or repairing any damage to the seal as a result of opening it;
- hiding or erasing any evidence of entry as a result of opening the seal;
- replacing the seal with a duplicate or counterfeit (or replacing certain parts);
- tampering with the seal data;
- tampering with the seal installation, inspection, or interpretation process;
- bypassing the seal and attacking the container or hasp instead;
- false alarming and discrediting;
- social engineering, bribery, or intimidation; and
- hybrid or alternative methods.

In addition to tags and seals, tamper detection for nuclear security or verification purposes may also involve the use of intrusion detectors, portal monitors, information barriers, and video surveillance. Intrusion detectors (essentially “burglar alarms”) are often used in conjunction with seals; they differ in that they report unauthorized entry in real-time, rather than later at the time of inspection. Such detectors offer the advantage that security forces can respond quickly to intruders. Typical disadvantages as compared to seals include significant occurrences of false alarms, high cost, the need for electrical power, and the additional vulnerabilities associated with sending an alarm signal to a distant location for interpretation. Portal monitors (such as radiation sensors or metal detectors) observe the comings and goings through entryways, doors, and hallways to control access and to assist with containment. Information barriers are hardware or software designed to block or filter the release of specific information. They are envisioned as a way to prevent radiation detectors from revealing classified information while still providing useful results to nuclear inspectors. Video cameras are frequently proposed or used to reduce the intrusiveness or manpower requirements for security, safeguards, and verification applications. While intrusion detectors, portal monitors, information barriers, and video cameras can sometimes be used in place of tags or seals, they must still be protected from tampering themselves. This can be addressed through the use of additional tags and seals.

TAG AND SEAL FANTASIES

Many analysts have expressed realistic views about the limitations and fallibility of verification, tamper detection, and tags and seals. There are also persuasive calls for better worldwide practices and standards for the safeguarding of nuclear materials. Nevertheless, among many nuclear security practitioners, as well as disarmament/nonproliferation theorists, there continues
to be an erroneous belief that totally “tamper-proof” tags, seals, and other monitoring technologies exist, or will exist in the near future. This is a fantasy.

The term “tamper-proof” is particularly unrealistic and even nonsensical. Most tags and seals will break if they are struck hard enough with a hammer. This is a particularly vehement kind of tampering. By “tamper-proof,” however, most people probably mean that the tag or seal cannot be defeated. Even in this context, however, the term “tamper-proof” is problematic because it is usually not possible to prove a negative. How can one prove that a tag or seal cannot be defeated for every possible adversary, attack strategy, and attack technology, present and future? Any given vulnerability assessment may fail to find vulnerabilities—though this should be viewed as an inherently suspicious result. It may mean merely that the study lacked adequate funding, time, technology, personnel, expertise, motivation, or cleverness to find some of the inevitable vulnerabilities. It is also often the case that the assessors do not really want to find vulnerabilities. The assessors are sometimes the tag/seal developer or promoter, or may be under subtle or not so subtle pressure to “certify” that the tag or seal is ready for field use after large sums of money have been spent on its development and/or procurement. The embarrassing discovery of vulnerabilities can cause unwelcome consternation.

The use of the term “tamper-proof” is sometimes excused by saying that it is not meant literally. In my experience, however, people using this term usually do mean it literally. Those who do not, however, should avoid such sloppy terminology. When issues of nuclear warfare, terrorism, and national security are involved, and when disarmament and nonproliferation regimes require international diplomacy and multi-lingual translations, it is essential to use precise terminology. Words are powerful. The phrase “tamper-proof seal” has become so ubiquitous, that people come to believe it literally. Indeed, I have been told more than once by security personnel, including those involved in domestic nuclear security and safeguards applications that, “our seals are tamper-proof,” apparently based primarily on the fact that they are called “tamper-proof seals.”

The issue of vulnerability is important because theorists planning START III or other disarmament, nonproliferation, or safeguards regimes often rely heavily on the use of indefeatable tags, seals, video cameras, and other monitoring hardware. (These invulnerable devices may or may not be called “tamper-proof” by the theorists themselves.) In some cases, invulnerable tags, seals, or other monitoring hardware is envisioned as the sole or most critical means for verification of treaty compliance, with absolute verification often being thought essential for the success of the regime.

The imaginary, “tamper-proof” tags and seals that are invoked by theorists are often not identified. When they are, they are usually described as electronic or fiber optic seals, or tags based on intrinsic microscopic surface roughness or other complex surface features. Often they will report their status remotely, or else will be inspected every few months or years as part of a periodic on-site inspection. In either case, the inspectors will have total faith that these tags and seals will detect diversion or undeclared activities because they are “tamper-proof.” The fact that the tags and seals will be out of the hands of the inspectors for extended periods of time and under the control of the nation being monitored (with all its massive resources), is thus not considered a problem.

Some of these hypothetical tags and seals appear to have an amazing power beyond being merely “tamper-proof” themselves. They apparently can impart “tamper-proofness” on the objects or containers to which they are attached. Thus, if a “tamper-proof” tag is attached to a missile, for example, we apparently do not need to worry about attempts to cut into the missile at a location well away from the tag in order to remove the contents. The tamper-proof “aura” of the tag somehow prevents this. Similarly, “tamper-proof” seals seem to somehow impart “tamper-proofness” on entire containers and on the container hasp to which the seal is attached.

To their credit, some theorists at least try to devise a mechanism for this volumetric protection. For example, it is suggested that multiple fiber optical cables could be used to form a net around the object to be protected. It is not clear, however, what keeps the nodes of this net intact and safe from movement and physical tampering.

The unfortunate reality is that there is no convincing evidence that “tamper-proof” tags and seals exist and a number of reasons to believe they are not possible. There is, furthermore, little theoretical understanding of tamper detection, no useful tag/seal vulnerability testing standards, and (as discussed above) no way even
to prove a given tag or seal is tamper-proof. Indeed, ALL seals that have been subject to a comprehensive and effective vulnerability assessment by personnel intent on finding problems (rather than striving to “certify” the seal) have shown significant vulnerabilities, though details of the application and the exact use protocols appear to be highly relevant. Moreover, there has been remarkably little research and development (R&D) by government or the private sector in the past six-plus years devoted to developing new, high-security tags and seals, especially for transparency and treaty monitoring applications. This, despite the fact that dramatically better tags and seals seem possible, are clearly needed, and that additional R&D on verification technologies has been repeatedly called for over the years.

The common assumption that the best seals will always be high-tech is also dubious. Los Alamos National Laboratory found, after studying 135 seals in detail, that high-tech seals are often easier to defeat than low-tech seals. There are a number of possible reasons for this, including the fact that low-tech, hands-on verification methods often work best and are easier to negotiate. Even if high-tech seals were to provide superior tamper detection, they might still not be appropriate for certain applications (such as use in Russia) because of the problems associated with upkeep and sustainability, their susceptibility to unpredictable failure and radiation damage, and concerns (by the nation being inspected) about safety and espionage during treaty monitoring.

A related, equally common assumption is that tampering can be better detected if the seals (even if low-tech) are read with high-tech readers. “Readers” are electronic or optical devices (often hand-held) used in the field to inspect a seal to determine if tampering has occurred. The reality is that high-tech readers, at least the way they are typically used, often decrease security. Even though high-tech readers are usually introduced in order to save time and money, seals read by high-tech readers typically require more effort—not less—than manually inspected seals to achieve reliable tamper detection.

Another fantasy some disarmament theorists float about is the idea of using high-tech black boxes for treaty monitoring. “Black boxes” are on-site monitoring devices owned by the inspectors that are not fully described to the inspected (host) nation in terms of function, mechanisms, encryption, and/or detailed technical specifications. Given, however, the current meticulous, mandatory requirements for obtaining nuclear explosive safety (NES) and security approval for any kind of equipment brought into MPC&A control areas inside U.S. nuclear facilities, as well as the inevitable concerns by any inspected nation about loss of secret information, it seems highly unlikely that mystery hardware, encryption, or “traps” (covert seals) will be allowed inside sensitive nuclear facilities, or anywhere near nuclear warheads.

GENERAL PROBLEMS

The way seals are currently used in the United States and worldwide for nuclear (or other) applications is far from ideal. Seals are frequently chosen for a given application without careful analysis, and sometimes based on hearsay. Seal vulnerabilities are rarely understood and effective countermeasures are usually lacking. The training of seal inspectors typically emphasizes rigid formality rather than the flexibility and observational skills required to provide effective real-world security. Seal inspectors are usually given little useful information on how to detect tampering, no information about the vulnerabilities and most likely attack scenarios for the seals they are using, and zero practice at detecting seals that are attacked either crudely or subtly. Effective, independent, periodic vulnerability assessments of tamper detection programs or devices are rare; vigorous outside input and review are even rarer. When vulnerability assessments are undertaken, the findings and recommendations are often ignored.

Even more counterproductive—at least from the viewpoint of a vulnerability assessor—are attempts to suppress vulnerability findings, or even the assessors themselves. It is not unusual, in my experience, to demonstrate a seal vulnerability to security personnel, and then have them request (or demand) that, “this not be discussed with my superiors.” This is not the sign of a healthy security program! Vulnerabilities are always present. The discovery of them should ideally be viewed as good news since it allows the possibility of improving security.

Many current seal users appear to believe (incorrectly) that the seals they are using are “tamper-proof,” or nearly so. In my experience, they usually quickly change their minds when one or more attacks are demonstrated on the seals they are using. They then often contemplate
doing away with seals entirely. This may be an example of what Kevin J. Soo Hoo calls (in the context of computer security) a “binary” view of security: “...systems are [believed to be] either secure, in which case they have no vulnerabilities, or are insecure...”. The more realistic and useful view is that security is a continuum. Seals (like everything else in the world) are imperfect compromises and will always have vulnerabilities. Some of these vulnerabilities may be very serious, others can be mitigated or eliminated with countermeasures, and others will never even be known by the user.

Unfortunately, nuclear tamper detection programs sometimes insist—for political, self-image, or public relations reasons—that vulnerabilities do not exist, have never existed, and never will exist. Such a position is irresponsible. One also often hears assurances from seal users that seal tampering has never occurred. This conclusion is highly problematic. Without an independent method of verifying that there has been no tampering or diversion, e.g., by establishing a material balance, seal inspections alone cannot support such a conclusion. By definition, defeated seals are never detected.

It is not uncommon for security managers to have little interest in the vulnerabilities of the seals they are using. The reason typically given (other than that the seals are “tamper-proof”) is that there are multiple layers of other physical security to “backup” the seals should they be defeated. There are five serious problems with this rationale. Firstly, seals should not be considered part of the physical protection system (the “P” in “MPC&A”) for nuclear materials as they often are; seals are more properly part of the control and accounting function (“C&A”). Secondly, the idea that the alarms and security failures at one level of security will be automatically compensated for by other layers is surely a recipe for lax security. Each layer must be taken seriously in its own right and optimized to the extent practical. Thirdly, seals (and tags) will often be the security feature found physically closest to the nuclear material or warhead being monitored. As such, they are certainly deserving of serious consideration. Fourthly, dismissing seal vulnerabilities as not worth correcting might be valid if the countermeasures required substantial cost or difficulty. In many cases, however, effective countermeasures for seal vulnerabilities can be implemented relatively cheaply and easily.

A fifth reason that it is dangerous to assume that seal failures will be caught by other levels of security is that potential adversaries do not necessarily have to defeat all the outer security layers. An insider such as a security guard who attempts to divert nuclear materials or to sabotage operations will already be authorized to pass through many or all of these outer layers of physical security. External inspectors will typically be escorted past at least some of the layers of security in order to accomplish their assigned tasks. In the case of transparency and treaty monitoring, furthermore, the nation being monitored owns the facility and most or all of its layers of security. Thus, at least some of these security layers do not provide “backup” to the tamper-indicating seals because the people who control these layers are the potential adversaries being monitored by the seals!

One of the continuing problems in applying tamper detection to transparency and treaty monitoring is confusion about how they differ from domestic security and safeguards. It is often assumed that existing domestic security and safeguards measures (including seals) can simply be borrowed with little modification for use in transparency and treaty monitoring. In reality, domestic “safeguards” differ dramatically from international (IAEA-like) “safeguards” in terms of goals, personnel, economics, environment, adversaries, secrecy, confidence in the preceding and subsequent processing steps, optimum hardware, who owns/operates/installsthe hardware, and consequences of a safeguards failure. These differences are often ignored. We are assured, for example, that perimeter monitoring for international nuclear production monitoring will be “easier than it first appears because sensitive production facilities presumably already have a perimeter security system.” This overlooks the fact that the existing perimeter security system has a completely different purpose, different potential adversaries, and is owned, operated, and controlled by the nation being monitoring for treaty compliance. Similarly, discussions about how START III might be implemented at the U.S. Pantex warhead storage and dismantlement facility in Texas are often prefaced on the idea that international inspectors can simply use the existing Pantex seals and seals database for treaty monitoring functions. This makes no sense because the domestic seals are intended to deal with one type of adversary—an individual or small group working at cross purposes to the facility—while seals for transparency and treaty compliance monitoring are intended to detect tam-
pering by the very nation that owns the facility. The monitored nation that is the adversary for international “safeguards” will have six to nine orders of magnitude more resources than the rogue individual or relatively small group of concern to domestic nuclear “safeguards.”

Seals for transparency and treaty monitoring applications require significantly different attributes than seals used for U.S. domestic security and safeguards. Existing domestic seals, for example, are not designed to give observers (or video cameras) a good view of seal installation, inspection, and removal. Yet such “transparency” may be essential for bilateral or trilateral monitoring of nuclear warhead dismantlement. The reason is that foreign inspectors are unlikely to be permitted to handle nuclear warhead containers or to directly install seals on them due to nuclear explosive safety (NES) and security concerns. Instead, host facility personnel will probably install and remove seals under the watchful eye of inspectors. Even if foreign inspectors are eventually allowed to personally install seals on warhead containers, however, current seal designs and use protocols for domestic security and safeguards are based on the idea that the seal installer has no hidden agenda. This is not a given for treaty monitoring.

Another problem with current tamper detection practice is that, although it is well over 7,000 years old, the field remains poorly understood. There is no underlying theory, and surprisingly little published (classified or unclassified) about tags and seals. Only a handful of security or physical security textbooks devote more than a paragraph to seals, and fewer still mention tags. There is no general text on the subject of tamper detection. The few standards that exist for seals are neither comprehensive nor substantive regarding seal choice, performance, or how vulnerabilities should be tested. There is considerable discussion about “international norms or standards” for the general physical protection of nuclear materials, as well as great interest in the U.S. “Stored Weapons Standard” and the IAEA (INFCIRC/225, Revision 4) recommendations for protecting nuclear materials. None of these, however, have much to say about tags, seals, and tamper detection.

SPECIFIC PROBLEMS

As has been well documented and discussed, Russian nuclear MPC&A, including technical assistance provided by the United States, has a number of serious problems. Russia tends to use antiquated seals, seals that can be trivially defeated, or no seals at all. The Russians often seem relatively uninterested in dealing with insider threats. There is no comprehensive MPC&A testing program and no push from the U.S. Department of Energy (DOE) to install one, though this is essential for effective operation. Overall DOE management of MPC&A assistance programs to Russia has been far from ideal, and the U.S. Department of Defense (DOD) threat reduction programs are also beset with difficulties. In the case of the Mayak Fissile Material Storage Facility, for example, DOD is unclear about what the United States is supposed to be “verifying,” i.e., the effectiveness of the Russian domestic MPC&A program or Russian compliance with bilateral/trilateral agreements, or both. Both DOE and DOD are deeply confused about the differences between domestic security and safeguards versus transparency and treaty monitoring, and about what security or monitoring hardware is appropriate for use in Russia and who should own and operate it.

In contrast to Russia, the U.S. domestic nuclear MPC&A program is generally recognized as being the most rigorous and effective in the world. There have been, however, continuing problems and criticisms, and there is clearly significant room for improvement. When it comes to tamper detection, the DOE complex generally lacks sophisticated seal knowledge or implementation. Many DOE managers believe that DOE uses “tamper-proof” seals. The main DOE handbook for safeguards seals programs is remarkably devoid of useful information about seals, and shows no interest in training that would let seal inspectors understand seal vulnerabilities and likely attack scenarios. DOE, furthermore, maintains that seals can help to reduce personnel radiation exposures. In reality, the way some passive seals are used does the exact opposite. DOE seal installation, inspection, and removal often require such time-consuming manual procedures that personnel receive exposures that would be unnecessary if seals were not used. DOE’s frequent double-checking of seals, and ordering of replacement seals when security procedures are second-guessed, also adds extra personnel radiation exposure.

There are seals in use for U.S. domestic nuclear security and safeguards that have never undergone any kind of vulnerability assessment, seals that have undergone only cursory vulnerability assessments or “certification”
testing (sometimes by the developer or promoter of the seal), and seals that have undergone vulnerability assessments producing significant findings that are ignored or unknown to the seal users. Few seal users or security managers within the U.S. nuclear complex appear to have even a rudimentary understanding of the vulnerabilities associated with the seals and use protocols that they employ.

A particularly unfortunate practice in recent years has been the premature transfer to the international community of MPC&A methods and hardware used for U.S. domestic security and safeguards. Technology transfer may well be warranted after hardware characteristics and vulnerabilities are well understood, or when the hardware clearly offers only modest security, or is not implemented in U.S. nuclear facilities. It does not seem prudent, however, to hand over critical domestic MPC&A systems when the United States has only a rudimentary understanding of the issues associated with their use. Not only does this potentially compromise U.S. national security, but also it severely confuses the differences between security and safeguards applications versus those of transparency and treaty monitoring. No one security system or device can be optimized for both kinds of applications.

Turning to the IAEA, it is clear that the agency must deal with a variety of difficult challenges and constraints including the “zero-budget growth” policy, funding holdups, limited resources, morale problems, cultural and language differences, harsh and sometimes adversarial field conditions, the need to work closely with bureaucratic governments and diverse member states having conflicting agendas and widely differing attitudes about security, and unrealistic expectations from some critics. Despite all these challenges, the IAEA operates a safeguards program with a truly commendable degree of professionalism, quality, and efficiency. The IAEA has a sophisticated tags and seals program, and considerable understanding of practical tamper detection issues. It conducts first-class postmortem exams on seals returned from the field. The IAEA also has a highly educated, well-motivated group of inspectors unequaled in the world in terms of qualifications and dedication.

The IAEA, however, appears to have a number of deficiencies and problems, at least in regards to tamper detection. The agency takes a somewhat binary view of its safeguards (as discussed above), and largely maintains—without convincing arguments—that its seals are tamper-proof. The IAEA has also been accused of lacking sufficient transparency in its safeguards programs, and failing to undergo or accept sufficient outside, independent review and feedback that may not always be positive. There are concerns about the agency’s willingness to aggressively report evidence of tampering, diversion, or cheating; concerns about its lack of intelligence capabilities; and concerns about public misconceptions of what the agency does.

The IAEA is generally conscientious about arranging for vulnerability assessments on many of the seals it uses. It often begins thorough vulnerability assessments, however, only after having (at least informally) committed to using a given seal design. The agency has no substantial in-house tags/seals R&D program, and no internal program for conducting vulnerability assessments or optimizing seal use. The IAEA relies instead upon uneven technical assistance provided in an ad-hoc, political, and inefficient manner by various member states, with limited and unreliable funding. It is not clear that the vulnerability assessment findings that are generated are fully incorporated into IAEA seal use protocols, inspector training, or postmortem exams, or that the seals that are chosen in the first place are optimum for the application of interest. Though highly trained and motivated, IAEA seal inspectors are typically unfamiliar with the vulnerabilities of the seals they are using or with the most likely attack scenarios. This greatly decreases the odds that they can detect tampering. There are also concerns that IAEA inspectors lack a holistic, proactive, and critically observant approach, and that they are not permitted the necessary flexibility or individual initiative.

The IAEA conducts blind (not double blind) tests on its seals program to check if defeated seals will be detected. These tests, however, appear to be more focused on quality control than evaluating the probability of detecting real-world tampering. The test seals introduced into the postmortem analysis primarily involve substitution or blatant tampering, instead of seals that have been attacked with more subtle and realistic methods.

Another problem that should be of enormous concern for any safeguards or on-site inspection program is the reliability of security personnel and inspectors. IAEA INFCIRC/225 recommendations on background checks are vague, and IAEA inspectors themselves appear to
undergo no significant background screening either before or after being hired. The reliability of tag and seal inspectors is a critical issue for effective tamper detection and can be the source of serious vulnerabilities. Apart from their role in tamper detection, giving inspectors who have not undergone a thorough background screening access to nuclear facilities and nuclear materials is unwise. Many IAEA inspectors, safeguards personnel, and high-level managers are probably more thoroughly screened when applying for a personal credit card than when they are granted access to seals, safeguards data, monitoring hardware, and nuclear materials and facilities. The IAEA also appears unprepared for social engineering and other attacks upon seal inspectors and managerial IAEA personnel involved in the safeguards program.

The reliability of IAEA safeguards and tamper detection is weakened by the organization’s lack of basic security measures. Little of substance has changed from 1994 when David Kay accused the IAEA of being “…an international bureaucracy that does not even perform background checks on its own staff before or after hiring, has no real communications security, does not have document storage that measures up to national secure storage standards, and lacks any counterintelligence culture or capability.”

NEW TAMPER DETECTION APPLICATIONS

There is considerable interest in using “e-monitoring” such as video surveillance and remote monitoring systems for treaty monitoring purposes. Traditionally, video surveillance has been used to protect facilities from outside attack, or for double-checking the activities of insiders. In the case of treaty monitoring, however, the potential adversaries are typically neither outside intruders nor rogue insiders. The adversary is the nation that owns the facility and the very walls that the video cameras are mounted on. Little analysis of video security has been conducted in this context, a context that is not simply a trivial extension of conventional video monitoring approaches.

The limited vulnerability assessment that has been done for video signals and video encryption usually assumes that the sending unit and the receiving station are physically inaccessible to the adversary. This is not a safe assumption given the relatively mundane efforts undertaken to date to protect video surveillance systems from physical tampering at the sending or receiving end, and to guard against counterfeited optical or electronic signals. Sensor data from other types of remote monitoring devices are also subject to tampering.

Even if the hardware is somehow “tamper-proof,” the video encryption (or authentication) itself is likely to be vulnerable to attack. This particularly should be a concern given that the most advanced encryption methods are unlikely to be available for international treaty monitoring, and that the monitored nation may be able to marshal considerable resources to break an encryption algorithm.

Continuous, close-up video monitoring of tags and seals is an unconventional type of video monitoring that may prove useful for nonproliferation or dismantlement regimes. It is not uncommon to use video cameras in security applications that also employ seals. Ordinarily, however, the video surveillance is directed at a room, portal, or at people; it is usually not focused close-up on the seals themselves. Little is understood about the vulnerabilities and optimum use protocols associated with close-up, continuous video surveillance of tags and seals.

Another potentially important application for seals in treaty monitoring involves preserving inspection evidence, such as environmental samples. International arguments about the veracity of environmental samples may eventually become as controversial as arguments about drug testing results for world-class athletes.

WHAT IS NEEDED?

Given the variety of problems discussed above, what is needed for better tamper detection—both now and in the future—for domestic security and safeguards, as well as for international transparency and treaty monitoring? Here are some recommendations.

1. Existing seals need to be used more effectively. This should include implementing better use protocols and more relevant training that fully incorporate a sophisticated understanding of the vulnerabilities and most likely attack scenarios of the specific seals being used. Seal inspectors should practice detecting subtlety attacked seals, and should be encouraged to think about seal vulnerabilities.

2. Existing seals and tamper detection programs need more vulnerability assessments. Any resulting recommendations should be implemented if useful, practical, and cost-effective.
3. At least some minimal level of background screening should be implemented for seal inspectors and tamper detection personnel, as well as for other inspection personnel granted access to nuclear facilities.
4. Existing seals need to be chosen with more analysis and care.
5. New/better tags and seals need to be developed, especially for transparency and treaty monitoring applications. Their vulnerabilities need to be fully understood. Better containers are also needed.
6. There should be R&D on protecting video surveillance equipment and other types of remote monitoring hardware from tampering.
7. Studies should be undertaken to understand the security implications and vulnerabilities of close-up, continuous video monitoring of tags and seals.
8. Tags, seals, and tamper detection in general deserve more theoretical study and practical analysis. This should include developing a better understanding of what to do when tampering evidence is found. This is usually not well worked out in current tamper detection programs.
9. Security norms and standards for tamper detection should be further developed and widely adopted.
10. We need realistic expectations and an understanding that treaty verification is, in the end, a probabilistic, “interpretive activity” that involves both evaluating the evidence and attempting to understand its meaning. No matter how sophisticated and quantitative the monitoring technology, or how great our confidence (rightly or wrongly) in it, verification will always come down to subjective judgments.

When it comes to tags and seals, the point is not to despair of the possibility of effective verification, or to abandon the use of tags, seals, and video surveillance simply because they—like all security measures—have vulnerabilities. Rather, the prudent approach is to have a realistic, continuum (non-binary) view of verification and tamper detection, a clear understanding of the vulnerabilities of the devices and security programs being used or contemplated, a willingness to incorporate reasonable countermeasures into the devices or the overall tamper detection program, and a commitment to engage in R&D to improve tamper detection and to better understand its role and limitations.

In the end, the realistic goals of any tamper detection program should be to:
1. detect amateurish or overt tampering with high probability;
2. detect tampering by a sophisticated adversary with some probability significantly above zero (but that will never be 100 percent), maximized to the extent consistent with a cost-benefit analysis;
3. have a low false alarm rate; and
4. provide a significant level of psychological deterrence by making would-be tamperers spend significant amounts of money developing/implementing an attack, and also make them worry about getting caught.

Finally, it may be worth noting that treaty verification would be considerably easier, cheaper, more negotiable, and more reliable if a limited amount of classified information could be shared between each party to a treaty. A partial release of sensitive or classified information tends to occur over time as nonproliferation or dismantlement regimes are maintained, especially when intrusive on-site inspections are involved. It would be useful for both Russia and the United States to undertake a realistic review of what must truly be kept secret from each other. There may well be a category of information that can be shared between the two nations, but that must not be released to the public or to third parties. The likely problem with this kind of review is that it must be thorough, holistic, and well balanced. Security managers, weapons designers, and conservative political leaders will tend to see the harm done to national security by releasing some of their own country’s secrets, but may ignore or underestimate the benefits to national security of learning the analogous secrets of the other side. Intelligence analysts and disarmament advocates, on the other hand, may tend to get excited about the new information that can be gained from the other side, while being less concerned about the implications of giving up the secrets of their own nation.

---

1 The views expressed in this paper are those of the author and do not necessarily reflect any official position of the Center for International Security and Cooperation (CISAC), the United States Department of Energy (DOE), or Los Alamos National Laboratory (LANL).
2 Tampering with nuclear weapons or nuclear materials is defined as gaining unauthorized or surreptitious access for purposes of theft, diversion,
sabotage, vandalism, espionage (military, political, or industrial), or in an attempt to cheat or breakout from a treaty, commitment, or declaration.

2 The term “safeguards” as used by the U.S. government typically means domestic nuclear Material Protection, Control, and Accounting (MPC&A) functions. Sometimes nuclear “security” and “safeguards” are considered separate functions, in which case the former is the “P” in “MPC&A” and the latter is the “C&A.” There can be confusion about the differences between domestic “safeguards” and IAEA international “safeguards,” the latter really being treaty monitoring, not nuclear custodianship.


5 Tamper-evident (tamper-indicating) packaging and so-called “secure containers” are other forms of tamper-indicating seals.

6 It is thus not helpful to define a lock as “a device similar to a seal except that it can be opened with a key” as is done in Patricia Lewis, “The New Verification Game and Technologies at Our Disposal,” in Dietrich Schroer and Alessandro Pascolini, eds., The Weapons Legacy of the Cold War: Problems and Opportunities (Brookfield, VT: Ashgate, 1997), p. 151.

7 DeVolpi, Tags and Seals to Strengthen Arms Control Verification, pp. 1-10.


10 Ibid.

11 “Social engineering” is compromising security by manipulating, exploiting, or compromising people.


13 Duncan W. MacArthur and Rena Whiteson, Comparison of Hardware and Software Approaches to Information Barrier Construction, Los Alamos National Laboratory Report LAUR-00-2422.


17 The term “tamper-resistant” is sometimes used instead of “tamper-proof” when discussing tags and seals. This is at least less absolute, but it is still misleading. Many seals are made of paper or plastic and can be easily ripped open—thus not resisting tampering in the slightest. This does not automatically make them ineffective as seals. Because they were so misleading, the U.S. Food and Drug Administration abandoned its original terms “tamper-proof” and “tamper-resistant” in referring to packaging, and now requires “tamper-evident” packaging for over-the-counter pharmaceuticals. Note that we can probably dismiss as disingenuous the idea that the “tamper-resistance” provided by a seal actually refers to the (very real) psychological hesitancy on the part of an adversary to attempt tampering if he may be caught by the seal.


Seals...allow conclusions that no material has disappeared,” according to IAEA, International Safeguards and the Peaceful Uses of Nuclear Energy, <http://ft40.iaea.org/worldatom/Periodicals/Factsheets/English/safeguards.html>.


Robert Mozley, “Verifying the Number of Warheads on Multiple-warhead Missiles,” p. 120 ff.

An outstanding analysis of the psychology and politics of treaty verification can be found in Nancy Gallagher, The Politics of Verification (Baltimore: John Hopkins University Press, 1999).


See, for example, Thomas, “Verification of Limits on Long-Range Nuclear SLCMs,” pp. 29-39; Greenpeace, TL: a Nuclear Weapons Materials Production Cutoff.


Even the U.S. Food and Drug Administration (FDA) “standards” for the tamper-evident packaging legally required for U.S. over-the-counter drugs are skimpy and vague. Yet this is an area where one would expect there to be enormous care and effort, and well developed standards. See, for example: Title 21 of the Code of Federal Regulations, Sec 211.132 covering tamper-evident packaging requirements for over-the-counter (OTC) drugs and also FDA, May 21, 1992, Tamper-Resistant Packaging Requirements for Certain Over-the-Counter (OTC) Human Drug Products, FDA Compliance Guides, Chapter 32A, Drug Alteration Guide 7132A.17.

A vulnerability assessment involves finding and demonstrating weaknesses (vulnerabilities) in a tag, seal, or tamper detection program, perhaps accompanied by suggested countermeasures. A definition of an “effective” vulnerability assessment can be found in Johnston, “Effective Vulnerability Assessment of Tamper-Indicating Seals,” pp. 451-455.

Seal “use protocols” (or simply “protocols”) are the official and unofficial procedures used for seal procurement, storage, accounting, installation, inspection, removal, disposal, reporting, interpreting, and training. A seal is no better than the protocols for using it.

Johnston, “Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management.”


Seals play a role in nuclear accounting, not just control/containment. See, for example, Daniel Pollack, “Security Issues in the Handling and Disposition of Fission-physical security, but not in the MC&A section: Herbert L. Abrams and


48  There tends to be enormous concern on the Russian side about the possibility of audio listening devices being covertly embedded inside monitoring hardware.

49  Richard Feynman gives an entertaining (but unhappily all too common) account of the pitfalls of exposing security vulnerabilities in Edward Hutchings, Ralph Leighton, Richard Phillips Feynman, and Albert Hibbs, Surely You are Joking, Mr. Feynman: Adventures of a Curious Character (New York: Bantam, 1985), pp. 119-137.


51  An excellent discussion of how redundancy often makes things worse, not better, can be found in Scott D. Sagan, The Problem with Redundancy Problem: Or Why Organizations Try Harder and Fail More Often, unpublished manuscript, Center for International Security and Cooperation, Stanford University, 2000.

52  Johnston and Garcia, Simple, Low-Cost Ways to Dramatically Improve the Security of Tags and Seals, pp. 1-9; Johnston, “Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management.”


54  It is not surprising that there should be confusion about tamper detection for verification purposes when transparency and treaty monitoring themselves are so poorly understood. See, for example, Ronald B. Mitchell, “Sources of Transparency: Information Systems in International Regimes,” International Studies Quarterly 42 (March 1998), pp. 109-130.

55  Thus historically, many IAEA seals and their use protocols were simply copied from those used for U.S. domestic security and safeguards. This occurs despite the fact that the IAEA “safeguards program” (actually treaty monitoring) differs substantially fromU.S. nuclear “safeguards” (MC&A). In some cases, however, the IAEA has implemented significant improvements or modifications, such as the double e-cup vs. the single e-cup. Ivan C. Oelrich, “Production Monitoring for Arms Control,” in Michael Krepon and Mary Umberger, eds., Verification and Compliance: a Problem-Solving Approach (Cambridge, MA: Ballinger, 1988), p. 116.

56  There are also problems with sharing classified information from a seals’ database with foreigners.

57  Johnston, “Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management.”


60  Thus historically, many IAEA seals and their use protocols were simply copied from those used for U.S. domestic security and safeguards. This occurs despite the fact that the IAEA “safeguards program” (actually treaty monitoring) differs substantially from U.S. nuclear “safeguards” (MC&A). In some cases, however, the IAEA has implemented significant improvements or modifications, such as the double e-cup vs. the single e-cup.


This may be partially due to the IAEA’s unwillingness to admit that vulnerabilities exist.


Frances Mautner-Markhof, “The IAEA Experience,” in Richard Kokosi...


93 For an excellent discussion of the meaning of verification, including its intrinsic nature as “an interpretive activity” (p. 39), see Seong W. Cheon and Niall M. Fraser, “Arms Control Verification: An Introduction and Literature Survey,” *Arms Control* 9 (May 1988), pp. 38-58.


95 Hopefully such a review would result in a new classification category. This is certainly needed for classified transport information. For legitimate security reasons, the United States considers information about the movement of nuclear weapons to be secret. Under future dismantlement regimes, Russian or third-party inspectors may need advance notice about the movement of treaty-limited items and might even accompany them in transit. This creates the somewhat bizarre situation (which has already occurred) where adversarial foreigners are given classified information that the U.S. government keeps from its own citizens. A new classification scheme would similarly be useful for confidential/secret deliberations and agreements undertaken via bilateral commissions such as the Standing Consultative Commission (SCC) created by the U.S. and Soviet Union in 1972 to deal with a variety of treaty issues. See Gloria Duffy, “Arms Control Treaty Compliance,” in Mary E. Lord, ed., *Encyclopedia of Arms Control and Disarmament* (New York: Scribner’s Sons, 1993), pp. 289-292. Ideally, any new scheme to classify such information would avoid the problems of information categories such as “UCNI” (DOD/DOE), “Official Use Only” (DOE), or “Safeguards Confidential” (IAEA). In practice, these categories are often arbitrary, inconsistent, and ambiguous.