IMPROVING TAMPER DETECTION FOR HAZARDOUS WASTE SECURITY

R.G. Johnston, A.R.E. Garcia, A.N. Pacheco, S.J. Trujillo,
R.K. Martinez, D.D. Martinez, and L.N. Lopez
Vulnerability Assessment Team
Los Alamos National Laboratory
MS J565, Los Alamos, NM 87545

ABSTRACT

Since September 11, waste managers are increasingly expected to provide effective security for their hazardous wastes. Tamper-indicating seals can help. This paper discusses seals, and offers recommendations for how to choose and use them.

INTRODUCTION

After September 11, waste managers are increasingly expected to provide improved levels of security for the hazardous materials in their charge. Many low-level wastes that previously had minimal or no security must now be well protected, while high-level wastes require even greater levels of security than previously employed. This demand for improved security comes, in many cases, without waste managers being provided the necessary additional funding, personnel, or security expertise.

Contributing to the problem is the fact that—at least in our experience—waste managers often fail to appreciate certain types of security vulnerabilities. They frequently overlook or underestimate the security risks associated with disgruntled or compromised insiders, or the potential legal and political liabilities associated with nonexistent or ineffective security. Also frequently overlooked are potential threats from waste management critics who could resort to sabotage, vandalism, or civil disobedience for purposes of discrediting a waste management program.

Tamper-indicating devices, often called "seals", can be useful tools for improving the security of waste management, including the security of hazardous materials in storage, waste undergoing transport, instruments for waste characterization, and data on wastes [1]. Seals provide a low-cost, relatively non-invasive, and (deceptively) simple way to detect unauthorized access or tampering. Tampering or unauthorized access can be for such nefarious purposes as theft, diversion, espionage, sabotage, vandalism, or illegally hiding high-level waste inside containers previously certified to hold only low-level waste. Seals can also be useful for quality control or accountancy purposes in detecting inadvertent, erroneous access or redundant handling/processing by authorized personnel with no malicious intent.

The problem facing waste managers who wish to employ seals is that seals appear on the surface to be quite trivial to use. Manufacturers and vendors of tamper-indicating seals naturally encourage this view. In reality, however, seals require at least a somewhat sophisticated user in order to be effective. All seals are relatively easy to spoof, even by unsophisticated adversaries, unless the seal user has a good understanding of how to choose a seal, what limitations it has, and exactly how to install and inspect it in order to obtain optimum security given the existing constraints [2-4]. An understanding of the most likely attack scenarios is also critical [5]. Since most waste managers are not security experts, and because even many security experts are not knowledgeable about seals, effective tamper detection is not guaranteed.

We in the Vulnerability Assessment Team at Los Alamos National Laboratory have extensively studied seals and how to use them [2]. We have conducted detailed vulnerability assessments on over 200 different tamper-indicating seals. These range from low-cost seals through expensive high-tech seals, and include both government and commercial devices. As a result of our vulnerability assessments, as well as our interactions over the last few years with commercial and government seal users around the world who have various real-world applications for seals, we have developed some general guidelines, suggestions, and recommendations for seal users. These may be of use to waste managers who are currently using tamper-indicating seals, or who may wish to consider the use of seals.

SEALS, LOCKS, TAGS, & INTRUSION DETECTORS

A **lock** is a device intended to delay or complicate unauthorized access or entry. Locks do not stop adversaries who are adequately motivated and/or knowledgeable. Unlike locks, tamper-indicating devices ("**seals**") typically provide little resistance to unauthorized entry— they simply record that it took place [6]. Indeed, some seals are made of paper or plastic and can be easily torn off. This does not necessarily make them ineffective as tamper-indicating devices. Perhaps the most familiar examples of seals is the tamper-evident packaging used for consumer products such as food and over-the-counter pharmaceuticals.

Seals and locks differ in that seals must be inspected manually or electronically to determine if unauthorized access has occurred. Locks, in contrast, perform their function even when ignored. Locks are also typically meant to be re-used. Most seals, however, are designed for one-time use, though there are re-usable electronic and electrooptic seals.

A **tag** is an intrinsic or applied unique characteristic ("fingerprint") used to unambiguously identify an object or container. The license plate on a car is an example of a tag. There are, however, different kinds of tags. A "security tag" is intended to be both difficult to counterfeit, and difficult to "lift", that is, remove from one object and place on another. An "anticounterfeiting tag", often used to deter product piracy, is designed to be difficult to counterfeit, but not necessarily to lift. An "identity tag" is used to mark an object or container when there is no malicious adversary interested in either counterfeiting or lifting. A "buddy tag" is a type of token that demonstrates that the bearer possesses the object or container the buddy tag represents, without actually having to produce that object or container. A buddy tag should be difficult to counterfeit, but lifting is not an issue. Unlike other types of tags, a buddy tag is not necessarily located on or near the object or container it is paired with.

Intrusion detectors ("burglar alarms") differ from seals in that they report unauthorized access in real-time (immediately), instead of after the fact. There are advantages and disadvantages to this. Usually the application of interest determines whether seals or intrusion detectors make the most sense, though often they are used together. Intrusion detectors are typically useful for guarding a room or building, and quickly summoning security personnel to respond to any intruders. Intrusion detectors tend, however, to be complicated, expensive, and impractical to place on large numbers of waste containers, especially if the containers are frequently moved or transported.

The boundaries between the various security devices (locks, seals, tags, and intrusion detectors) are not always clear. There is, for example, a type of security device called a "**barrier seal**" that operates as both a lock and a seal [6]. Such a hybrid device, however, tends to be a compromise—neither the optimum seal nor the optimum lock for a given application [5]. Barrier seals also tend to confuse users about what the device is intended to accomplish [6]. There is sometimes also confusion because seals and security tags can be used somewhat interchangeably [1]. Indeed, a security tag needs—like a seal—to have tamper-indicating capabilities in order to detect when it has been lifted. A seal, on the other hand, needs—like a security tag—to have a unique identifier, such as a serial number, so that the seal cannot be removed and trivially replaced with another identical seal. The difference between a seal and intrusion detector can also become blurred when the intrusion detector responds periodically (rather than instantly), or is periodically polled for its alarm status.

WHY USE SEALS?

There are many different reasons why tamper-indicating seals might be used as part of a waste management program. Indeed, any given waste management application might employ seals for more than one of these reasons simultaneously. Some of the reasons to use seals include:

(1) to detect unauthorized access, tampering, or theft of hazardous materials;
(2) to increase the amount of time it takes an adversary to engage in surreptitious unauthorized access, tampering, or theft without being detected;
(3) to psychologically deter unauthorized access, tampering, or theft of hazardous materials;
(4) to emphasize to employees the seriousness of waste hazards;
(5) to detect the unscrupulous introduction of high-level waste inside containers previously certified to hold only low-level waste;
(6) as a check on the effectiveness of physical security, material control, and accountability measures;
(7) to protect against tampering with the performance, settings, or calibration of waste characterization instruments;
(8) to protect against inadvertent erroneous changes to the performance, settings, or calibration of waste characterization instruments;
(9) to protect the integrity of data and paperwork;
(10) for quality control, or to increase the formality of operations;
(11) for accountability purposes;
(12) as legal evidence of trespassing, breaking & entering, or vandalism;
(13) to reduce legal liability by exhibiting standard, good, or best practices;
(14) to demonstrate good faith to the public;
(15) as identity tags to mark waste containers and/or their current status;
(16) to prevent inadvertent erroneous mishandling, redundant handling, or unnecessary opening of waste containers.

Uses 1-3, 5-7, 9, 12, and 13 above are meant to counter malicious adversaries. Malicious adversaries are not primarily of concern for 4, 8, 10, 11, and 14-16.

WHY USE A SEAL INSTEAD OF A LOCK?

Seals have a number of positive attributes and advantages compared to locks for many applications. Some of the reasons that waste managers might want to use a seal instead of a lock include:

- All locks can be defeated, even by determined amateurs, and usually quickly—no matter how well the lock is used.

- Locks require complicated and expensive key-control or combination-control procedures. The keys or combinations can represent additional vulnerabilities.

- After locking up a truck, railcar, transportainer, or cargo, the key or combination must usually be present at the receiving location, or sent there (ideally via a different route).

- Seals are often easier and faster to remove than locks, including in emergencies and by customs officials.

- Seals are usually cheaper than locks.

- Seals are usually lighter and smaller than locks, something particularly important for cargo shipments and courier packages.

- It is often more useful and practical to know that tampering has occurred than to try to stop it. (The classic example of this is product tampering with over-the-counter pharmaceuticals.)

- Most locks are not very effective at recording tampering.

- Whereas a robust lock may encourage an adversary (who doesn't care about the intrusion being detected after the fact) to damage the container, vehicle, transportainer, or railcar to gain entry, a seal may encourage the adversary to enter non-destructively through the door or lid, causing no damage except to the seal.

- There may be additional security, safety, and environmental reasons why we would prefer the adversary to enter through a given portal, rather than from any random direction.

- Seals can encourage security personnel to carefully inspect the container, its contents, and surrounding area, with a potential improvement in overall security and safety.

- Locks aren't generally covert, whereas seals can be. (A covert seal is called a "**trap**".)

- Many seals are more corrosion resistant than locks, and may perform better under extreme environmental conditions.

- Locks usually require a hasp and provide only portal security. While this is also the case for many traditional seals, some seals, including newer designs, do not require a hasp and can provide volumetric security.

WHY USE A SEAL INSTEAD OF AN INTRUSION DETECTOR?

Some of the reasons that waste managers might want to use a seal instead of an intrusion detector include:

- Seals, unlike intrusion detectors, do not require a real-time response when unauthorized access or entry occurs.

- Seals are usually much less susceptible to false alarms—typically a very serious problem with intrusion detectors.

- Seals are usually much cheaper, smaller, easier, and faster to install.

- Intrusion detectors require a source of electrical power. Most seals do not.

- Intrusion detectors usually do not work well outdoors or under extreme environmental conditions. This is not the case for many seals.

- Intrusion detectors require some kind of continuous (or frequent) one-way or two-way communication. This greatly complicates things, adds to the cost, and creates reliability problems, especially for cargo, containers, or vehicles traveling great distances.

- Simultaneously monitoring (in real-time) large numbers of moving containers, vehicles, railcars, or transportainers for intrusion can be extremely impractical.

- Seals are easy to use on an *ad hoc* basis, and (unlike intrusion detectors) can usually be added for extra security without impeding existing security layers.

TYPES OF SEALS

There are over 5,000 different kinds of commercially available seals. Some are shown in figure 1.

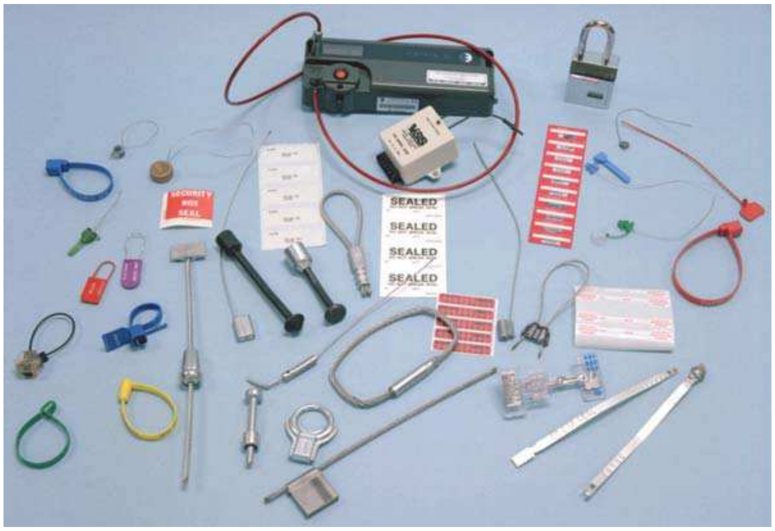

Figure 1 - Just a few of the 5,000+ commercially available seals.

Most seals can be categorized as passive or active (also called "dynamic"). Active seals use electronics or electrooptics. The first eight seal types discussed below are passive. The last two are active.

wire loop seal: This seal consists of one wire twisted around one or more wires. The wire bundle is then passed through the hasp of a container or door to be secured. A metal or plastic head or housing then crimps, traps, or irreversibly captures the ends of the wire bundle. See figure 2. The lead-wire seal (second from left in figure 2) is the classic example of this type of seal. A blob of soft lead is used to crimp the ends of the wire bundle. Lead-wire seals, however, have fallen out of favor because of the poor security they offer and because of the health and environmental problems presented by lead.

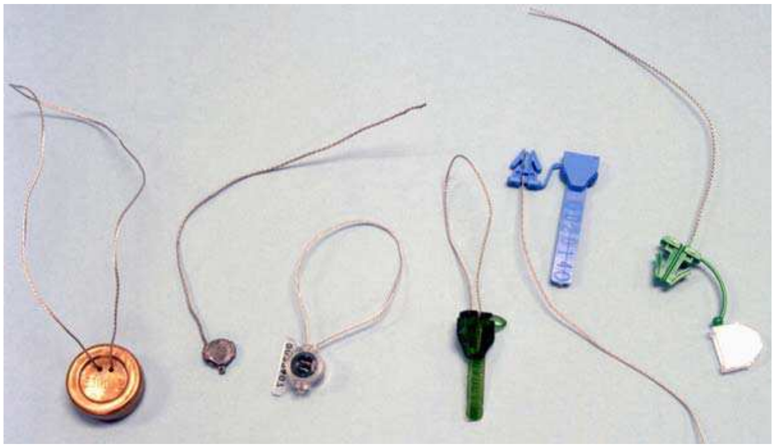

Figure 2 - Examples of wire loop seals

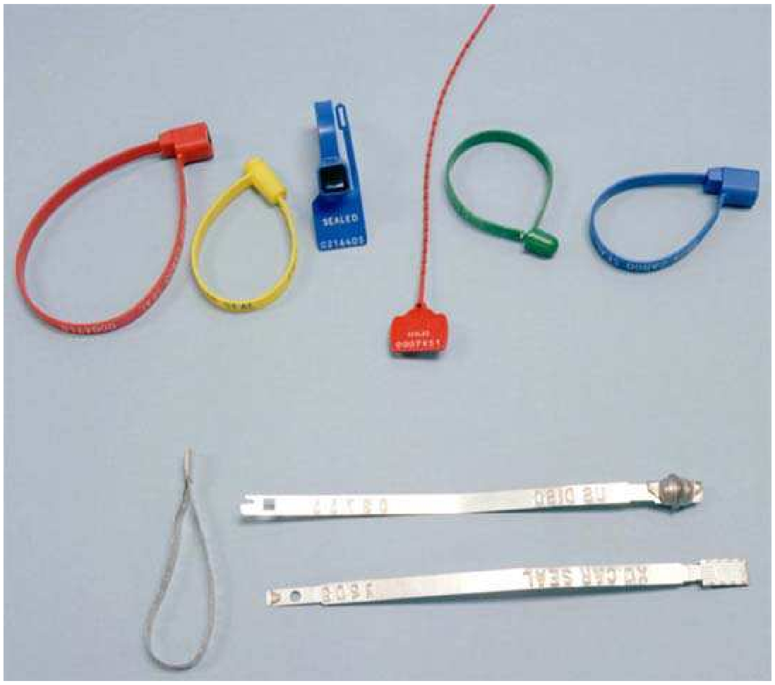

Figure 3 - Some plastic strap seals (top) and metal ribbon seals (bottom).

metal cable seal: A larger and sturdier version of the wire loop seal. Aircraft cable is used, with each end crimped or irreversibly clamped into a head or housing. Because of its great resistance to force, this is a barrier seal—part lock and part seal.

plastic strap or ribbon seal: A one-piece plastic molded strap with one end that snaps irreversibly into a head or housing on the other end, after the plastic strap is passed through the hasp of a container or door. Examples of these inexpensive seals are shown in figure 3. This type of seal has the advantage that it is less likely to injure personnel who come in contact with sealed moving containers, and less likely to puncture waste containers, than is the case with metal seals.

metal ribbon (car-box or car-ball) seal: A seal made from sheet metal. See figure 3. One end of the ribbon snaps irreversibly into a head on the other end. Popular for use on railcars. Though robust, this is not a barrier seal.

bolt seal: A barrier seal consisting of a strong bolt with one end larger than the hasp and the other end designed to snap irreversibly into a cylindrical head or housing called the "locking head" or "locking body". These barrier seals are popular for use on trucks and transportainers. Bolt seals can usually withstand substantial force without opening.

padlock seal: A "self-locking" metal or plastic seal that looks like a padlock. Intended for one-time use. Despite the name, these are seals, not locks. They are often used on residential and commercial utility meters. A seal of this sort is shown installed on a 55-gallon drum in figure 4. The plastic "padlock" seal in the figure will be damaged if the bolt is removed. Better tamper detection is possible if the bolt, the lid closure band, the lid, and the container body are each carefully inspected, not just the seal. This is necessary for the most reliable tamper detection because the container can be opened without disturbing the seal.

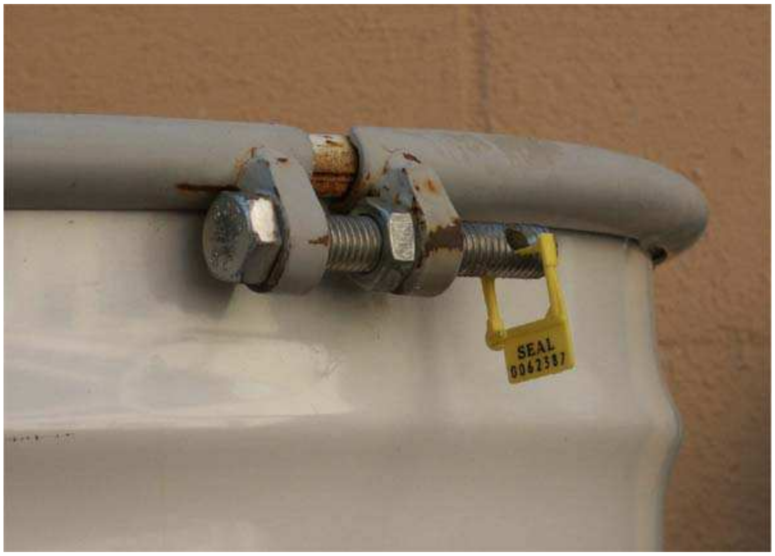

Figure 4 - An example of using a seal on a 55-gallon drum for low-security applications.

adhesive label seal (adhesive tape seal or pressure-sensitive adhesive seal): These seals are sticky labels that become damaged if removed from what they are stuck to. Examples are shown in figure 1. They are often used as tags. These types of seals are inexpensive and easy to use, but do not typically provide high levels of security, nor are they very robust.

(passive) fiber optic seal: The cable is an optical fiber or bundle of optical fibers. Cutting the optical fibers changes their light transmission or other properties.

(active) fiber optic seal: In an active fiber optic seal, light pulses are sent down the optical fibers continuously, a number of times per second. If the optical fibers are cut, the light pulses fail to complete the loop and this is detected by the electrooptics. This type of seal is typically reusable.

(active) electronic seal: Seals of this sort are usually battery powered and check continuously for signs of tampering. This type of seal is most often reusable.

SEAL VULNERABILITIES

We have studied in detail over 200 different tamper-indicating seals [2,7,8]. These include government and commercial seals, passive and active seals, and seals ranging from low-cost, low-tech seals, through expensive high-tech seals. At least 56% of these seals are in use for high-security applications, and more than 16% are currently in use for nuclear applications somewhere in the world.

As a result of this work, we have demonstrated how all of these seals can be defeated quickly, using low-tech methods, tools, and supplies available to almost anyone [2-4]. To "defeat" a seal means to open the seal, then to reseal the container using either the original seal or a counterfeit, without being detected. Simply removing a seal does not defeat it, since its absence, or the damage it sustains, will indicate that tampering has occurred. (To "attack" a seal means to undertake a sequence of actions intended to defeat it.)

We conclude from this work that current seals, and especially current use protocols are not satisfactory. By "seal use protocols", we mean the official and unofficial procedures for seal procurement, transport, storage, checkout, installation, inspection, removal, disposal, interpretation, and training of personnel. A seal is really no better than the protocols for using it.

Fortunately, it appears that relatively minor changes to how seals are typically used—even without improvements to the seals themselves—can dramatically improve the effectiveness of tamper detection [1,2,5]. In the next two sections, we offer some suggestions for effective seal use.

RECOMMENDATIONS FOR CHOOSING A SEAL

We offer the following recommendations for how to choose a seal based on our experiences with tamper detection, seal vulnerability assessments, and the review of various security and waste management programs:

1. Bear in mind that the unit cost of a seal is often the least important economic factor. Costs associated with installation, inspection, associated hardware, and training are often much larger. (Not to mention the potential costs of undetected tampering!)

2. Tamper detection effectiveness is not well correlated with seal cost, or the degree of high technology employed by the seal [2]. An inexpensive, modest seal can provide good tamper detection if used effectively, but a sophisticated seal that is used poorly will not.

3. It is important to keep in mind that simple physical attacks on high-tech seals are often highly effective because of the ease with which they can be accomplished, and because users and developers of high-technology systems often focus on the wrong issues. Indeed, high-tech seals are often easier to defeat than low-tech seals [2].

4. In choosing a seal, it is very important to carefully consider the container, lid, door, and/or hasp that the seal will be used on. Many waste containers, such as 55-gallon drums, are not particularly well designed for use with seals, or for tamper detection in general. (See figure 4.)

5. Using a high-tech reader to check a seal often increases seal vulnerabilities unless the use protocols and training for the seal inspectors and installers include significant manual and visual inspection procedures, and counter-measures for the known seal vulnerabilities.

6. A seal design and its use protocols will usually be most vulnerable near the end of the life of the product.

7. There is no one "best" seal (anymore than there is a best car or a best baseball player). The best seal for your application depends critically on details of your application, security goals, containers, likely adversaries, budget, resource limitations, security personnel, seal use protocols, and training program.

8. Vendors, developers, and manufacturers of seals often emphasize how difficult it is to counterfeit their products. Potential users should be wary of this; the degree of difficulty is often exaggerated. In addition, counterfeiting is usually one of the least likely attack scenarios for most seals. Other methods of defeating seals are often easier [2,8].

9. There is no such thing as an undefeatable seal, and probably never will be. (The same thing is true of any other kind of security device, system, or program.) The phrases "tamper proof" seal or "tamper resistant" seal, used by some seal manufacturers and vendors should be rejected. These phrases are meaningless, and misleading [1,2,7].)

10. A seal that is complex and difficult to use, that has significant ergonomic problems, and/or that is resisted by seal installers and inspectors will usually not provide good tamper detection.

11. Factors in addition to security and economics deserve particular attention in choosing a seal for waste management applications. These include ease of use, robustness, durability, and safety. Ease of use may be critical if the seals must be installed, inspected, and removed under inclement weather conditions or poor lighting, or while wearing chemical protective gear or gloves. Robustness may be an important factor for seals used on waste containers that can potentially receive rough handling. Environmental durability can be very important if the seals are to be used, for example, on waste drums stored outdoors. (Many commercial plastic seals are doped with compounds to protect them from ultraviolet damage caused by sunlight.) Certain metal seals may not be good choices for use in a salt-air environment (such as near the ocean) because of the potential for corrosion. Extreme temperature ranges may also eliminate the use of certain seals. Safety can be an important issue as

well, particularly for wire-loop, metal cable, and metal ribbon seals. If they are attached to waste containers such as 55-gallon drums that are moved frequently, there is the possibility of catching fingers in the loops, or gouging the skin, eyes, or protective clothing of waste workers.

12. (Ideally the same) serial number should appear on every independent part of a seal. If serial numbers are stamped or embossed on a seal by the manufacturer, they should be done deeply enough that they can't be easily buffed off. Ideally, serial numbers are made from punch-through stencils, or are embedded inside a transparent body.

13. The physical and record-keeping security of the seal factory and seal vendor, and the reliability of their personnel are very serious vulnerability issues. The security of the seals as they are shipped between the vendor/manufacturer and the user is also critical. It is relatively easy for an adversary to install a "backdoor" in an unused seal that can make it easier for him or her to defeat the seal once it is installed.

14. Reliable tamper detection is hard work. No seal can negate that unavoidable fact.

15. The way a seal is used is more important than which seal is chosen.

RECOMMENDATIONS FOR USING A SEAL

1. Many seal users are remarkably vague on what they are trying to accomplish. It is essential to fully understand the goals of the tamper detection program, the resources available (time, money, personnel), the required functions of the seals, what is being protected and why, the consequences of a security failure, the nature of potential adversaries and the resources they have at their disposal, and the training program for seal installers and inspectors. Security and reliability cannot be optimized without a clear understanding of these issues. These matters should be revisited on a regular basis.

2. Seal installers and inspectors should be familiar with the most likely attack scenarios for the specific seal they are using, and explicitly look or test for them. They should have hands-on practice and training detecting seals that have been attacked subtlely and crudely. Merely giving seal inspectors vague instructions to, for example, "look for signs of tampering" are not sufficient. Inspectors should be shown examples of defeated seals so they know exactly what to look for. This suggestion is somewhat controversial in that many security managers are reluctant to disseminate vulnerability information to relatively low-level security personnel. In most security programs, however, disloyal security personnel can compromise security with ease, even if they lack specific vulnerability information.

3. Seals that are inspected visually should be examined with an identical, unused seal held right alongside [5]. People do not accurately remember details of exact color, size, surface texture, gloss, and patterns, but they are much more proficient at visual side-by-side comparisons. Counterfeits and cosmetic repairs of the seal can be more reliably spotted in this way.

4. Seal personnel (and other security personnel) should be encouraged to observe, pay attention, think on the job, and report concerns. To the extent practical, they should be emotionally and intellectually engaged in "catching the bad guys". Seal personnel should fully understand the reasoning behind the seal installation and inspection processes; they should not be mindlessly following an overly formal seal use protocol that is not well motivated. For the best security, personnel should be trained in

observational skills, and educated about the dangers of social engineering, misdirection, and sleight of hand techniques.

5. Seal installers and inspectors should be rewarded, not punished, for finding potential problems, raising important issues, and thinking on the job. In many security programs, low-level personnel are afraid to raise concerns about suspicious seals or questionable procedures because of the consternation this causes their supervisor [5].

6. Seal (and container) data must be well protected because one of the easiest ways to defeat a seal is to tamper with its paperwork or data [8]. Information about a seal, such as its serial number, must not be stored in or on the container or vehicle being protected, unless the information is appropriately encrypted. The driver of a sealed truck should not possess the working copy of paperwork containing the seal serial number. Seal data that is communicated, shipped, or carried to another location must be secure.

7. Seal readers, i.e., hand-held devices designed to check a seal, must be tested occasionally in a random, unpredictable manner to verify that they will reject a seal if it has been tampered with, or if it has the wrong serial number. This is to prevent attacks where the adversary tampers with the reader so that it reports everything is fine all the time, even if it isn't.

8. There should be periodic, effective vulnerability assessments of both the seals being used and the overall security or verification program.

9. Most seal users are careful about protecting the devices prior to use. Seals, however, must also be thoroughly protected or destroyed after use. Discarded seals, even if partially destroyed, provide potential adversaries with a useful source of information, practice samples, and counterfeit parts.

10. If practical, used seals should be (securely) archived for possible future analysis as new attacks are uncovered, or issues of past vulnerability arise. If it is impractical to archive all seals, consider saving a random subset of used seals.

11. Because postmortem exams on seals are expensive and time-consuming, many seal users who perform postmortem forensics do so only on suspicious seals. It is, however, important to perform postmortems on some percentage of randomly chosen seals that are not suspicious. It is also important not to become overly confident that, simply because the tamper detection program *can* perform a postmortem exam on a seal, that it *will*. Do not become over-confident with the security provided by potential postmortems.

12. If postmortem exams are performed on a subset of removed seals, it is important to return more seals to headquarters or the laboratory than you will actually analyze. This increases the concern of an adversary that he may be caught if he/she attempts tampering.

13. The seal manufacturer or vendor should accept seal orders from only a small number of authorized personnel within the seal user's organization. These people must provide the manufacturer or vendor with the proper password, or the order should not be filled.

14. Assurances from seal manufacturers that they will protect seal logos or certain serial numbers from unauthorized users are not always reliable. This should be covertly tested by the seal user.

15. Pressure sensitive adhesive label seals, although cheap and easy to use, do not provide high levels of security, nor are they very robust. They also are difficult to use on containers that are dirty, corroded, cold, wet, or that are exposed to large thermal fluctuations. If pressure sensitive adhesive labels seals are used, they should be protected for the first 48 hours after application, because of incomplete adhesion. (Heat can help speed up the process.)

Users should clean the surface prior to application, and watch for surfaces that may have been pre-oiled or pre-coated by an adversary to reduce adhesion. Watch also for porous surfaces that can leach oils or solvents.

The adhesive, printing ink, and label substrate should be soluble in exactly the same solvents. The adhesive should melt at a higher temperature than the printing inks and substrate.

Inspectors should examine not just the label, but also the general area around the label, looking for solvent stains or other evidence of surface modification. They should also pay particular attention to areas on the label that have not adhered to the surface, such as over slots, grooves, or screw holes.

Labels should be compared side-by-side with an unused label. The feel of the adhesive label seal when it is removed is essential for detecting tampering—though inspectors must have experience to know how the seal should feel when it is lifted from the particular surfaces of interest. The smell of the pressure sensitive adhesive label seal when it is removed can also be useful for detecting trace amounts of solvents, oils, epoxies, paints, or adhesives that might have been used to attack the seal or cover-up an attack, but the inspector again needs enough practice to be able to spot anomalies.

16. Loop-type seals that are adjustable should be cinched as tightly against the container hasp as practical. Any excess length of wire or plastic strap should be removed. Both of these suggestions often contradict the instructions given by seal manufacturers. They also complicate the tasks of inspecting and removing the seal. Tight cinching and removing of excess wire or strap, however, complicates seal attacks and increases the odds of detecting them. It also improves safety.

17. Seal installers and inspectors must carefully check the container that is being sealed, as well as its door/lid, hasp, and closing mechanism. They need to be sure they are not putting a seal on a compromised container, and they need to look for attacks on the container that bypass the seal.

18. Employees, former employees, security personnel, or community members who are disgruntled can severely compromise security. A waste management program that wishes to optimize security should strive to treat people well and fairly—and be widely perceived as doing so. A legitimate, fair, and effective complaint resolution process should also be in place to deal with employee concerns and grievances, and employees should widely view it as being legitimate, fair, and effective.

CONCLUDING REMARKS

Seals can be of considerable value for improving the security of waste management applications. It is important, however, that they be chosen appropriately and used in a manner that optimizes their effectiveness. Seals are only as good as the security program and the personnel who use them. Seals that are used mindlessly or without paying close attention, or that are slapped in place and then forgotten, will not provide effective security. Indeed, they may be less than worthless if they create a naive over-confidence in the mind of the user.

We have offered here some generic recommendations for waste managers interested in tamper detection. The most useful suggestions, however, depend critically on details of the application, security goals, likely adversaries, facilities, personnel, containers, and the time and money budget. Waste managers interested in introducing seals into their waste management program, or wishing to improve their existing tamper detection methods, are encouraged to contact us to discuss their specific situation.

ACKNOWLEDGMENTS & DISCLAIMERS

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. The seals shown in the figures were chosen at random as samples; there is no significance to which commercial products appear in the figures and which do not. We benefited from the assistance of Eric Baca and Anna Nogar.

REFERENCES

1. R.G. JOHNSTON, "Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management," Science & Global Security 9, 105 (2002), http://lib-www.lanl.gov/la-pubs/00818333.pdf

2. R.G. JOHNSTON, A.R.E. GARCIA , and A.N. PACHECO, "Efficacy of Tamper-Indicating Devices", Journal of Homeland Security, April 2002, http://www.homelandsecurity.org/journal/Articles/displayarticle.asp?article=50

3. R.G. JOHNSTON and A.R.E. GARCIA, "Vulnerability Assessment of Security Seals", Journal of Security Administration 20, 15 (1997), http://lib-www.lanl.gov/la-pubs/00418796.pdf

4. R.G. JOHNSTON, A.R.E. GARCIA, and W.K. GRACE, "Vulnerability Assessment of Passive Tamper-Indicating Seals", Journal of Nuclear Materials Management 224, 24 (1995).

5. R.G. JOHNSTON, "The Real Deal on Seals," Security Management, 41, 93 (1997), http://lib-www.lanl.gov/la-pubs/00418795.pdf

6. L. TYSKA (Editor), *Guidelines for Cargo Security & Loss Control* (Annapolis, MD: National Cargo Security Council, 1999), pp. 29-38.

7. R.G. JOHNSTON, "Effective Vulnerability Assessment of Tamper-Indicating Seals", Journal of Testing and Evaluation 25, 451 (1997), http://lib-www.lanl.gov/la-pubs/00418792.pdf

8. R.G. JOHNSTON and A.R.E. GARCIA, "An Annotated Taxonomy of Tag and Seal Vulnerabilities," Journal of Nuclear Materials Management 28, 23 (2000).