

How to be a Better Seal User

Roger G. Johnston, Ph.D., CPP
Vulnerability Assessment Team
Los Alamos National Laboratory
Los Alamos, NM 87545 USA
rogerj@lanl.gov

Introduction

Tamper-indicating seals have been used for over 7,000 years. Today, seals are widely used to help counter cargo theft, smuggling, sabotage, vandalism, tampering, terrorism, and espionage. Despite their antiquity and modern widespread use, however, there remains considerable confusion about seals, as well as a lot of misconceptions, wishful thinking, sloppy terminology, and poor practice.

The Vulnerability Assessment Team (VAT) at Los Alamos National Laboratory has intensively studied tamper-indicating seals for the last 12 years. We have provided consulting, vulnerability assessments, and security solutions for over two dozen government agencies and private companies. This article summarizes some of our recommendations for using seals more effectively and with greater sophistication.

Terminology

A **seal** is a tamper-indicating device (TID) designed to leave non-erasable, unambiguous evidence of unauthorized access or entry. Unlike locks, seals are not necessarily meant to resist access, just record that it took place. Seals must be inspected before there can be a determination of whether tampering has taken place. Devices that detect intrusion in real-time (instead of after-the-fact, like seals) are called **intrusion detectors** (or “burglar alarms”).

Other useful terminology:

passive seal: a seal that does not rely on batteries or electrical power to monitor for tampering.

active seal = electronic seal: an electronic or electrooptic seal that uses batteries or electrical power to monitor for tampering. Active seals are usually more expensive than passive seals, but are often reusable.

transponder seal: a seal that is passive while watching for tampering, but that is briefly powered up by (or for) the seal reader to check if tampering has occurred. Examples include seals that incorporate passive radio frequency (rf) transponders, or contact memory buttons.

seal reader = seal verifier: a device (usually electronic or optical) that checks a passive or active seal for evidence of tampering.

barrier seal: a single, hybrid security device that is both a lock and a seal. Barrier seals make sense for certain applications, but for many applications, it is better to use a good lock in conjunction with a good seal if both functions are truly necessary. This is because a barrier seal is usually a compromise, neither the optimum seal nor the optimum lock for a given application. Moreover, barrier seals tend to confuse users with their multiple purposes.

trap: a covert seal.

inspecting a seal: checking the seal for evidence of tampering.

postmortem exam: returning a used seal from the field and examining it further for evidence of tampering, using low-tech and/or high-tech methods and forensics. Postmortem exams are expensive and time-consuming, but can greatly increase the odds of detecting tampering.

seal (use) protocols: the official and unofficial procedures used for seal manufacture, procurement, shipping, storage, accounting, installation, inspection, removal, postmortem exams (if any), disposal, reporting, interpreting, and training. A seal is no better than the protocols for using it.

defeating a seal: opening a seal, then resealing (using the original seal or a counterfeit) without being detected. Simply yanking a seal off a container does not defeat it, since the fact that the seal is damaged or missing will be noted.

attacking a seal: undertaking a sequence of actions designed to defeat it.

backdoor attack: an attack where an adversary modifies the seal prior to use to make it easier to enter surreptitiously at a later time.

Terminology to Avoid

The following terminology should be avoided because it is misleading, confusing, and demonstrates a lack of understanding of tamper detection fundamentals:

“tamper-proof” seal: This term is ludicrous. The last thing we want is a seal that can’t be tampered with; what we need are seals that are easy to tamper with, but also easy for the seal user to tell they have been tampered with. Moreover, the term implies invincibility. The truth is that there are no security devices that are impossible to defeat, and even if there were, absolute invincibility is unprovable. “Tamper-indicating seal” is the preferred term.

“tamper-resistant” seal: This terminology is similarly misleading because seals are not meant to resist tampering; that is what locks do. Seals are instead meant to record that tampering has occurred.

security seal vs. tamper-indicating seal: There is (unfortunately) a distinction often made between barrier seals, which are said to provide security, and tamper-indicating seals, which supposedly do not. Such reasoning, however, is confused. Tamper detection is a legitimate

security function. Thus, all seals provide security—even if made only of flimsy paper or plastic, and all seals are tamper-indicating.

antipilferage seal: while tamper-indicating seals can help detect pilferage they don't prevent or resist it, except perhaps in some vague psychological sense.

Why Use a Seal Instead of a Lock?

There are a number of reasons why using a seal for a given application may make more sense than using a lock:

1. All locks can be defeated, even by determined amateurs, usually quickly.
2. Locks often require complicated and expensive key-control or combination-control procedures. Usually, the key or combination must be present at, or sent to, the receiving location. This presents additional vulnerabilities.
3. Seals (especially passive seals) are often cheaper than locks.
4. Seals are typically easier and faster to remove than locks, including in emergencies.
5. Seals are usually lighter and smaller than locks, something particularly important for cargo shipments and courier packages.
6. There are many applications where knowing that tampering has occurred may be more useful and practical than trying to stop it, e.g., tampering with over-the-counter pharmaceuticals or consumer food products.
7. Most locks are not very effective at recording tampering.
8. Whereas a robust lock may encourage an adversary who doesn't care about the intrusion being detected after the fact to bypass the lock and instead damage the container, vehicle, transportainer, or railcar to gain entry, a seal may encourage the adversary to enter through the door, causing no damage except to the seal. There may be additional security, safety, and economic reasons why we would prefer the adversary to enter through a given portal, rather than from any random direction.
9. Seals give security personnel a reason to carefully inspect the container and surrounding area, with a potential improvement in overall security.
10. Locks aren't covert, whereas seals (that is, traps) can be.
11. Many seals are more corrosion resistant than locks, and seals (especially passive seals) may perform better under extreme environmental conditions.
12. 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 in the prototype stage—do not require a hasp and can provide volumetric security.

Types of Seals

There are at least 5,000 different commercially available seals. Most seals can be categorized as belonging to one of the following 11 categories (though there is some overlap):

wire loop seal: This passive 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 1. The lead-wire seal (second from left in the figure) 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. Other, safer soft alloys are sometimes used instead, though such seals are still easy to defeat.



Figure 1 - Examples of wire loop seals

metal cable seal: A larger and sturdier version of the wire loop seal. See figure 2. 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.

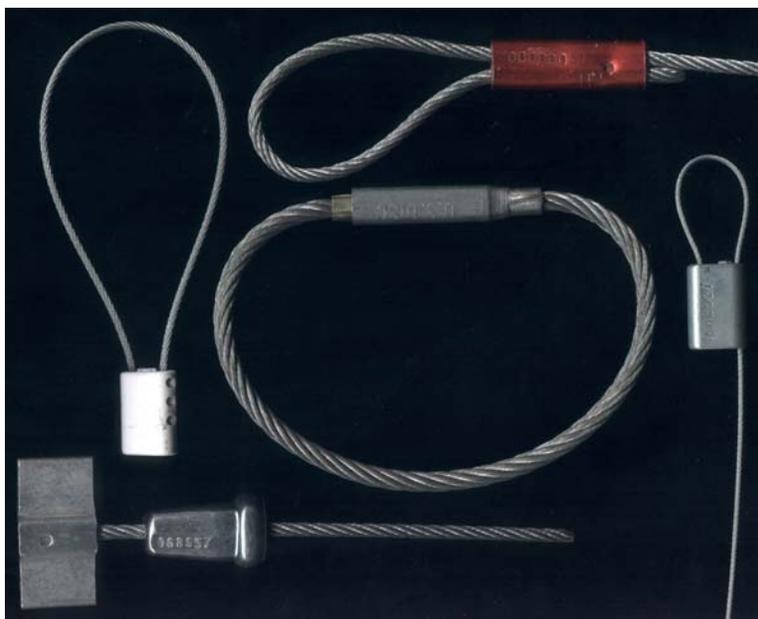


Figure 2 - Examples of metal cable seals

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 or damage equipment coming in contact with sealed moving containers than is the case with metal seals. Plastic also will not corrode.

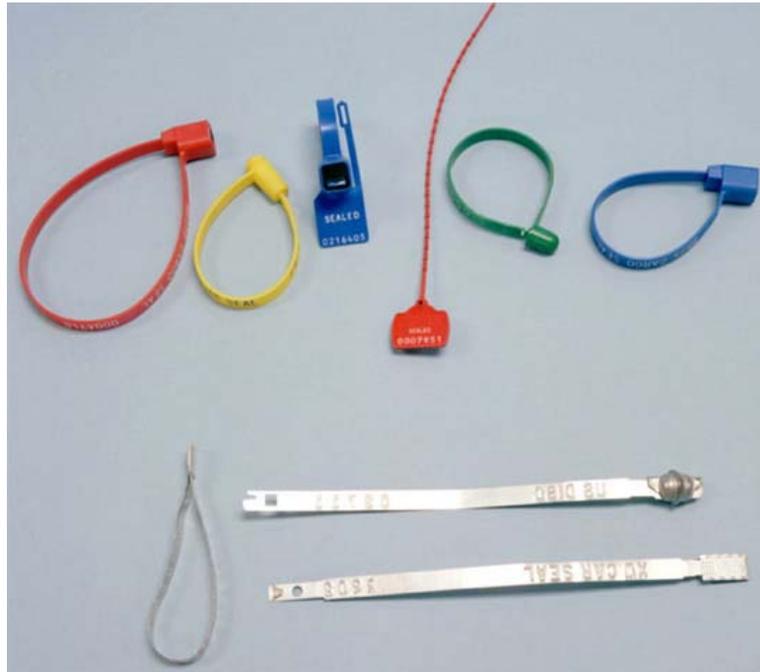


Figure 3 - Some plastic strap seals (top) and metal ribbon seals (bottom).

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: See figure 4 for examples. This is a barrier seal consisting of a strong bolt with each end larger in diameter than the hasp. One half is designed to snap irreversibly into the other half through the hasp. 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. See figure 5. Despite the name, these are seals, not locks. They are often used on residential and commercial utility meters.

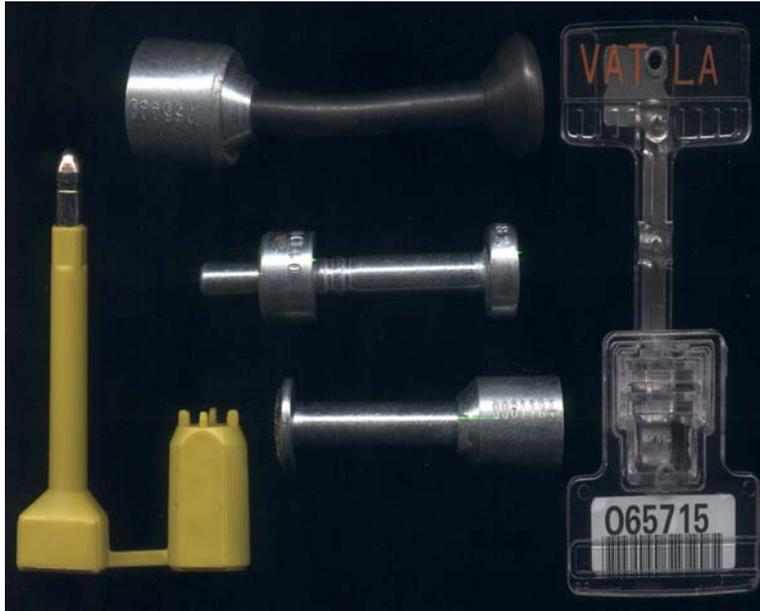


Figure 4 - Some examples of bolt seals. The seal on the right contains a bar code.



Figure 5 - Some examples of "padlock" seals.

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 6. They are often used as tags. (A tag is a device to uniquely identify an object or container.) These types of seals are inexpensive and easy to use, but do not typically provide high levels of security, nor are they very robust.



Figure 6 - Some low-cost, pressure-sensitive adhesive label seals.

frangible seal: This type of seal is often used for tamper-evident packaging, such as found on over-the-counter pharmaceuticals. The seal material, which can be a film, foil, dried paste, or plastic cap, fractures or ruptures when the container is opened.

(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: This type of (typically reusable) seal is battery powered and checks continuously for tampering.

VAT Findings

The Vulnerability Assessment Team (VAT) at Los Alamos has analyzed 213 different tamper-indicating seals in detail, both government and commercial. We have also studied 100+ other seals in lesser detail. These seals run the gamut from inexpensive, low-tech seals, through expensive, reusable, high-tech active seals. The unit cost of the seals varies by a factor of more than 10,000. Most of these seals are in widespread use. About half are currently employed in applications that can reasonably be considered “critical” or “high security”. At least 16% of the seals are currently in use somewhere in the world for nuclear safeguards.

In the course of this work, the VAT has determined that all of these seals, at least the way they are conventionally used, can be defeated quickly using only low-tech, inexpensive methods, tools, and supplies available to almost anyone. The good news, however, is that most of the attacks have simple and inexpensive countermeasures. Sometimes these involve modifying the seal, but often they involve minor changes to the seal use protocols. Unfortunately, these countermeasures are rarely implemented.

Caveats About Active Seals

Passive seals require a great deal of manual labor to inspect. Many seal users hope that by replacing passive seals with active (electronic or electrooptic) seals, or using high-tech seal readers, they can reduce the time and labor needed for inspection. In our experience, however, transponder seals, active seals, and seal readers currently available tend to require *more* effort from seal installers and inspectors for a given level of security than simple mechanical seals. Indeed, current high-tech seals and seal readers tend to be susceptible to a wide variety of simple physical attacks.

Now it is almost certainly true that high-tech, active seals have the *potential* for providing more effective tamper detection than simple mechanical seals. We do not believe, however, that this potential has yet been realized in existing products, or in how these seals are typically used.

Active seals are also hampered, in contrast to passive seals, with issues of battery lifetime and replacement. The performance of active devices under extreme environmental conditions, and how they fail when the battery power gives out, can also create significant vulnerability and logistics problems.

Active seals tend to be much more expensive than passive seals. In theory, their ability to be reused can overcome this limitation. In practice, however, cargo thieves or vandals who don't care about their intrusion being detected after the fact may steal, damage, or destroy the active seal in the process of breaking and entering. This can create havoc with the economics of reusable seals, and can even be an effective deliberate attack strategy on the part of an adversary to discredit active seals. Moreover, if the active seal is to be removed from a container or vehicle for reuse by the cargo shipper, there are extra labor costs, plus extra shipping costs if the seal is to be returned to the original shipping location.

A recent trend that should be viewed with some suspicion involves adding high-tech components to existing passive seal designs. This can include, for example, the use of passive radio frequency (rf) transponders (figure 7), bar codes (figure 4), or electronic contact memory (e.g., iButton) devices (figure 7). These allow the seal identity (serial number) to be read automatically in a non-contact manner (for rf transponders or bar codes) or via brief contact (for electronic contact memory). The intent is to “modernize” a given passive seal design, improve security, and make the seals easier and quicker to use.

In reality, these high-tech components—while very useful for inventory functions—typically add nothing to a seal's ability to detect tampering. They are usually unaffected when the seal is tampered with or damaged. Moreover, the way these high-tech components are currently being used actually make attacks easier for an adversary, and typically result in a decreased probability of detecting

tampering. Transponders, bar codes, and contact memory buttons need to be used in a more intelligent manner for tamper detection than we are currently seeing.



Figure 7 - Two commercial passive rf transponders (top), and a contact memory device (iButton) on the lower left. These do not require battery power, but instead get their electrical power at the time they are read. They then report a unique serial number to the reader. (The reader is typically a few cm from the rf transponders, but must touch the iButton.) Even though these devices are very useful for cargo inventory, mindlessly adding them to a passive seal does not increase the chances of detecting tampering, and may actually decrease security.

It is also common to assume that adding sophisticated encryption or digital authentication capabilities to an active seal or a seal reader will significantly improve security. This is not automatically true. Encryption and authentication are useful for securing communications between a sender and receiver location that are themselves physically secure. Encryption or authentication is not useful if the adversary can compromise the sender (or receiver). Once an adversary gets inside an active seal or a reader, he can tamper with the encryption electronics or software, or even get direct access to the raw, unencrypted data.

Inventorying vs. Securing

Bar codes, rf transponders, and memory buttons are examples of devices that are very useful for inventory functions, but add little to security—at least the way they are currently being used. We believe it is a serious mistake to confuse inventory functions with security functions. This often results in serious security vulnerabilities. Inventorying is the act of counting and locating cargo or other assets. There ordinarily is no nefarious adversary to worry about. Security, however, is all about trying to neutralize the bad guys.

Another example of an inventory technology that is being used for security—potentially with serious consequences—is the Global Position System (GPS). GPS tracking systems are often used for cargo security, especially for tracking trucks. GPS is certainly useful for navigation and for keeping tabs on a truck and its driver, but it is crucial to bear in mind that GPS is not an intrinsically secure

technology for most users. It is trivial for adversaries to block or jam the civilian GPS satellite signals, and relatively easy to spoof them. Spoofing means sending fake data to a GPS receiver. We have demonstrated how easy this is to do. Cargo thieves and truck hijackers need little knowledge of electronics, computers, or GPS to spoof a civilian GPS receiver. (Civilian GPS satellite signals are the only ones available to private companies and to over 90% of the federal government. Unlike the military GPS satellite signals used for cruise missiles and smart bombs, the civilian GPS signals are neither encrypted nor authenticated. This means they are not secure.)

While we know of no examples of cargo theft or truck hijacking based on attacking GPS receivers, it is only a matter of time. Fortunately, there are some inexpensive countermeasures against at least spoofing that can be retrofitted onto existing GPS receivers.

Guidelines, Norms, & Standards

There is little in the way of useful guidelines or standards for how to choose or use seals. There are no widely accepted norms or best practices for seal use. Indeed, in our experience, most seal users employ poor use protocols, even for critical applications. Few know how to choose a seal for a given application. Most are unaware of the vulnerabilities of the seals they are using, and few provide their seal installers and inspectors with the hands-on training needed to reliably detect tampering.

Contributing to the problem is the fact that few manufacturers or vendors of seals provide sufficient information for customers to use their products effectively. Some make exaggerated or blatantly false claims for their products.

In the absence of useful guidelines, standards, and norms, we offer here some general suggestions for using seals more effectively. The best recommendations, however, depend on details of the application of interest, the facilities and personnel available, the relevant economics, the goals of the cargo security program, the nature of the adversaries, and the specific seal(s) being used.

Things to Remember When Choosing a Seal

1. There is no one “best” seal. The optimal seal for your application depends critically on your application and situation.
2. A seal should be chosen with a careful consideration of the containers, doors, or hasps to be sealed.
3. (Ideally the same) serial number should appear on every independent part of a seal. If serial numbers are stamped or embossed on a tag/seal, they should be done deeply enough that they can't be easily buffed off.
4. Unit cost is often the least important economic factor associated with a seal. Costs associated with installation, inspection, readers, and training are often much larger.
5. Tamper detection effectiveness is not well correlated to seal cost, or the degree of high technology employed by the seal.

6. Combining two existing seals into a single tamper-indicating device usually results in less security, not more.
7. Using a high-tech reader to check a seal often increases seal vulnerabilities unless the use protocols and training for the seal inspectors & installers include significant manual and visual inspection procedures, and counter-measures for the new vulnerabilities introduced by the reader.
8. A seal design will usually be most vulnerable to attack near the end of its life.
9. Counterfeiting is rarely the easiest attack on a seal.
10. Seal developers, vendors, and manufacturers usually overestimate the degree of difficulty of defeating their seals.
11. A seal that is complex and difficult to use, that has significant ergonomic problems, and that is resisted by seal installers and inspectors will not provide good tamper detection.
12. 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.)
13. Reliable tamper detection is hard work. No seal can negate that unavoidable fact.

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 for 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 associated with the seal they are using, and specifically look or test for them. Vague instructions to, for example, “look for signs of tampering” are not satisfactory. 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 tamper detection programs, however, disloyal seal installers and inspectors can usually defeat a tamper detection program with ease, even if they lack specific vulnerability information.
3. Seal inspectors should have hands-on practice and training detecting seals that have been attacked both subtly and crudely.
4. Seal personnel should be trained in observational skills, social engineering tactics, and misdirection & sleight of hand techniques.

5. Seal personnel should be encouraged to observe, think on the job, and report concerns.
6. Inspectors should be rewarded, not punished, for finding potential problems, raising important issues, and thinking on the job. In many security programs, inspectors are afraid to raise concerns about suspicious seals or questionable procedures because of the consternation this causes their supervisor. Seal installers and inspectors should always be treated with respect, and their skills frequently tested.
7. To the extent practical, personnel involved with seals should be emotionally and intellectually engaged in the security task. Inspectors 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. Contests of prowess can be used to motivate, educate, and make the job more interesting.
8. Seal data (and any seal reader) must be very well protected. Information about a seal, such as the serial number, must not be stored in or on the container being protected, unless the information is appropriately encrypted. Seal data that is communicated, shipped, or carried to another location must be secure.
9. Seal readers must be checked 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.
10. There should be periodic, effective vulnerability assessments of both the seals being used and the overall security or verification program.
11. Seals that are inspected visually should be examined with an identical, unused seal held right alongside. Humans do not accurately remember details of exact color, size, surface texture, gloss, and patterns, but they are very proficient at visual side-by-side comparisons. Counterfeits can be more reliably spotted in this way.
12. The security of the seals at the manufacturer and vendor, while being procured or shipped, and while awaiting use is critical. Backdoor attacks are easy to implement if adversaries can gain access to unused seals prior to the time they are installed.
13. 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.
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. 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.

Concluding Remarks

In the experience of the VAT, high-tech, active seals are not automatically better than simple, passive, mechanical seals. Sometimes, they are worse. High-tech seals, however, do have significant unmet potential. In any event, cargo handlers must be careful not to mix up inventory and security functions. If a single system or device must be used for both, it should be analyzed first for its role in taking inventory, then reanalyzed separately for security applications.

The VAT is convinced that a modest seal used correctly can provide effective tamper detection, while any seal (even if high-tech) that is used poorly will not. The key, in our view, is practical hands-on training for seal installers and inspectors. In particular, seal inspectors must understand the vulnerabilities and most likely attack scenarios for the specific seals they are using—and actively look for those attacks. They must have hands-on training that gives them an opportunity to see examples of attacked seals. They must be motivated (ideally through a rewards system) to detect tampering.

It would also be helpful if better seals were available. While there are many possible ways to dramatically improve seal designs, there is unfortunately little research and development currently underway in either industry or government to improve tamper detection. Few seal users, unfortunately, are demanding better seals.

Acknowledgements & Disclaimers

Anthony Garcia, Adam Pacheco, Ron Martinez, Sonia Trujillo, and Jon Warner contributed significantly to this work.

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

The seals and commercial products shown in the figures were chosen at random as examples. Whether a particular product appears in these figures or not should not be construed to have any significance or implications in regards to that product's performance, suitability, vulnerabilities, or whether it has been analyzed by the Vulnerability Assessment Team (VAT) at Los Alamos National Laboratory.

For More Information

1. LANL Vulnerability Assessment Team home page: <http://pearl1.lanl.gov/seals/default.htm>
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, "The Real Deal on Seals," *Security Management*, 41, 93 (1997), <http://lib-www.lanl.gov/la-pubs/00418795.pdf>
4. C.P. Kissane, C.P. and J. DeSanto, "Cargo Theft Loss Prevention Techniques," in *Handbook of Loss Prevention and Crime Prevention*, L.J. Fennelly, Editor, Butterworth, Boston, 1992, pp. 689-691.
5. U.S. Naval Facilities Engineering Services Center (NFESC), "DoD Training Course for Effective Seal Use", <http://locks.nfesc.navy.mil/Seals.htm>
6. L. Tyska (Editor), *Guidelines for Cargo Security & Loss Control* (Annapolis, MD: National Cargo Security Council, 1999), pp. 29-38.