UNITED NATIONS **E**

Economic and Social Council

Distr.
GENERAL

TRANS/WP.30/2003/13
15 April 2003

Original: ENGLISH

ECONOMIC COMMISSION FOR EUROPE
INLAND TRANSPORT COMMITTEE
Working Party on Customs Questions
affecting Transport
(One-hundred-and-fourth session, 17-20 June 2003,
agenda item 7 (c) (v))

CUSTOMS CONVENTION ON THE INTERNATIONAL TRANSPORT OF GOODS UNDER COVER OF TIR CARNETS (TIR CONVENTION 1975)

Application of the Convention

Issues relating to technical provisions

Tamper-Indicating Seals: Practices, Problems, and Standards

Transmitted by the Government of the United States of America

Note: The secretariat reproduces below a communication transmitted by the Government of The United States.

* * *

A. EXECUTIVE SUMMARY

1. Tamper-indicating seals can have an important role to play in customs, nonproliferation, law enforcement, and counter-terrorism. Unfortunately, the tamper-indicating seals currently available, given how they are typically used, can be quickly and easily spoofed by almost anyone. High-tech electronic seals are not automatically better than simple mechanical seals, and are often worse. More reliable tamper detection is possible with greatly enhanced training for seal installers and inspectors, better seals, and a more thoughtful use of high-technology.

B. INTRODUCTION

2. Tamper-indicating seals have been used by customs officials for over 7,000 years. Today, seals are widely used to help counter theft, smuggling, sabotage, vandalism, 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 absence of meaningful norms and standards, together with the surprisingly limited amount of research and development (R&D) in the field of tamper detection, has also hindered the effective use of seals.

3. The Vulnerability Assessment Team (VAT) at Los Alamos National Laboratory has intensively studied tamper-indicating seals for the last 12 years. We have engaged in vulnerability assessments, R&D, consulting, and training for over two dozen United States government agencies and private companies, as well as for the International Atomic Energy Agency (IAEA) and Euratom. The VAT has also analyzed over 200 different types of seals in detail. This paper summarizes some of our conclusions, recommendations, and warnings regarding seals and tamper detection.

C. TERMINOLOGY

4. We encourage the use of the following terminology which is, unfortunately, not universal:

(a) Security Devices

- tampering: gaining unauthorized access or entry for the nefarious purposes such as theft, smuggling, sabotage, vandalism, terrorism, or espionage.

- lock: a device to delay, complicate, and/or discourage unauthorized entry.

- seal = tamper-indicating seal: 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. Indeed, some seals are made of paper or plastic and can be easily yanked off a container; this does not necessarily make them ineffective as seals.) Seals must be inspected before there can be a determination of whether tampering has taken place. There are different types of seals:

- passive seal: a seal that does not rely on batteries or electrical power.

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

- barrier seal: a single, hybrid security device that is both a lock and a seal. 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. With a type 1 trap, the intruder becomes aware of the trap only after engaging in the unauthorized access, at which point it is ideally too late to cover his tracks. In a type 2 trap, the intruder is never aware of the existence of the trap, either before or after tampering has occurred. A trap is said to be tripped when it has recorded unauthorized access or entry.

- intrusion detector: a device that reports unauthorized access or entry in real-time (immediately), rather than at the time of inspection as seals do.

- tamper detector: a seal.

(b) Seal Vulnerability Terms

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

- seal reader = seal verifier: a device (usually electronic or optical) that checks a 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, 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 cutting a seal off a container is not automatically the same as defeating it, since its absence or the damage done to it can be noted by the seal inspector.

- 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.

- vulnerability assessment: discovering and demonstrating ways to defeat a security device, system, or program. May include suggesting counter-measures and security improvements.

(c) Tags

- tag: a device, or an applied or intrinsic feature, used to uniquely identify an object or container. Because they have similar attributes, seals are sometimes used as security tags, and security tags are sometimes used as seals. The different types of tags include:

- inventory tag: a tag meant only for accounting purposes, when there is no nefarious adversary.

- anticounterfeiting tag: a tag attached to an object or container that is difficult or expensive to counterfeit, but for which lifting (see below) is not a concern. Often used to inhibit product counterfeiting.

- security tag: a tag designed to be difficult or expensive to counterfeit, and that has tamper-indicating features so that lifting attempts can be detected. Often interchangeable with tamper-indicating seals (and vice versa) because of their tamper-indicating features.

- buddy tag: a token that is difficult or expensive to counterfeit, but that is not meant to be attached to, or even adjacent to, the unique object it is partnered with. Often used to demonstrate you possess a particular object without having to present that object.

- lifting a tag: removing a tag from one object or container and placing it on another, without being detected.

- defeating a tag: counterfeiting or lifting the tag, without being detected.

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

(d) Terminology not to Use

5. The VAT strongly discourages use of the following terminology because it is misleading, confusing, and demonstrates a lack of understanding of tamper detection fundamentals:

- "tamper-proof" seal: This term is ludicrous. Seals are not meant to be unaffected by tampering, they are meant to readily record it. Moreover, there are no security devices that are impossible to defeat, and even if there were, absolute invincibility in unprovable. "Tamper-indicating seal" is the preferred term.

- "tamper-resistant" seal: This terminology is similarly misleading because seals are not meant to resist tampering, but instead indicate when it has occurred. "Tamper-indicating seal" is the preferred term.

- 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 do not prevent or resist it, except perhaps in some vague psychological sense.

D. WHY USE A SEAL INSTEAD OF A LOCK?

6. All locks can be defeated, even by determined amateurs, usually quickly.

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

8. After locking up cargo, a package, container, railcar, truck, or transportainer, the key or combination must be present at, or sent to, the receiving location.

9. Seals are usually cheaper than locks.

10. Seals are often easier and faster to remove than locks, including in emergencies.

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

12. There are many applications where knowing that tampering has occurred is more useful and practical than trying to stop it, e.g., tampering with over-the-counter pharmaceuticals or food products.

13. Most locks are not very effective at recording tampering.

14. Whereas a robust lock may encourage an adversary who does not 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 through the door, causing no damage except to the seal.

15. 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.

16. Seals give security personnel a reason to carefully inspect the container and surrounding area, with a potential improvement in overall security.

17. Locks are not covert, whereas seals (i.e., traps) can be.

18. Many seals are more corrosion resistant than locks, and (passive) seals may perform better under extreme environmental conditions.

19. 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.

E. WHY USE A SEAL INSTEAD OF AN INTRUSION DETECTOR?

20. Many applications do not require real-time notification of unauthorized access or entry.

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

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

23. Intrusion detectors require a source of electrical power. Many seals do not.

24. Intrusion detectors require some kind of continuous one-way or two-way communication channel. This greatly complicates things, adds to the cost, and creates reliability problems, especially for moving cargo.

25. Simultaneously monitoring multiple moving containers, vehicles, railcars, or transportainers for real-time intrusion can be extremely impractical.

26. Seals are more practical for small packages or containers.

27. 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 measures or layers.

F. TYPES OF SEALS

28. 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):

(a) 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.

Figure 1 - Examples of wire loop seals

(b) 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.

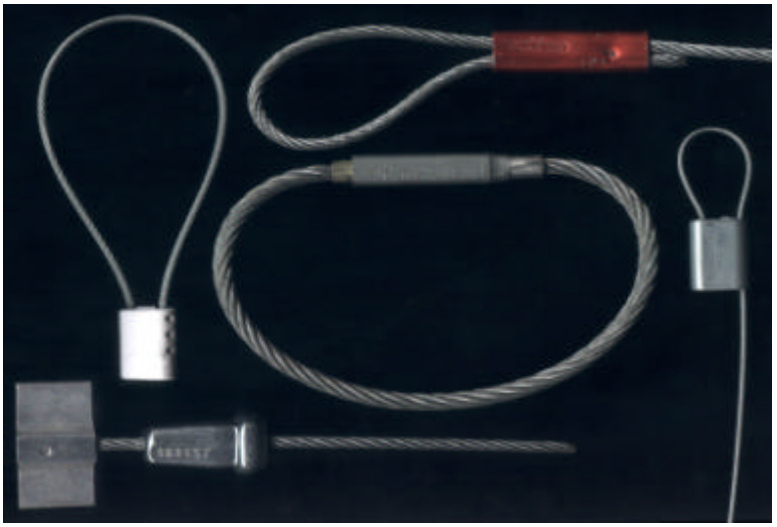

Figure 2 - Examples of metal cable seals

(c) 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.

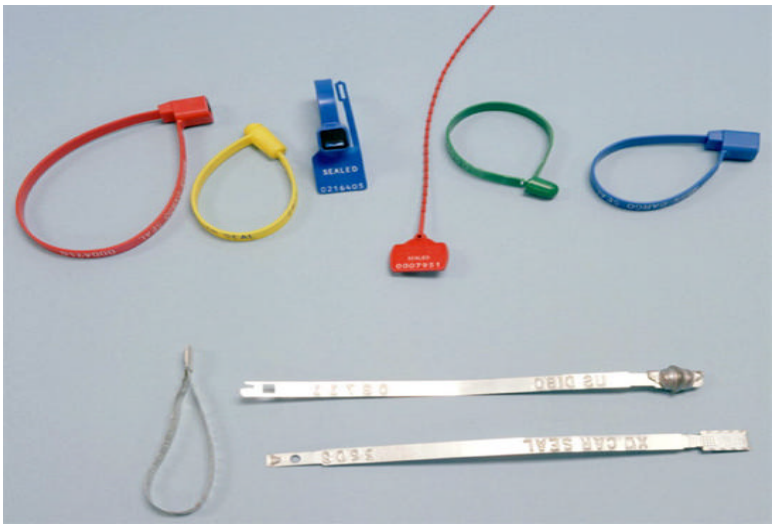

Figure 3 - Some plastic strap seals (top) and metal ribbon seals (bottom).

(d) 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.

(e) 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.

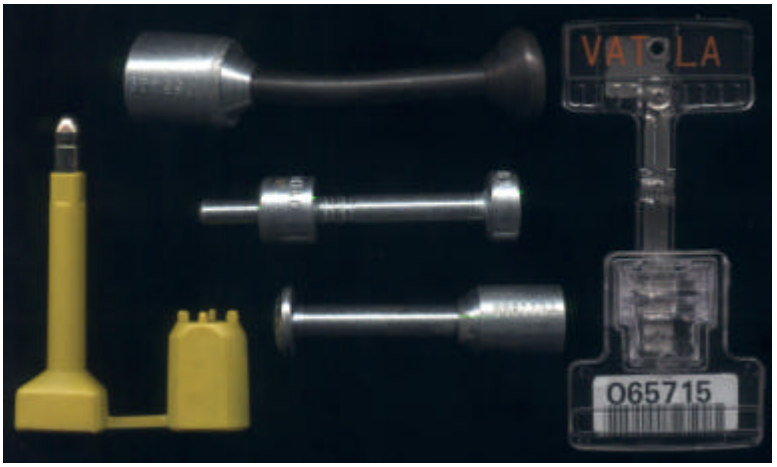

Figure 4 - Some examples of bolt seals. The seal on the right contains a bar code.

(f) 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 5 - Some examples of "padlock" seals.

(g) 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. These types of seals are inexpensive and easy to use, but do not typically provide high levels of security, nor are they very robust.

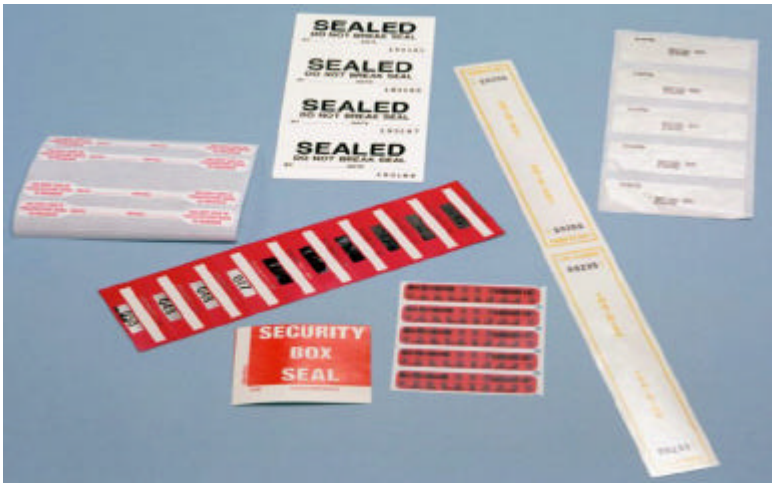

Figure 6 - Some low-cost, pressure-sensitive adhesive label seals.

(h) 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.

(i) (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.

(j) (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. See figure 7.

(k) (active) electronic seal: This type of (typically reusable) seal is battery powered and checks continuously for tampering. See figure 7 for an example.

Figure 7 - Three examples of active seals.

G. VAT FINDINGS

29. The Vulnerability Assessment Team (VAT) at Los Alamos has analyzed 213 different tamper-indicating seals in detail, both government and commercial. 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.

30. In the course of this work, the VAT has determined that all of these seals, at least they way they are conventionally used, can be defeated quickly using only low-tech methods, tools, and supplies available to almost anyone at low cost. Figure 8 shows the percent of these 213 seals than can be defeated in less than a given amount of time by one individual, working alone. For some of the attacks, having an assistant would speed up the attack, while for other attacks, an assistant just gets in the way.

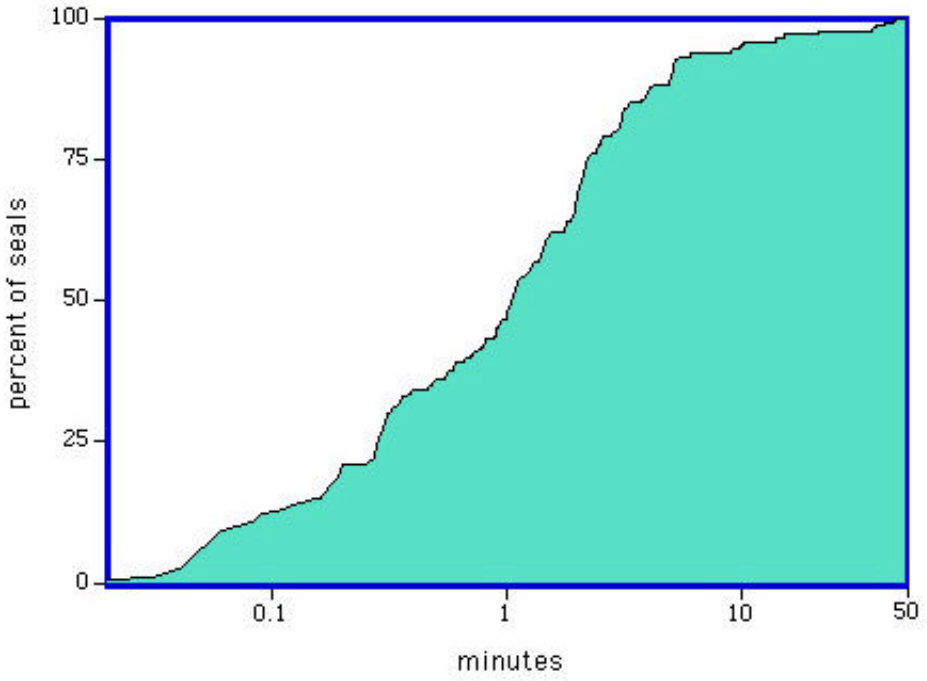

Figure 8 - The percent of seals that can be defeated in less than a given amount of time by one well-practiced attacker, working alone, using only low-tech methods, tools, and supplies.

31. Table 1 shows average results for the seal defeats. Note how quickly the attacks can be completed on average (< 3 minutes), the low cost of the tools and supplies needed ($144), and the low marginal cost of the attacks (42¢). (The marginal cost is the cost to attack another seal of the same design. The cost is very low because the tools and supplies can typically be reused.) Note also that the VAT could devise successful attacks very quickly (less than 5 hours on average), though it often took considerably longer to practice the attack enough to become highly proficient.

attribute	mean (average)	median (mid-point)	range
defeat time	2.7 mins	1.0 min	1 sec to 45 mins
attack cost	$144	$5	2¢ to $4800
marginal attack cost	42¢	9¢	1¢ to $40
Time to devise attack	4.8 hrs	12 mins	1 min to 240 hrs

Table 1 - Results for the fastest successful attacks on 213 different seals.

32. Figure 9 (a log-log plot) shows that expensive seals, such as high-tech electronic or electrooptic seals, are not substantially superior to inexpensive, low-tech passive seals. The defeat time is shown plotted as a function of seal cost for 307 different attacks on 213 different seals, at least one attack per seal. The correlation is very weak (linear correlation coefficient of r=0.14). In fact, adding $1 to the cost of a seal only increases the defeat time by less than 2 seconds on average.

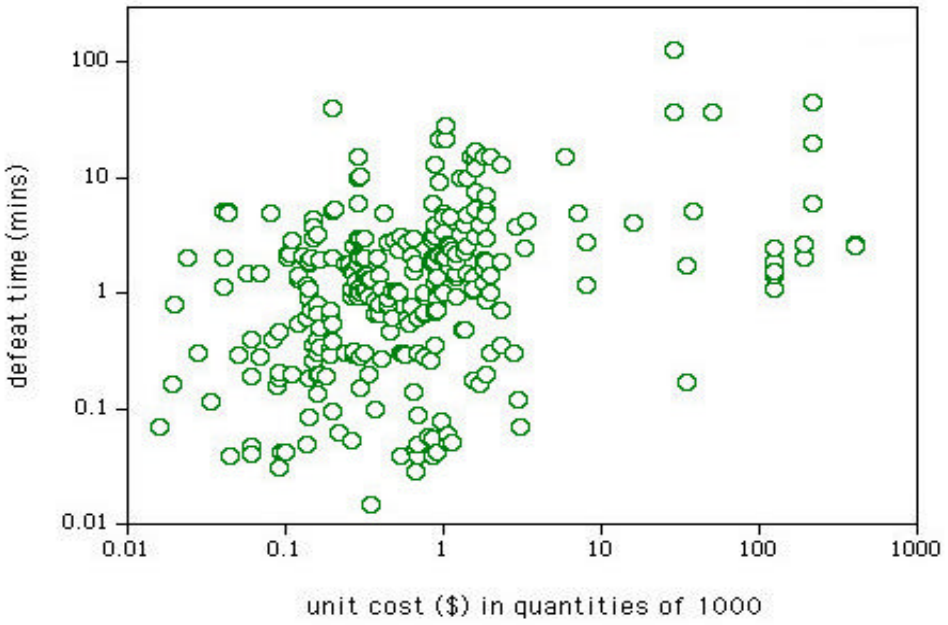

Figure 9 - Seal cost is not a good predictor of vulnerability.

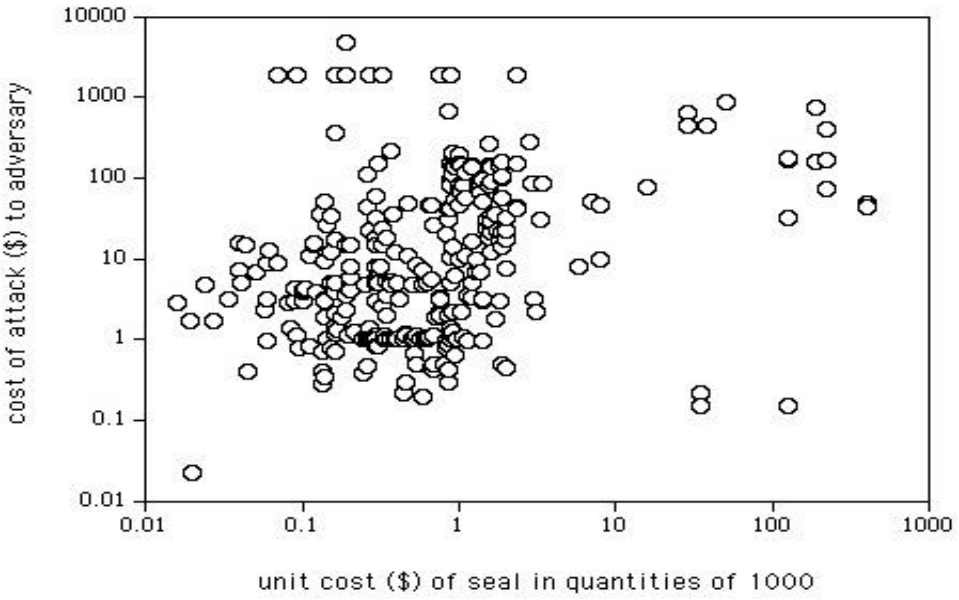

Figure 10 - You can not outspend the adversary.

33. Figure 10 (above) demonstrates that the cost to the adversary of the tools, materials, and supplies needed for an attack depends little on the cost of the seal. The correlation is again very weak (r=0.03). Adding $1 to the unit cost of a seal only increases the cost of an attack by an average of 27¢.

H. CAVEATS ABOUT ACTIVE SEALS

34. 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, the 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, high-tech seals and seal readers tend to be susceptible to a wide variety of simple physical attacks because:

(a) An active, high-tech seal must be physically coupled to the real world.

(b) The standoff distance possible with some high-tech readers usually decreases the chances that the seal inspector will carefully and holistically examine the scene for evidence of tampering.

(c) High-tech devices provide more legs for an adversary to attack.

(d) The high-tech features often become a distraction and/or fail to address critical vulnerability issues.

(e) Security still depends on the loyalty and effectiveness of the seal user's personnel.

(f) Users often do not understand high technology—a serious vulnerability that adversaries can exploit.

(g) Developers of high-tech security devices often have the wrong expertise for real-world applications.

(h) Developers and users often focus on the wrong issues.

(j) High-tech devices are subject to the "Titanic Effect"—arrogance and overconfidence associated with high technology.

35. 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.

36. 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.

37. Moreover, 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 do not 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.

38. When evaluating the economics of active (or passive) seals, many seal users focus on the unit cost of the seal. Bear in mind, however, that costs associated with seal procurement, storage, inspection, record keeping, and training are typically more significant.

39. 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 11), bar codes (figure 4), or electronic contact memory (e.g., iButton) devices (figure 11). 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 our view, however, the approaches currently being used actually make attacks easier for an adversary, and typically result in a decreased probability of detecting tampering. Transponders, bar codes, and iButtons need to be used in a more intelligent manner for tamper detection than we are typically seeing.

Figure 11 - 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.) Mindlessly adding these devices to a passive seal does not increase the chances of detecting tampering, and may actually decrease the chances.

40. It is also common to assume that adding sophisticated encryption or digital authentication capabilities to an active seal will significantly improve security. This is usually a fallacy. 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, he can tamper with the encryption electronics or software, or even get direct access to the raw, unencrypted data. Even if an adversary does not open a seal, however, he may be able to break the cipher or authentication algorithm. The security of common ciphers or authentication algorithms is usually overestimated.

41. Finally, people concerned with cargo security often tout the use of a Global Positioning System (GPS) for tracking moving cargo. This is a useful approach for cargo inventory, 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, and relatively easy to counterfeit, the (non-DoD encrypted) GPS satellite signals available to the public. GPS cargo tracking systems that encrypt or authenticate the latitude and longitude information before relaying it back to headquarters do not solve the underlying problem that the original GPS satellite signals available to non-DoD users are not safe from spoofing. There is minimal benefit to encrypting or authenticating raw data that an adversary can readily spoof in the first place.

J. GUIDELINES, NORMS AND STANDARDS

42. There is little in the way of useful guidelines for how to choose or use seals, though some of the references at the end of this paper offer general suggestions. 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.

43. 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.

44. There is currently no fundamental theory of tamper detection, only minimal guidelines for seal use, remarkably little research and development in the area, and no meaningful standards for seals. Some of the existing guidelines and standards are listed at the end of this paper. None adequately address how to choose or use a seal, compare seal performance (beyond mechanical strength and environmental durability), test seal vulnerabilities, or train seal installers and inspectors. Given the generally poor understanding of tamper detection, the VAT is skeptical that useful standards can be developed at this time. Attempts to develop standards are, in our view, likely to create more problems than they solve.

K. CONCLUDING REMARKS

45. 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.

46. 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.

47. It would also be helpful if better seals were available. While there are many possible ways to improve seal designs, there is unfortunately little research and development currently underway in either industry or government to improve seals and tamper detection with an emphasis on improved security.

Disclaimers

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. The VAT has access to many more seals than it has analyzed.
