A reprint from
American Scientist
the magazine of Sigma Xi, The Scientific Research Society

Tamper-Indicating Seals

From the earliest civilizations to the present, seals have provided evidence of unauthorized access

Roger G. Johnston

Since the dawn of history, people have wondered about some deeply philosophical issues: Who am I? How was the world created? What is the meaning of life? And for as long as human beings have been thinking of such things, they have also been occupied by another classic question: Has anybody been messing with my stuff?

Archaeologists know that people at least 7,000 years ago worried about the safety of their possessions. Examples of various tamper-detecting efforts are found in museums all over the world. Today, concerns about unauthorized access and tampering loom large in all areas of life. Perhaps the most obvious are matters of public security, such as looking for weapons or explosives at airports and seaports, monitoring of facilities in countries bound under the Nuclear Nonproliferation Treaty, transporting and storing nuclear materials and hazardous chemicals, and securing election ballots and voting machines.

But there's just as much impact on the everyday consumer as well, regarding the safety of food, drugs, and paper and computer records. Others also have to worry about improper use or handling of medical equipment and supplies, instrument calibration, fire extinguishers, utility meters, courier bags and forensic evidence, to name a few.

Cargo security is another enormous area, but one that is mostly invisible to average people, although they are

Figure 1. Cuneiform writing on this 3,700-year-old clay tablet, excavated from the Syrian-Turkish border, details a property transaction. The contract was enclosed in a clay envelope, now broken, which was then stamped with the personal seals of witnesses to the deal. Such intricate impressions were used for thousands of years to ensure authenticity and mark ownership. Throughout the ages, seals have evolved to use many materials, formats and technologies. Today's versions range from plastic films on food products to fiber-optic loops on containers of nuclear material. But the purpose of seals remains unchanged: to alert their users to any tampering that might be attempted.

Figure 2. Over the centuries, people have used a multitude of materials to fabricate seals, stamping them into various media. This Mesopotamian cylinder seal, which is made of volcanic rock and dates to around 3000 B.C., was rolled across clay tablets *(top left)*. A gold signet ring from circa 500 B.C. Egypt was pressed into clay or wax blobs to seal papyrus documents *(top right)*. Decorative gemstones were often used to make seals for the wealthy, such as this carnelian example, which belonged to the chief store-keeper of Iran in the 5th century A.D. *(bottom left)*. Resin, lead and other metals were later used to seal the knots of strings tied around correspondence. A metal seal secures the parchment cover of official correspondence from Emperor Andronicus 11 from 14th century Byzantium *(bottom right)*.

ultimately the ones who pay for the losses. There are no official numbers, but security experts calculate that 2 percent of all freight worldwide is stolen. In the United States, such losses could amount to about $50 billion a year, but estimates range from $2 billion to $150 billion, give or take. Transporters also have to worry about drug smugglers, who do not steal merchandise but who use shipping containers to import contraband. Such criminals break into these sealed or locked metal enclosures, hide their wares, leave behind no evidence of entry, then return to collect their goods later.

Tampering can thus have very serious implications, in many different areas, for safety, security, privacy, economics and public well-being.

Inspection Gadget

There are many components in a complete security system. Here I focus on seals, devices designed to record evidence of tampering. To understand how they work, it helps to compare them with other types of security apparatus. First, consider locks, which are normally intended only to delay, complicate and discourage unauthorized entry, it usually being difficult and expensive, if not impossible, to keep people from entering a building, package or vehicle if they are determined to do so. (Hence, the old saying, "locks keep honest people honest.") The threat of capture and punishment should not be overlooked as a major factor in the success of any type of security mechanism.

For critical applications, locks are often used in conjunction with intrusion detectors, or in other words, burglar alarms. These units most often transmit an alert so that the police or security guards can descend on the point where break-in took place. The hope is that they can apprehend the trespassers or at least chase them off before they cause harm. Typical problems with intrusion detectors include their cost, complexity and tendency to go off a lot when nothing is amiss. Moreover, they require having on standby police or a private

Roger G. Johnston has been head of the Vulnerability Assessment Team at Los Alamos National Laboratory (LANL) since 1992. He received a B.A. from Carleton College in 1977, and M.S. and Ph.D. degrees in physics from the University of Colorado in 1983. Johnston has authored more than 90 technical papers and 45 invited talks and holds 10 U.S. patents. He has won numerous awards, including the 2004 LANL Fellows Prize for Outstanding Research. Address: Los Alamos National Laboratory, MS J565, Los Alamos, NM 87545. Internet: rogerj@lanl.gov

guard force that can respond quickly, and these devices can be very difficult to employ on moving cargo.

Often, it's just not practical to try to stop unauthorized access or to respond to it rapidly when detected. Frequently, it's good enough to find out some time after the fact that trespassing took place. This is where tamper-indicating seals come into play. Unlike locks, seals do not attempt to resist or seriously delay breakins. And unlike intrusion detectors, they do not sound a real-time alarm. Instead, seals are meant to leave behind evidence that unauthorized access took place. They often take the form of tamper-evident packaging, commonly found on consumer products such as foods and drugs, or they can be engineered as barrier seals, which combine a lock and a seal into a single device and are often used on truck, railcar or container doors for cargo security.

It is incorrect to refer to seals as "tamper-proof" or even "tamper-resistant." In fact, they are often easily breakable, but their point is that they are difficult to repair. Indeed, if a seal were tamper-proof, it would defeat its purpose, because it would not retain evidence that any manipulation took place.

For some applications, locks and alarms just aren't practical. Items sold over the counter or packages being delivered by courier can't be weighed down with such devices. But seals can be light, cheap and disposable. These features are also important for cargo containers, which may wander the planet for years before returning to their original owners. The facts that seals don't have combinations or keys to keep track of, often don't require power to function and can be removed quickly in an emergency, are also important for shipping.

Nobody knows for sure, but probably well over 10 million seals are installed or inspected each day in the United States alone. If one includes tamper-evident packaging in the tally, that number greatly exceeds 200 million per day. Seals are thus a large part of modern-day security.

Murky Origins

Tens of thousands of years ago, people probably swept the ground in front of their dwellings, religious shrines or stashes of food or weapons before heading elsewhere. On their return, they'd look for footprints left in the sand or dirt, which would signal trou-

Spoofing Clay Seals

For thousands of years in ancient Mesopotamia and Egypt, earthen seals secured property and correspondence against tampering. But just how secure were such sealings?

Not very. Indeed, evidence of ancient counterfeiting may exist in the form of small cylinders with ornate designs, dating from around 2500 B.C. Unlike more typical cylinder seals of that era, which are made of stone, these were fashioned from clay. Their complex markings could have been transferred to the clay cylinders by rolling them over the flat impressions of other seals. If so, these clay cylinders could then have been used to create forgeries. Whether they were actually employed in this way is, however, not known. There are also suspected examples of forgeries, ancient and modern, by artisans who carved new seals that looked similar to the original.

Having studied the security of modern seals, my colleagues at Los Alamos National Laboratory and I decided to see whether we could defeat clay seal impressions, using materials commonly available thousands of years ago. We demonstrated several methods, but counterfeiting proved the easiest. We stamped several types of clay with modern brass seals. We greased the impressions with sesame or olive oil, then made casts of them using clay or beeswax. Once hardened, these castings could be used to create counterfeit impressions.

Volunteers inspected our handiwork in several trials. We showed these people an original and either allowed them to keep it or had it taken away. We then presented them with single or multiple impressions at once and asked them to decide which examples were counterfeit. On average, the volunteers were wrong nearly one-third of the time. And although they were told that the counterfeits were greatly in the minority, the inspectors tended to claim an inordinate number of impressions were fakes.

Volunteer inspectors were not instructed on how to spot a counterfeit, to their frustration. It's likely that their ancient counterparts were in much the same situation. But close comparison of counterfeit impressions with originals shows one reliable way of spotting fakes. The clay or beeswax castings we used to create the counterfeit sealings shrank as they dried. Thus, counterfeit impressions made from these castings were smaller, by an average of 7.5 percent for wax and 9.5 percent for clay, than the genuine stampings, although this modest reduction in size might not be noticed without a side-by-side comparison with the real thing. In the image below, the counterfeit sealing is at the bottom right.

Modern seal inspectors are rarely given examples of genuine seals to use for reference, which may allow reasonably accurate forgeries to go unnoticed. Were ancient seal inspectors in the same position? Archaeologists have found small clay rectangles impressed with seals. These may have been business tokens, identity cards or calling cards. But perhaps they were also given to an envoy so that he would know the correct sealing to look for and be able to make an accurate comparison.

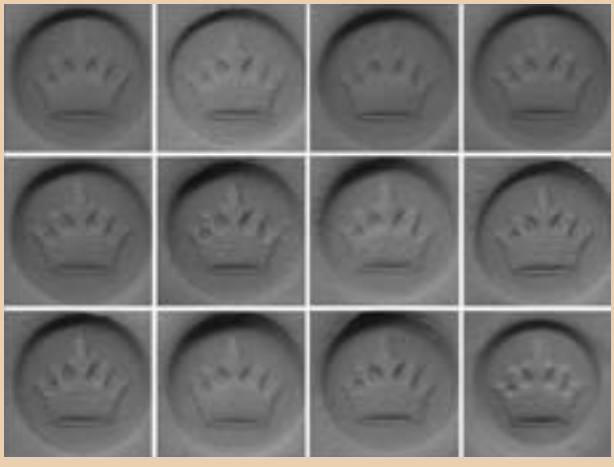

Figure 3. The author estimates that there are more than 5,000 types of modern seals, which come in various sizes, shapes, weights and materials. Some of the most high-tech are electronic, using fiber optics and sensors to monitor for tampering *(top row).* Certain passive seals also use optical fiber *(two black loops, second row, right).* Some designs, called barrier seals, are designed to serve as locks as well as seals *(second and third rows, left).* Strap-type seals, nowadays mostly made from plastic, are used on cargo containers *(middle left).* Wire-loop seals are updated versions of ancient lead seals *(bottom left).* Frangible paper or plastic films are made to tear or deform irreparably if opened *(middle and bottom right).* Similar-looking seals have a wide range of uses: The purple wire loop is used on utility meters, whereas the green and copper wire loops next to it are used in nuclear safeguarding. The center electronic seal and the passive fiber-optic seals are also used in nuclear applications. (Photograph courtesy of the author.)

ble. Of course, a trespasser could easily thwart this system with nothing more than a tree branch. So at some point in the distant past, the utility of marking such places with designs that could not easily be copied became obvious.

People began making personalized seals in Neolithic times. A typical ancient seal consisted of a small disk or cylinder made of clay, wood, bone or stone, one that was carved with a unique design. The seal was used, for example, to add distinctive markings to the earthen stopper of a jar, either by pressing a disk-shaped seal into it or by rolling a cylinder seal along it while the clay was still soft. If anyone opened the vessel, the newly applied pattern would be destroyed. Lacking the original seal, the intruder would have trouble replicating the design when reapplying a stopper.

People were stamping their property with disk-shaped seals for thousands of years before the invention of writing in about 3200 B.C. Indeed, some scholars think that the symbols used on seals may have encouraged the development of both writing and arithmetic. Cylinder seals were invented in Mesopotamia around 3500 B.C. They had the advantage of cramming more artwork onto a given seal, and the pattern could be replicated indefinitely by continuing to roll the seal along the clay. Some cylinder-seal designs were crafted so that the seal pattern could be laid down with no discontinuity.

The earliest seals were carved into relatively soft clay, wood or bone, so most haven't survived. There are, however, many examples of ancient stone seals. The oldest show simple geometric patterns, but the designs etched on later seals have considerable complexity.

Ancient seals served many of the same functions as their modern equivalents. They were used to detect unauthorized access to a container, package or room; provide cargo security; protect goods against tampering; and assist with customs inspections. They also had tag-like functions: guaranteeing authenticity, helping with inventory control, documenting ownership or trademark and conveying information (especially when few people could read or write). Ancient seals and their impressions were also used for decoration, for religious or magical purposes and as a kind of legal signature or identification card. Even today in parts of Asia, an individual's seal carries more legal and societal authority than his or her signature.

The Egyptians were using lumps of clay, called *bullae,* and string to seal papyrus documents shortly after 3000 B.C. They also used seals on the tombs of their dead. When the burial chamber was completed and the mummified body placed inside, the door edges were covered with mud and plaster. The door could still be opened, but it would then be obvious that the seal was broken. In modern times, archaeologists were able to tell if a tomb had been looted by checking to see whether the seal was intact.

As materials became more sophisticated, so did seals. Starting around

the 4th century A.D., lead seals became popular. A string was looped and tied around a bag, package or basket. The two loose ends were then passed through a soft blob or disk of lead. Next, a hand press, much like a modern-day paper embosser, was used to trap the cord inside the malleable metal and simultaneously imprint a pattern on each side. Anyone trying to access the contents would have to cut the string or rip apart the lead, and such tampering would be obvious.

After about 1100 A.D., Europeans began using wax seals. To mark a document or envelope, the sender would drip some melted wax on it and stamp it with his or her personal seal. Wax was later replaced by shellac or resin.

Some people still like to seal their letters with wax for decoration. Although it may seem an anachronism, the Russian nuclear-safeguards program continues to use wax seals, although much less so than in the past. And the United States and many other countries continue to use lead seals for important security applications.

The Modern Age

The next major advance happened in the 1880s and 1890s, when a number of inventors designed and patented various types of inexpensive, disposable seals for railroad cars. These innovations made it possible to secure boxcars without the need for large, heavy, expensive locks, which were time-consuming to remove when the train reached its destination. If the seal was intact on arrival, it was not necessary to take inventory of the contents or to investigate cargo theft.

Initially the most successful manufacturer of this kind of seal was a Swedish immigrant to the United States named Emil Tyden, who founded the International Seal and Lock Company in Hastings, Michigan, in 1897. His was one of the world's first automated, mass-production factories—a decade before Henry Ford put together his assembly lines for automobiles.

The devices that Tyden and others invented are closely related to metal-strap seals still in use today. After one end of the band is inserted into the other, the seal is irreversibly closed such that the easiest way to remove it is to cut it off. Each seal has a unique serial number embossed on it. If the seal is found to be damaged or missing at the time of inspection, or if it shows the wrong serial number, the seal inspector knows that tampering has taken place.

Other types of modern seals are electronic, or *active,* and run on batteries. For example, in an active fiber-optic seal, one end of the cable is passed through the hasp of the container to be monitored for tampering, then reinserted into the seal. The seal periodically sends a pulse of light down the optical fiber and registers that the cable has been cut or disconnected if these photons fail to complete their journey.

Modern passive seals include irreversible mechanical assemblies (like the metal-strap railcar seals), as well as highly frangible seals that become damaged if anyone tries to remove or open them. Barrier seals, in contrast, can withstand hundreds to thousands of pounds of force. Certain types of fiber-optic seals can also be passive. A photograph made of the end of the fiber-optic bundle is then compared with another taken at a later date. If the bundle has been cut or replaced by another, the "before" and "after" pictures will look different.

Consumers are not likely to see electronic seals in their day-to-day lives. For most people, tamper-evident packaging (TEP) is the most familiar form of antimeddling detection. Since the (still unsolved) 1982 Tylenol poisonings, which killed eight people, all over-the-counter pharmaceuticals sold in the United States are required by law to have TEP approved the U.S. Food and Drug Association (FDA). Many other consumer and industrial products, including food items, voluntarily make use of TEP, which can include delicate plastic films, "break-off" caps and lids, adhesively attached foil or other frangible liners placed under lids, and the "blister packs" used to dispense an increasing number of everyday medications.

Unfortunately, current TEP isn't very good. The FDA is quite vague on TEP testing and performance requirements, and the designs tend to be cheap and unimaginative. TEP is often engineered not so much to provide effective tamper detection as to show due diligence and to reduce jury awards should product tampering take place. It is also meant to encourage the bad guys to mess with somebody else's product.

Another problem with TEP is that the labeling and instructions to consumers are frequently unclear. Often information about the tamper-evident packaging is buried in the fine print or is completely

Bradley C. Bower/AP Images

Figure 4. In 1982 Tylenol laced with cyanide killed eight people. The crime was never solved, but since then, the readily accessible vials of the period *(left)* have given way to ones with tamper-evident packaging *(right).*

missing. It's also relatively common for the only indication that a seal is in use to be placed on the seal itself. If the seal is cleanly removed, there is then no sign that it was ever present.

The reason for this obvious shortcoming is that manufacturers do not really want their goods associated in the minds of consumers with product tampering, so they are often reluctant to point out the tamper-evident features of their packaging in too dramatic a fashion. They will also often obscure the issue by referring to the product's "freshness seal." As a result, foul play typically requires only low-tech methods and minimal skill, and can usually be accomplished in well under a minute (and sometimes just a few seconds) with practice.

Spoofing of TEP usually involves one of five possible attacks: opening the container or package without leaving any obvious evidence; removing the tamper-evident features and hoping the end user won't notice that they are missing; removing the tamper-evident features and putting on bogus replacements to falsely reassure the more-wary consumer; repairing, erasing or hiding any evidence of tampering; or recreating the packaging or its tamper-evident features with counterfeits.

The problems with TEP have received surprisingly little study, even by manu-

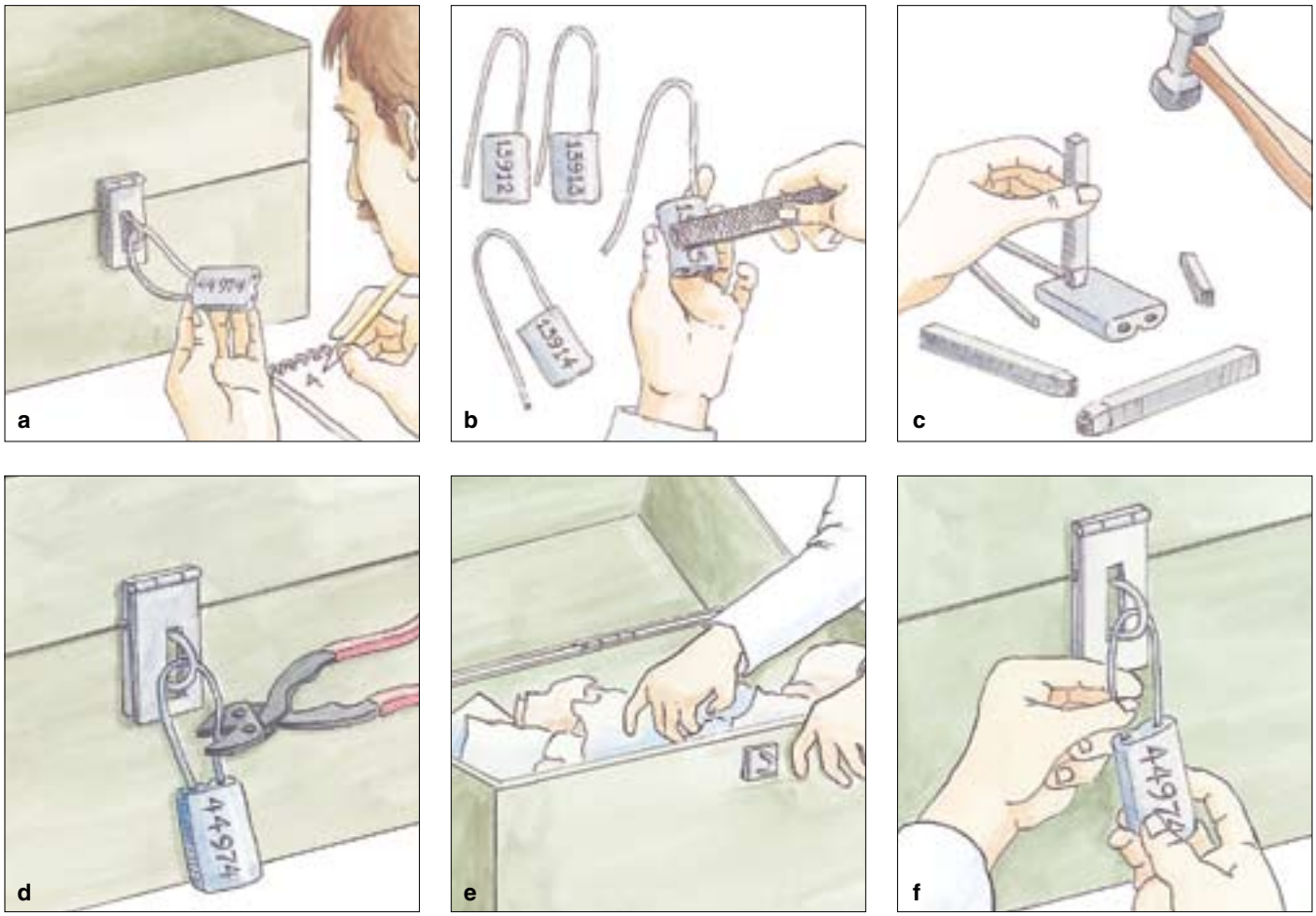

Figure 5. A counterfeiting attack was one of the techniques the author's group mastered to test seals. In this instance, the adversary wants to access a strongbox that has a wire-loop seal. He first notes the serial number embossed on the seal *(a)*. He acquires seals of the same type and removes their serial numbers *(b)*, then uses numbered dies to imprint the same sequence as that on the seal he wishes to remove *(c)*. After snipping off the seal *(d)*, he finds what he wants within the box *(e)* and then uses his handmade counterfeit to hide evidence of his unauthorized entry *(f)*.

facturers who face substantial legal liabilities if product tampering occurs. Our group recently did a brief test at the 7th Security Seals Symposium in Santa Barbara, California. A total of 72 tamper-detection experts attending the conference were asked to determine which food and drug products had been tampered with, and which had not. The attacks had been quickly done by one of our undergraduate students using readily available materials and tools. The conference participants turned out to be no more effective at detecting tampering than random guessing. If TEP designs are insufficient for tamper-detection experts to spot an attack, what chance does the average consumer have?

Tamper Trouble

There are at least 105 different general ways to defeat, or spoof, seals. By "defeat," I mean to remove the seal, then reapply it or replace it with a counterfeit, without detection. Merely yanking a seal off a container is not defeating it, as this will be noticed during inspection.

Most violations fall into 1 of 10 categories. In "pick attacks," the invader uses a special tool to open the seal without damaging it or leaving other evidence. This approach works well on a surprising number of seals. In "unsealing attacks," the apparatus may be marred, but indications of tampering are successfully hidden or repaired. If the malefactor has access to the seal prior to use, he may employ a "backdoor attack," putting an exploitable defect in the seal—either during design, manufacturing, shipping, storage or just prior to use. Alternately, he may sabotage the sealing process, using an insider to apply the wrong seal or not close the door prior to sealing, so an accomplice can access the container then properly close it before inspection. In a "failure-mode attack," the crook challenges the seal-security program directly or with misdirection, or waits until an error is made and then takes advantage of it.

Transgressors may also alter seal data, such as the serial number or reports and interpretations about the inspection. If seals are active, they or their readers are subject to electronic assailments on their various components, such as sensors, software or stored data. More involved are "replicating attacks," which require the creation of a duplicate of the seal at the factory where it is made. Somehow the felons must get employees or others at the production facility to compromise security. This strategy is different from counterfeiting, where a fake (typically a crude one) is made outside of the manufacturing plant using new seals, used parts or completely original materials.

My Los Alamos colleagues and I have analyzed hundreds of government and commercial seals, from low-tech mechanical varieties through high-tech electronic ones. The cost of

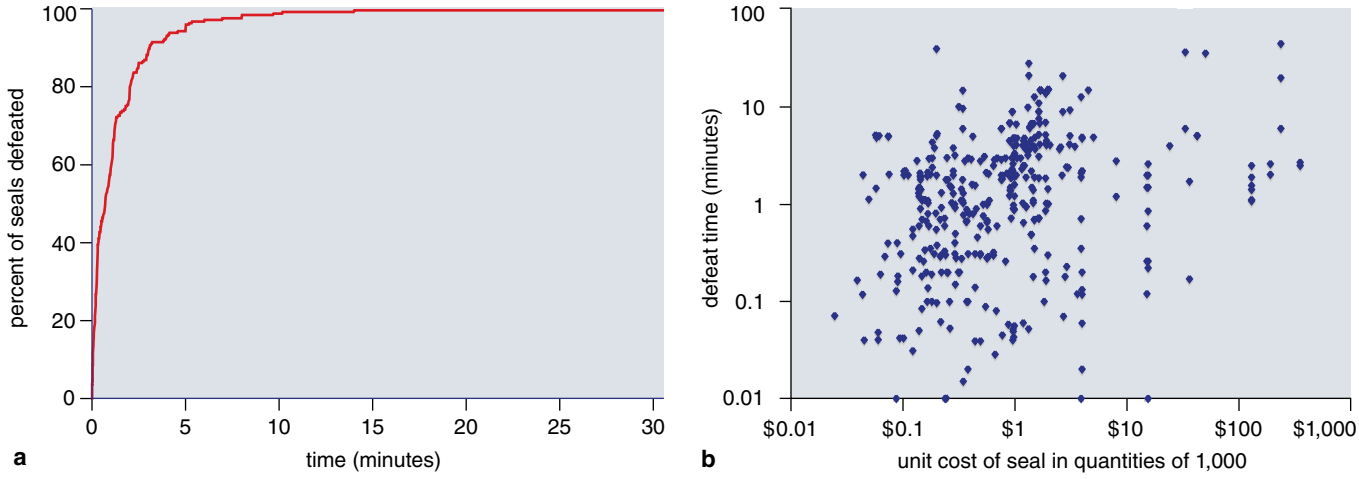

Figure 6. Tests of 244 different seal designs showed that most were relatively easy to attack. The majority could be defeated—removed and replaced without evidence—by one person working alone within about two minutes, and all of these devices could be thwarted within about 30 minutes *(left)*. More expensive seals were not less vulnerable. A plot of 393 different attacks on these 244 seals shows very weak correlation between defeat time and cost *(right)*. On average, spending an extra dollar per seal only increased the time to defeat the seal by 0.3 seconds.

these seals varies by a factor of 10,000. We have demonstrated how all these seals can be defeated quickly and easily using basic tools, supplies, methods and skills, resources that are readily available to almost anyone. Although we have access to considerable high technology at a national laboratory, we have not yet seen a seal—even ones used in nuclear safeguards—that requires a sophisticated attack.

And it's not for any lack of effort in looking. We intensively studied 244 different seal designs, plus several hundred additional designs in less detail. Of the 244 carefully studied seals, half are used for what can be considered critical, high-security applications, including 46 that are in use somewhere in the world for nuclear safeguards. We devised up to six ways to defeat a given seal.

Somewhat counterintuitively, we also discovered that expensive electronic seals are not substantially better than low-cost mechanical seals—at least the way the seals are currently designed and used. Active seals have more pieces that can be attacked, and inspectors of these seals often rely too much on the electronic readers. If the machine says the seal is good, the inspector believes it, even when there are obvious physical signs of tampering on the seal itself.

In our tests, the average attack time on each seal was 1.4 minutes, with a median value of only 43 seconds. The cost was also quite low. Tools and supplies for the first attack on a seal ran a mean average of $78 and a median of $5, but once that investment had been made, subsequent attacks on seals of the same kind dropped to a mean average of 62 cents, and a median of five cents, each. Perhaps the most telling statistic is that we needed an average of only 2.3 hours (12 minutes median) to devise what ultimately proved to be a successful incursion—although it often took much longer to become proficient at the technique. Practice also aided in reducing planning time.

A Better Mousetrap

When my colleagues and I show security managers the vulnerabilities of seals, a number of them wonder whether there is any point at all to using these devices. So we also emphasize that seals can be quite effective if used correctly. About 60 percent of the seal attacks we devised in our study have simple and inexpensive countermeasures, and another 30 percent have solutions that are more complicated. These may involve minor modifications to the seal, but more often the answer is in changing to the seal installation and checking procedures. For instance, most inspectors are not provided with an example seal with which to do side-by-side comparisons. Many companies are also not careful enough with their used seal disposal, providing wrongdoers with parts for counterfeits.

A large problem is that the effective use of current seals—even high-tech electronic seals read with a semi-automatic reader—requires seal inspectors to understand fully the potential weaknesses associated with their application and the specific seals they are using, and then look for evidence of the most likely attack scenarios. Gaining this expertise takes extensive training and practice, detailed information about seal shortcomings, and observational and critical-thinking skills in the field. Few seal users want to go to this much trouble and cost, even for high-security applications. Seal manufacturers also don't want to point out their product-attack countermeasures, as this information highlights their commodity's frailties, which they fear will harm sales.

Fortunately, better seals are possible. But to make better seals, one has to understand why existing seals are so easy to defeat. Their Achilles heel appears to be not so much detecting unauthorized access, as securely storing the *alarm condition,* or the fact that trespassing has been detected, until such time as the seal can be inspected. With current seals (even electronic ones), it is simply too easy for an adversary to hide or erase the alarm condition, or to replace the seal with a fresh counterfeit that shows no evidence of tampering.

One way to deal with this weakness is to invert the problem: At the start, when we first install a seal, we store information in or on it that unauthorized access has not yet been detected. We call this information the *anti-evidence.* These devices can be mechanical, but more often are electronic. Once the seal detects trespassing, it instantly erases its anti-evidence. At inspection time, the absence of the anti-evidence in-