LAUR-06-1310

New Tamper-Indicating Seals

Roger G. Johnston, Ph.D., CPP*, Jon S. Warner, Ph.D., Sonia J. Trujillo,
Anthony R.E. Garcia, Ron K. Martinez, Leon N. Lopez,
and Adam N. Pacheco

Vulnerability Assessment Team
Los Alamos National Laboratory
MS J565, Los Alamos, NM 87545
505-667-7414 rogerj@lanl.gov

Abstract

Product tampering is a serious product safety issue. Unfortunately, neither tamper-evident packaging used on consumer products, nor tamper-indicating seals used for cargo, warehouse, and factory security provide reliable tamper detection. We believe there is a better approach to tamper detection, at least for tamper-indicating seals: anti-evidence seals. Conventional seals must store evidence of tampering until such time as the seal can be inspected. But adversaries can too easily hide or erase the evidence, or replace the seal with a counterfeit seal. With anti-evidence seals, in contrast, we store information when the seal is first installed that tampering has NOT yet been detected. This information (the "anti-evidence") gets instantly erased once tampering is detected. There is thus nothing for an adversary to hide, erase, or counterfeit. This paper discusses 5 new prototype electronic seals based on the anti-evidence concept.

Introduction

Products that are designed to be safe may not stay that way in the face of nefarious tampering.[1-4] The deaths caused by the still unsolved 1982 Tylenol poisoning incidents are a vivid reminder of this fact.[2] Thus, any consideration of product safety ought to factor in the threat posed by product tampering. Tampering hoaxes and extortion threats also present serious problems.[5,6]

Despite the ongoing threat of product tampering, there has been remarkably little in the way of rigorous studies of tamper-evident packaging, and a puzzling scarcity of substantive literature on the general subject of tampering. Indeed, food and pharmaceutical manufacturers appear to be grossly over-confident about the effectiveness of the tamper-evident packaging used on their products. In our experience, they are always surprised when we demonstrate how easy it is to tamper with tamper-evident packaging without leaving evidence.

In our view, current tamper-evident packaging (TEP) is unimaginative and wholly inadequate to the threat. We have demonstrated how containers and packages with the following tamper-evident technology can be easily opened, then reclosed, without leaving any obvious permanent evidence:

- foil liners
- pop-up lids
- blister packs
- pressurized metal soda cans
- pressurized plastic soda bottles
- heat-sealed containers & wrappers
- containers with break-off lids or caps
- frangible ("shrink") plastic film, bands, & wrappings
- adhesive labels (including pressure-sensitive adhesive label seals)
- adhesively-sealed containers (including "glue-flapped" boxes)
- tamper-evident bags (including those used for forensic evidence)
- color-shifting inks
- holograms

The above TEP can be quickly spoofed, using tools, materials, and techniques readily available to almost anyone. (We typically use undergraduate students to develop and demonstrate these attacks.)

The attacks can be done either by repairing (or cosmetically hiding) the evidence of opening or entry, or by replacing the original tamper-indicating material or feature with an undamaged counterfeit or an authentic sample from a different container. The containers and packages themselves are also typically easy to penetrate and repair—thus bypassing the tamper-indicating technologies entirely.

Tamper-evident packaging (TEP) is primarily designed for individual containers and packages used by consumers. Reliable tamper detection, however, is also very important for cases, pallets, trucks, transportainers, warehouses, and factories[7,8]—particularly given that we cannot currently rely on consumer TEP to detect product tampering. Tamper-indicating seals are often used for these industrial security applications. See figure 1 for examples of commercial seals. Unlike locks, seals do not attempt to resist entry, just record that it took place.

Unfortunately, current tamper-indicating seals are not substantially more effective than consumer TEP.[9-11] The Vulnerability Assessment Team (VAT) at Los Alamos National Laboratory (LANL) has analyzed hundreds of different seals. This includes government and commercial seals, from low-tech mechanical seals through high-tech electronic seals. The unit cost of these seals varies by a factor of 10,000.

We have demonstrated how all these seals can be defeated quickly and easily using tools, materials, and techniques readily available to almost anyone. While we have access to considerable high technology at LANL, we have not yet seen a seal that requires high-tech attacks. This is true even for seals used in nuclear applications!

(To “defeat” a seal means to attack the seal by removing it, then re-sealing using either the original seal or a counterfeit, without being detected. Merely yanking a seal off a container, door, truck, or transportainer, for example, does not defeat it because the fact that the seal is missing or damaged will be noted at the time of inspection.)

We have studied 244 different seals in considerable detail, plus approximately 200 additional seals in lesser detail. The discussion here focuses on the 244 most carefully studied seals, but the results are qualitatively similar for the others. Figure 2 shows the percent of the 244 seals that can be defeated in less than a given amount of time by one person, well practiced in the attack, working alone, and using only low-tech methods.

Figure 3 demonstrates that expensive high-tech electronic seals are not substantially better than low-cost mechanical seals—at least the way the seals are currently designed and used. The correlation between seal defeat time and cost is very weak (linear correlation coefficient r=0.10). Moreover, adding an extra dollar per seal to the unit cost only adds, on average, 0.3 seconds to the defeat time.

Table 1 summarizes our findings. The average attack time for the fastest attack on each seal is 1.4 minutes, with a median value of only 43 seconds. The cost and marginal cost of the attacks are also quite low. Perhaps the most telling statistic is that we needed only an average of 2.3 hours (12 mins median) to devise what ultimately proved to be a successful attack—though it often took much longer to become proficient at the attack. In other words, these attacks are fairly obvious.

Countermeasures

60% of the attacks have simple and inexpensive countermeasures. These may involve minor modifications to the seal, but more often involve changes to the seal installation and inspection procedures. 27% of the attacks have countermeasures that are feasible, but not particularly simple or inexpensive.

In our view, effective tamper detection requires seal inspectors to fully understand the vulnerabilities associated with their application and the specific seals(s) they are using, and then look for the most likely attack scenarios. This requires substantial training, many samples of attacked seals, and considerable practice. In our experience, many seal users are unwilling or unable to spend the time and money necessary for reliable tamper detection using conventional seals.

Better Seals

Fortunately, much better seals are possible. We believe that conventional seals have a fundamental design flaw. Once tampering is detected, they must store the fact that tampering has occurred. This "alarm condition" is only noted at inspection time. Adversaries, however, can too easily hide or erase the alarm condition, or replace the seal with a fresh counterfeit.

A better approach is what we call "anti-evidence" seals.[12] With these novel seals, we store information in or on the seal when it is first installed that indicates that tampering has not yet occurred. When tampering is later detected, this "anti-evidence" information is instantly erased. There is thus nothing for an adversary to hide, erase, or counterfeit. The absence of the anti-evidence at inspection time indicates that tampering has occurred.

Some of the potential advantages of anti-evidence seals include [12]:

- High levels of security.
- Adversaries cannot defeat the seal by merely counterfeiting the hardware.
- Low to moderate cost.
- The seal is fully reusable (even if mechanical).
- No tools are needed to install or remove the seal.
- Some versions do not require a reader, i.e., a handheld device to check the seal for tampering.
- Volumes or surfaces can be monitored, not just portals (e.g., doors and lids) as with most conventional seals.
- If desired, the seal can often be placed inside the container being monitored for tampering. This means that:
    + The seal can be used as a "trap" (covert seal) because there is no external evidence that tamper detection is underway.
    + The seal is protected from inadvertent damage.
    + The seal may not have to be removed to open the container.
    + It may be possible to check the seal for unauthorized

access multiple times from outside, without opening the container.

- Anti-gundecking: We can automatically verify that the seal inspector actually inspected the seal (rather than just reporting that he did) by not telling him what the anti-evidence is in advance. This is particularly important advantage over conventional seals, especially for cargo security. ("Gundecking" is an old navy term for shirking one's duties.)

The anti-evidence approach also has important advantages for real time intrusion monitoring, especially for cargo security and so-called "smart containers". Such a real-time, anti-evidence approach is called "Town Crier Monitoring" and has been discussed in detail elsewhere.[13,14]

Seal #1 - Time Trap

The Time Trap is a type of electronic anti-evidence seal that does not require a reader. The battery-powered Time Trap prototype shown in figure 4 uses a Microchip 16F819 microprocessor. It is programmed using microEngineering Labs' PicBasic Pro compiler, along with Mecanique's MicroCode Studio Integrated Development Environment.

The microprocessor is programmed to compute a new hash value each minute that the seal is in use. (Roughly speaking, a "hash value" is a fixed length number computed from a larger number in a complex and irreversible manner.[9,12]) While monitoring takes place, the seal shows nothing on its liquid crystal display (LCD). This saves battery power, and helps to limit an adversary's potential understanding of the hash algorithm.

Once the seal detects that the container has been opened (by either the good guys or the bad guys), it immediately erases both the secret key (in a few μsecs) used by the hash algorithm and parts of the hash algorithm itself (in a few msecs). This erasure prevents an intruder from being able to predict future hash values. After erasure, the display permanently shows the time that the container was opened and the (previously computed) hash value associated with that time. The displayed hash value is of no help in determining future hash values, so intruders will not be able to determine what hash value should be on the display when the good guys later open the container.

The seal inspector can conclude that unauthorized access did NOT occur if the time and corresponding hash value is correct. Hash values can be checked using a computer program or a hand-held microprocessor circuit. Alternatively, the seal inspector can report the time and hash back to headquarters for checking. A secure communication channel is not necessary, because an adversary cannot tamper with the communication in a way that hides the evidence of tampering.

The secret key (K) used by the hash algorithm is different each time the seal is used. Knowing the hash algorithm is of little help to an adversary if he does not also know the secret key. Even if an adversary fully understands the hash algorithm—which ought to be unlikely—he only has a 0.25% chance of guessing the correct K value based on seeing one hash value. This is because, on average, 400 different K values produce the same hash value for a given time.

The secret key (K, in the range 00001 to 65535) is randomly chosen by the seal each time it is powered up, based on the exact microsecond when the user presses the start button. There are, however, many other possible ways to choose the key (or even reprogram a new hash algorithm) with each new seal usage. The key (and/or hash algorithm) could be communicated to the seal including using infrared, radio frequency, or acoustic signals, or else via USB flash memory. A new hash key could also be entered manually using a detachable mechanical keypad, or by using a button and the LCD on the Time Trap to manually scroll through possible keys or key digits.

Rather than literally being a number, the hash value displayed by our prototype Time Trap consists of 2 letters ("RF" for the example shown in figure 4). Each letter in the two-letter hash is chosen from a set of 13 possible letters. The set of possible letters for English speakers is {AEFGHKLMRSUWX}. These letters were selected because they sound and look distinct from among all 26 letters of the alphabet. Also, we wanted to avoid the letters I and O because they can be confused with the digits zero and one. A different set of 13 letters is used for other languages, e.g., {AEFJMRTUVWXYZ} for German and {GHJKMQRSTWXYZ} for Spanish.

With two-letters, each chosen from 13 possibilities, the odds than an adversary can guess the correct hash value is 1 in 13x13 = 0.59%. (He only gets one chance.)

The prototype in figure 4 reports the time and hash value via a LCD. For this prototype, these values are read visually. The seal, however, could easily be designed to report the time and hash other ways such as via direct electrical contact, or using non-contact means such as infrared, radio frequency, or acoustic signals.

The prototype Time Trap shown in figure 4 requires $8 of parts, in quantities of 1. (Throughout this paper, all costs are for retail quantities of 1. The cost of parts drops rapidly when purchased in quantity.) For this price, the seal includes a light sensor to detect opening of the container. This works well when the container is light-tight or nearly light-tight. The seal also monitors its battery voltage, and will instantly erase the anti-evidence should the battery voltage drop below a certain threshold. This feature is needed because certain attacks on electronic seals involve removing the battery or slowly reducing its voltage. (Battery failure cannot be reliably distinguished from tampering in any electronic seal.) In addition, the seal monitors for rapid or extreme changes in temperature that might indicate a thermal attack on the seal or battery.

When the Time Trap first starts monitoring inside the container, it measures the background light level, battery voltage, and temperature. These baseline levels are used to compute the threshold levels for deciding that tampering has occurred.

At additional cost, the prototype Time Trap in figure 4 can monitor up to 14 additional sensors simultaneously. When multiple sensors are used, they are polled in a random, unpredictable, constantly changing order so that an adversary cannot predict when a given sensor will be read by the seal.

We have demonstrated a number of different sensors that can work with the Time Trap. A number of these would allow the Time Trap to be attached to a container hasp on the outside of the container, instead of working from within the container. One interesting sensor [15] is a small, solid-state Hall Effect magnetic sensor (Honeywell SS94, ~$13 each). This sensor can monitor the opening of a container lid or a truck door. A small permanent magnet is placed on the lid or door; when opened, the Hall Effect sensor detects the change in magnetic field caused by the movement of the magnet. Unlike simple magnetic door switches, the Hall Effect sensor cannot be easily spoofed by just bringing another magnet close. This is due to its high sensitivity, approximately 200 nanoTesla (nT). (By way of comparison, the Earth's magnetic field at the surface is about 55,000 nT.) Exactly the same magnetic field strength must be detected by the sensor at all times—something very difficult for an adversary to achieve with an arbitrary magnet.

Changes in the magnetic vector as a moving transport vehicle changes orientation with respect to the Earth's field can either be ignored by raising the alarm threshold of the seal, or by correcting for the apparent change in the Earth's field using a second Hall Effect sensor located far from the magnet on the lid or door. If a magnet is placed on the assets of interest instead of the lid or door, then the Hall Effect sensor can detect the removal or movement of the assets if it is sufficiently close.

Another sensor [16] that can be used with the time trap is a solid-state tilt sensor (accelerometer) with 0.001g resolution (MEMSIC MXD2020E/FL, ~$9 each). If one of these sensors is placed on the container lid or vehicle door, and another is placed on a nearby perpendicular surface, they can be compared to tell when the lid or door has been opened as compared to jostling from overall movement of the container or vehicle.

A miniature Passive Infrared (PIR) sensor can also be used to detect the presence of people or a human hand. These typically cost $2 to $5 each and cover the thermal ir wavelength range 7 to 14 μm. Inexpensive ultrasonic motion detectors also work fairly reliably if used inside a closed container.

A solid-state colorimetric sensor [17] described in the section on the Tie-Dye Seal can also be very effective at detecting tampering or movement of assets, lids, or doors.

Seal #2 - Blinking Lights Seal

Figure 5 shows an even less expensive type of anti-evidence seal, which we call the Blinking Lights Seal. It consists of 5 light emitting diodes (LEDs), 5 push buttons, one or more sensors, and batteries. The 5 LEDs are labeled 1 through 5, as are the 5 push buttons. The version shown in Figure 5 uses a light sensor and requires less than $5 in parts.

Like the Time Trap, this seal requires no reader, and is typically placed inside the container to be monitored for unauthorized access. It can use the same sensors as the Time Trap. Also like the Time Trap, the Blinking Lights Seal can be checked for tampering after opening the container—unlike most conventional seals.

When the Blinking Lights Seal is first turned on, it chooses two random numbers: a password and an "anti-evidence" number. Like the Time Trap, these are chosen based on the exact microsecond that the user pushes a start button. Each number has 25 possible values, and is a 2-digit number of the form xy, where x={1,2,3,4,5} and y={1,2,3,4,5}. Prior to inserting the seal into a container, the password and anti-evidence are displayed by using the LEDs to blink the 4 digits. For example, if the password was 33 and the anti-evidence was 54, the seal would blink the sequence 3-3-5-4 continuously until the user is ready to insert the seal into the container to be monitored. Both the password and the anti-evidence must be recorded by the seal user so that they can be checked at seal inspection time.

At inspection time, the seal user first opens the container. She then has 1 minute to enter the correct password into the seal by using the buttons on the seal. (This 1-minute time period can be modified, if desired.) If she fails to enter a password within 1 minute, the seal erases the password and anti-evidence. It then indefinitely repeats a pattern of blinking LEDs that indicates that the seal has gone "offline". (A seal inspector that encounters the offline mode immediately upon opening the container knows that unauthorized access has previously occurred.)

If the seal inspector *does* enter the correct 2-digit password within 1 minute AND the container has not been previously opened, the seal then flashes the correct 2-digit anti-evidence for a period of 1 minute. This indicates that no previous unauthorized access has occurred. After that, the seal goes into offline mode.

If the bad guys enter the wrong password into the seal—and they only get one chance—the seal instantly erases the correct anti-evidence (in a few *μ*secs) and flashes two phony digits instead of the correct anti-evidence. The bad guys, however, cannot tell the true anti-evidence from the fake. They have only a 1 in 25 (4%) chance of correctly guessing either the password, or the anti-evidence to program into the seal or a counterfeit seal in order to fool the seal inspector. Reduced odds are possible by adding more LEDs and/or buttons to the seal, or by using a LCD such as on the Time Trap instead of LEDs. Doing this, however, would increase the cost of the seal.

Seal #3 - Saturated Response Blinking Lights Seal

Figures 6 and 7 show a "saturated response" version of the previous seal.[12] It uses a two-dimensional array of 16 LEDs driven by a microprocessor. At inspection time, the seal unleashes a high bandwidth stream of data based on a complex, temporally-varying flashing pattern of LEDs. Hidden somewhere in the data is one or a few bits that represent the anti-evidence, but the bad guys don't know which they are. This bit or bits tells the seal inspector whether the container has been opened previously. All the other data is just random noise.

The punch card shown in figures 6 and 7 is but one possible way for the seal inspector to interpret the blinking lights. It is designed to slide into a slot in front of the two-dimensional array of LEDs. (Each seal, and possibly each shipment, has a different card.) This card allows the seal inspector to focus on (for example) just 3 of the blinking LEDs. The lack of previous tampering can be indicated a number of different ways (otherwise tampering is indicated). Here are just a few of the possibilities:

- All 3 of the LEDs turn on or off in unison.
- The 3 LEDs turn on and off in sequence.
- The first LED blinks once, the second one twice, the third one

three times.
- If the LEDs are 3-color LEDs, they all show the same color simultaneously.

If desired, the card can be punched out just minutes before it is needed, based on information securely transmitted to the cargo's destination.

An adversary who does not know which of the LEDs are relevant is faced with a complex two-dimensionally array of rapidly blinking lights. To try to hide the fact that he has previously gained unauthorized access, he can record the complete pattern of blinking lights, then program the original seal or a counterfeit to replay that same pattern. This is certainly possible, but it requires at least some capability in electronics and microprocessors, plus it may not be easy to do rapidly in the field.

For extra security, a password may be required as with the previous seal. If the wrong password is entered, a complex light display still occurs, but the anti-evidence is long gone.

Seal #4 - Talking Truck Cargo Seal

Figure 8 shows a working prototype of another kind of password anti-evidence seal called the Talking Truck Cargo Seal. The unit at the right of the figure is the handheld unit, which remains outside the truck (or container) being monitored for unauthorized access. It can communicate with up to 1000 different seals using 434 MHz radio frequency (rf) signals.

The unit at the bottom of figure 8 is the actual tamper-indicating seal that goes inside the truck (or container) to be monitored. It includes a light sensor like our prototype Time Trap. When the seal first starts monitoring, it will verbally complain to the seal installer if the background light level inside the container is too high, or if the battery voltage is too low for sustained monitoring.) The seal can also simultaneously poll up to 12 additional intrusion sensors, including those discussed in the section on the Time Trap.

Our prototype talking truck cargo seals were designed for a fictitious trucking company called “Near Miss Trucking”. For one version of the seal, the anti-evidence consists of one randomly chosen slogan out of 135 possible slogans used by Near Miss Trucking Company. These slogans are not secret. In fact, it is advantageous if the seal inspectors are quite familiar with all the slogans. What is kept secret is exactly which slogan was chosen for each shipment. A new, random choice of slogan is made (by the handheld unit) each time a seal is reused.

After the container or truck is closed up, the handheld unit in figure 8 chooses the secret, random 4-byte password and one of the slogans. This information is transmitted by rf to the seal inside the truck through the truck wall (even if metal). The seal then stores it until unauthorized access is detected.

The secret password and slogan chosen by the handheld unit can be duplicated or read out a variety of ways so that the secret information can be sent (using encryption or a secure communications channel) to the cargo’s destination where it will be needed for seal inspection. Alternately, the original handheld unit can be physically transported to the cargo’s destination, or else the seal inspector can simply report back to headquarters which slogan was heard.

The version in figure 8 has the handheld unit speak the slogan through a built-in speaker, although an earphone can also be used in noisy environments. Other versions of the Talking Truck Cargo Seal have the truck itself do the speaking. This simply requires that a small speaker be added to the seal, or to the inside or outside wall of the truck. We use a digitally recorded human voice, rather than synthesized speech because this makes the slogan easier to understand. The slogan is repeated 3 times to be sure it is heard.

Only if the correct password is sent by the handheld unit to the seal in the correct rf format AND if there was no unauthorized access, will the correct slogan be spoken at inspection time. Otherwise, a different slogan is spoken so as not to tip off the bad guys that their intrusion was detected. For ease of use, the inspector can check off which slogan was heard from an alphabetized checklist of the 135 possible slogans on a clipboard.

Having a spoken slogan keeps the seal inspection process at a very human level. This is advantageous from a psychological standpoint. Too often, automated high-tech seal readers distract the seal inspectors, or mentally remove them from personal involvement in the details of the shipment. This is not conducive to good security.

Examples of the Near Miss Trucking slogans—some admittedly facetious—that we use in our prototype include:

- The "go" in cargo.
- We'll make it fit!
- Sleep, what's that?
- We eat our road kill.
- Fewer felons work for us.
- The center lane marker is only a suggestion.
- At least one fire extinguisher per dozen trucks.

With 135 possible slogans, an adversary has a 1 in 135 (0.7%) chance of guessing the correct slogan. Then he must program the original seal or a counterfeit to say the correct slogan when the secret password is presented. He does not get a second chance. If even better odds are desired, up to 4000 possible slogans can be stored in the seal.

We also have a "food" version that says 3 different kinds of food out of 256 possibilities. Thus, if the inspector hears, for example, "hamburger-waffles-bananas" he can be assured there was no tampering, but if he hears 3 other foods (or nothing), then unauthorized access is indicated. With 256 possible food choices, the odds of an adversary correctly guessing the 3 foods in the correct order is approximately 1 in 17 million. (One disadvantage to this version of the seal is that it tends to make the user hungry!)

Seal #5 - Tie-Dye Seal

Color can be a difficult property to accurately counterfeit, thus making it of interest for tamper detection. Recently, small, inexpensive solid-state color sensors with remarkable color resolution have become commercially available. These perform precise color measurements that were previously available only with expensive colorimeters or spectrophotometers. For example, the TAOS TCS230 color sensor [17] outputs RGB color values from an electronics package approximately 5 x 6 x 1.7 mm in size. The sensors costs $3.50 to $5.70 each.

Figure 9 shows a prototype Tie-Dye Bolt Seal that exploits this color sensor. The color sensor is placed inside the hollow body of the seal and rigidly mounted. A white LED is used to provide illumination inside the seal. This does not need to run continuously, but can instead be turned on a random, unpredictable times so that a color spectrum can be measured intermittently (thus extending battery life).

The inside of the seal is painted with a complex varying color pattern, not unlike the “tie-dye” T-shirts popular in the 1960’s. Because this interior color pattern is so complex, it is difficult for an adversary to counterfeit it in order to try to defeat the seal. Moreover, any opening of the seal, or relative movement of the colored background with respect to the color sensor, is instantly detected as a substantial change in the color spectrum. (This might not be the case if the background was uniformly colored.) Moreover, any object such as a pick tool or drill bit, even if quite small, that passes between the color sensor and the colored background will also cause a change in the color spectrum. There is no one color that the tool could be painted that would allow it to blend into the background as it moves. In addition, any ambient light that is allowed inside the seal when the seal is opened or cut open will also be detected by the color sensor.

To make things even more difficult for an adversary, we can use 3 different LEDs, one red, one green, and one blue to provide the illumination inside the seal. They will be turned on in unison at random, unpredictable times to allow a color measurement. Each time they are turned on, however, each LED will have its own random intensity. Thus, the color spectrum seen by the color sensor at any given time cannot be easily predicted by the adversary in advance.

The microprocessor in the seal, on the other hand, can calculate the expected color spectrum for any combination of LED intensities. This is because it has run through color calibration curves (when the seal was first installed) by illuminating each LED one at a time. This is a luxury not available to the adversary.

To spoof the color sensor, an adversary needs to measure the intensity of the 3 different LEDs, then figure out what color spectrum to counterfeit. This must be repeated each time the LEDs light up.

Our prototype Tie-Dye Bolt Seal is a password anti-evidence seal. The reader shown in figure 9 plugs into a phono plug in the bolt seal. At startup time, the reader chooses the seal password and anti-evidence, then communicates them to the seal. For inspecting the seal, the reader is again plugged into the seal. A red or green LED on the reader then indicates tampering or no tampering, respectively.

Note that the Tie-Dye approach doesn't need to be limited to the interior of a seal. The concept can be scaled up to large containers, or even entire vaults or cargo-holds. Figure 10 shows a combination Tie-Dye seal and Time Trap that detects an attempt to rotate a doorknob.

Summary

Table 2 summarizes various aspects of the 5 electronic, anti-evidence seals presented in this paper.

Column 3 contains our estimate for the level of security offered by each seal, compared to the relatively low levels of security offered by conventional seals. These estimates are only speculation—although speculation based on our considerable experience with conducting vulnerability assessments on conventional tamper-indicating seals.[9-12] The problem with estimating levels of security is that none of these seals is fully developed, yet vulnerabilities depend critically on exact details of the design, how the seal is to be used, and for what applications.[10,11]

Disclaimer

The views expressed here are those of the authors and should not necessarily be ascribed to LANL or the United States Department of Energy.

Table 1 - Summary of the fastest attacks for 244 different seals. The mean is the average value. The median is the midpoint—half the seals fall below that value, and half lie above it. The marginal cost of an attack is the cost to attack another seal of the same design by reusing the attack tools and supplies.

parameter	**mean**	**median**
attack time	1.4 mins	43 secs
cost of tools & supplies	$78	$5
marginal cost of attack	62¢	9¢
time to devise the attack	2.3 hrs	12 mins

Table 2 - Summary of the Electronic Anti-Evidence Seals Discussed in This Paper.

Seal	Type of Anti-Evidence Seal	Level of Security	seal cost*	reader cost*
Time Trap	hash	high	$8	N/A
Blinking Lights Seal	password	medium	$5	N/A
Saturated Response Blinking Lights Seal	saturated response/password	medium	$7	N/A
Talking Truck Cargo Seal	password	high	$20	$45
Tie-Dye Seal	password	medium to high	$12	$6

* This is the cost for parts only, in retail quantities of 1. Costs may be higher with more or different sensors.

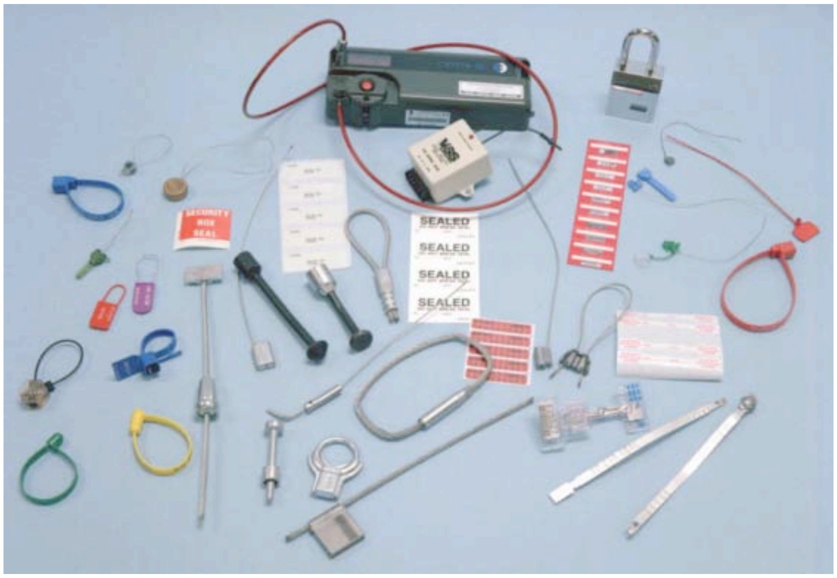

Fig 1 - Some examples of commercial tamper-indicating seals.

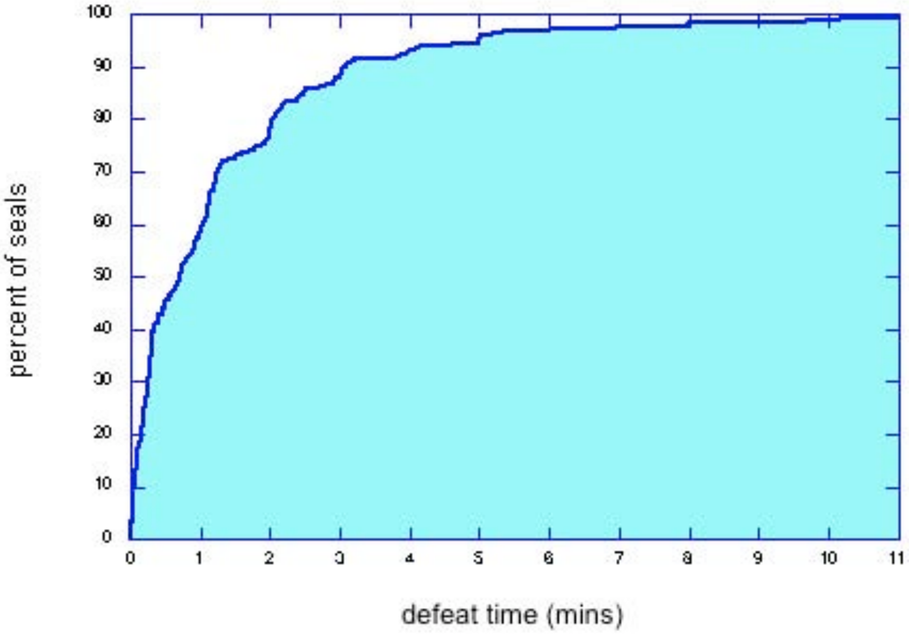

Fig 2 - Percent of seals that can be defeated in less than a given amount of time by 1 person. For some seals, an assistant would decrease the defeat times plotted here, but for others, an assistant just gets in the way.

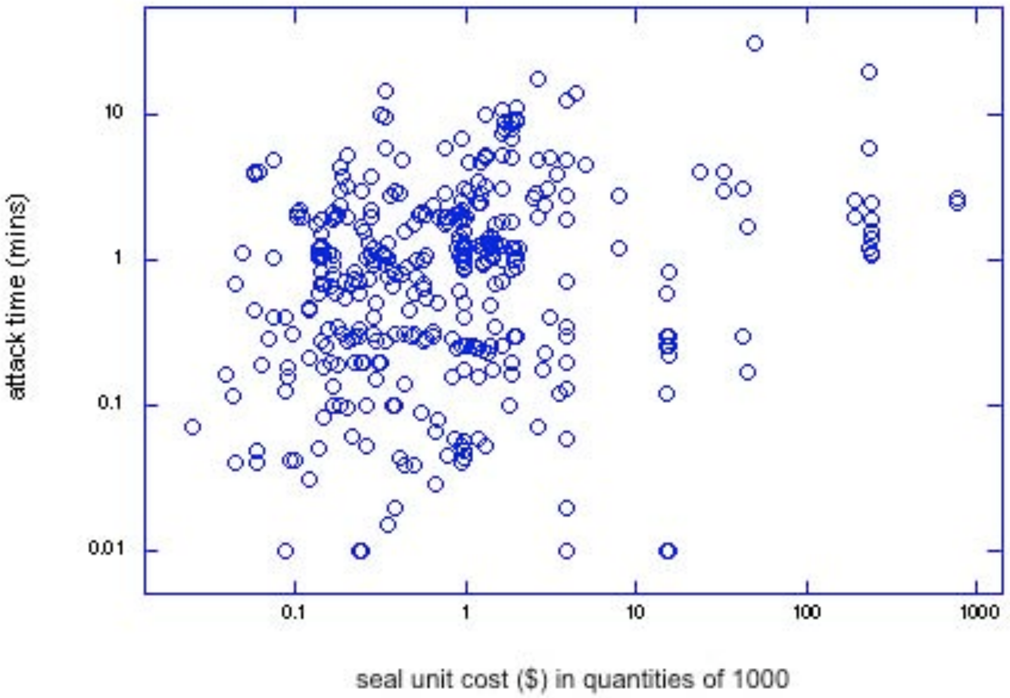

Fig 3 - Log-log plot of defeat time vs. seal cost (in quantities of 1000) for 393 different attacks on 244 seals, 1 to 8 distinct successful attacks per seal.

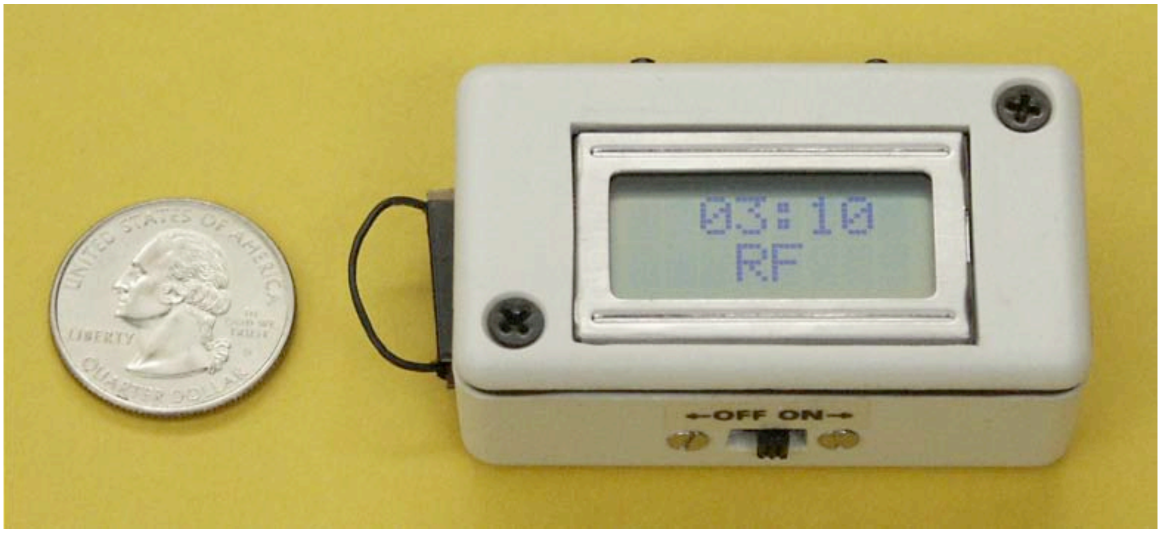

Fig 4 - Prototype Time Trap. When the container is opened, the time trap erases the secret key used by the hash algorithm, and then the time trap shows the time when the container was opened (elapsed or Greenwich Mean Time) and the 2-letter hash associated with that time ("RF" in the photo). In this photo, the container was opened 3 hours and 12 minutes after tamper monitoring began. Like the other (reusable) electronic seals described in this paper, the Time Trap has an adjustable countdown time when first powered up to allow the seal user to close the container or exit the transport vehicle before monitoring begins.

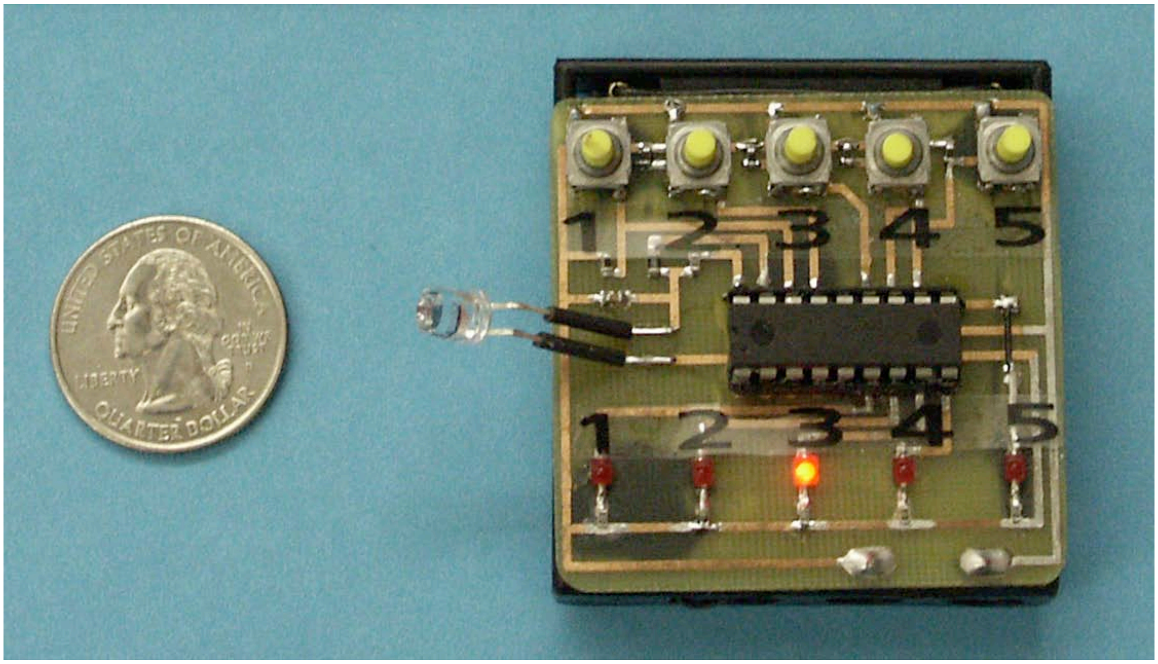

Fig 5 - Prototype Blinking Lights Seal.

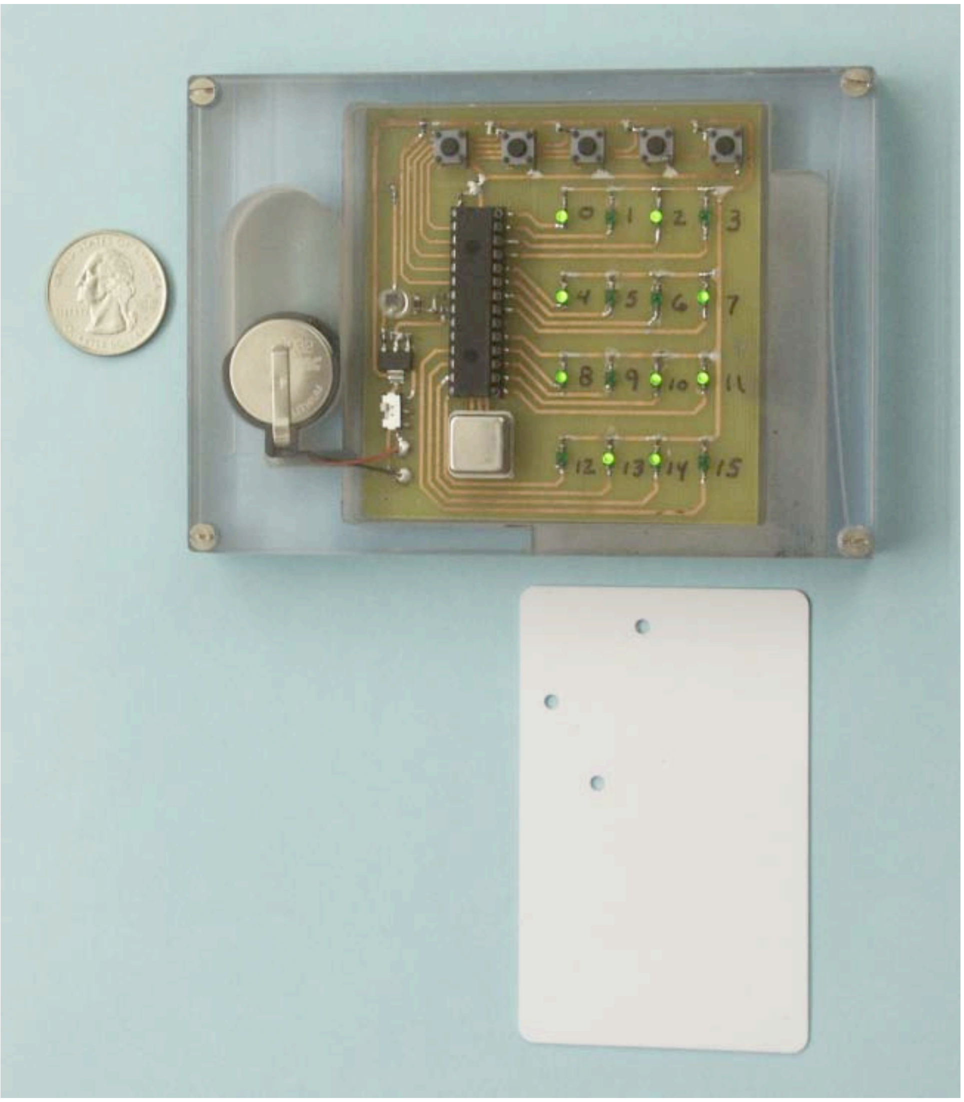

Fig 6 - A Saturated Response Blinking Lights Seal. A complex pattern of rapidly changing LED lights is displayed at inspection time. The punch card, shown below the seal, is used to focus on the LEDs that matter, as shown in the next figure.

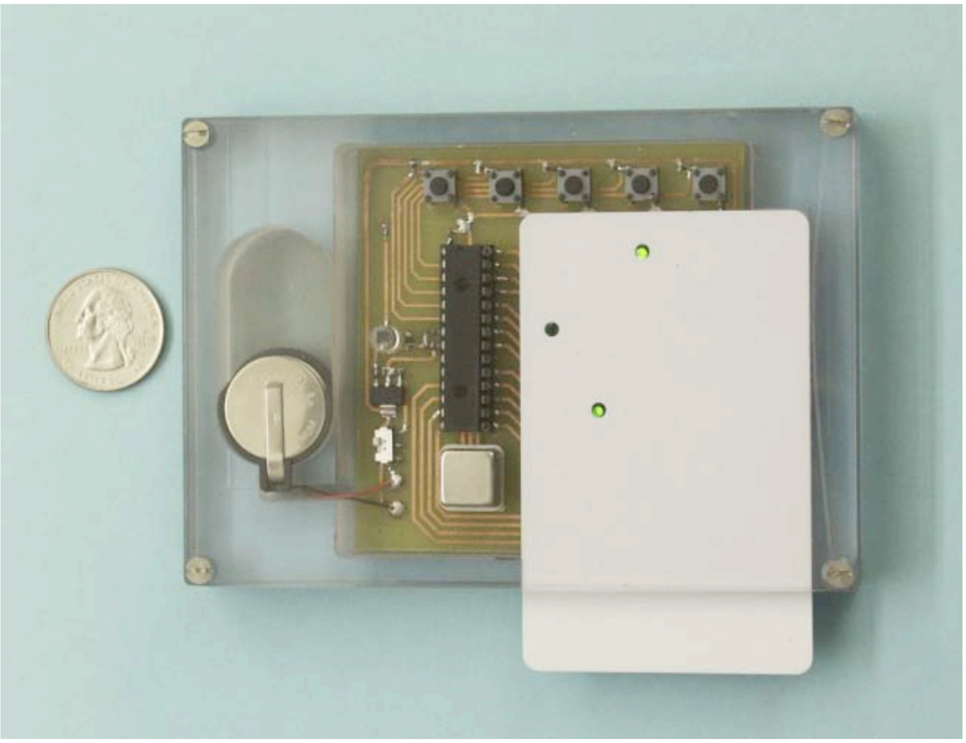

Fig 7 - Reading the Saturated Response Blinking Lights Seal. The appropriate punch card for this seal slides into a slot so that the seal inspector will view only the relevant LEDs. (Which ones are relevant is a secret.) The sequential illumination pattern of the 3 visible LEDs tells the inspector whether tampering has occurred.

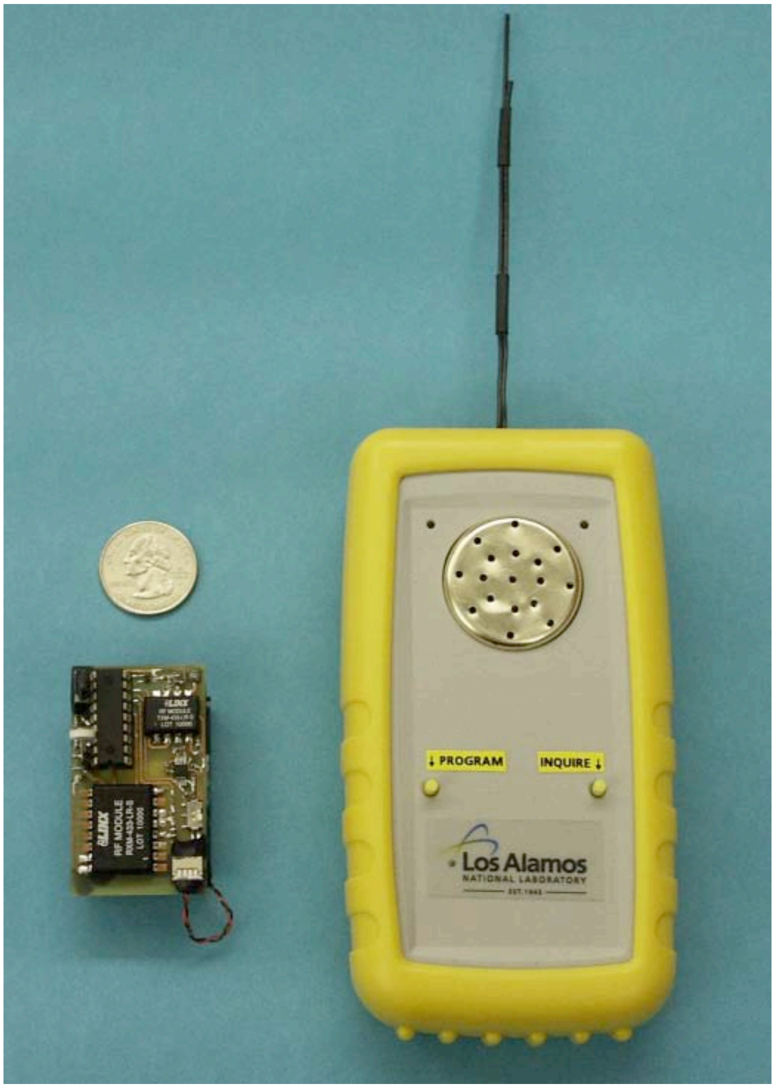

Fig 8 - Prototype Talking Truck Cargo Seal. The prototype seal (left) is placed inside the truck (or container) to monitor for unauthorized access, while the handheld unit (right) communicates with the seal from outside using radio frequency communication.

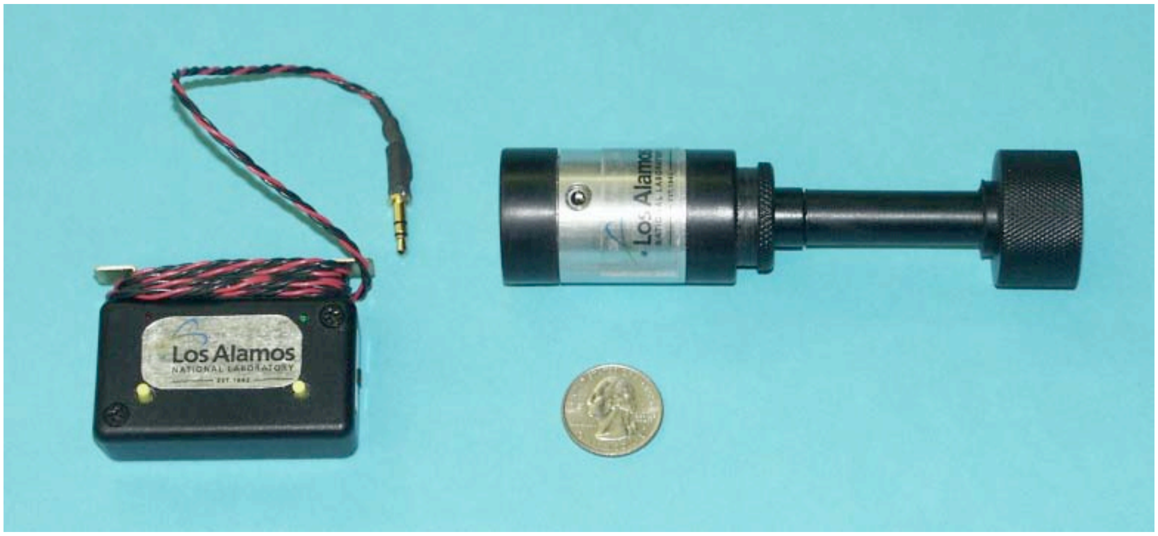

Fig 9 - Prototype Tie-Dye Bolt Seal (right) and the electronic reader (left). The two halves of the bolt seal snap together through a hasp on a door, container, or truck.

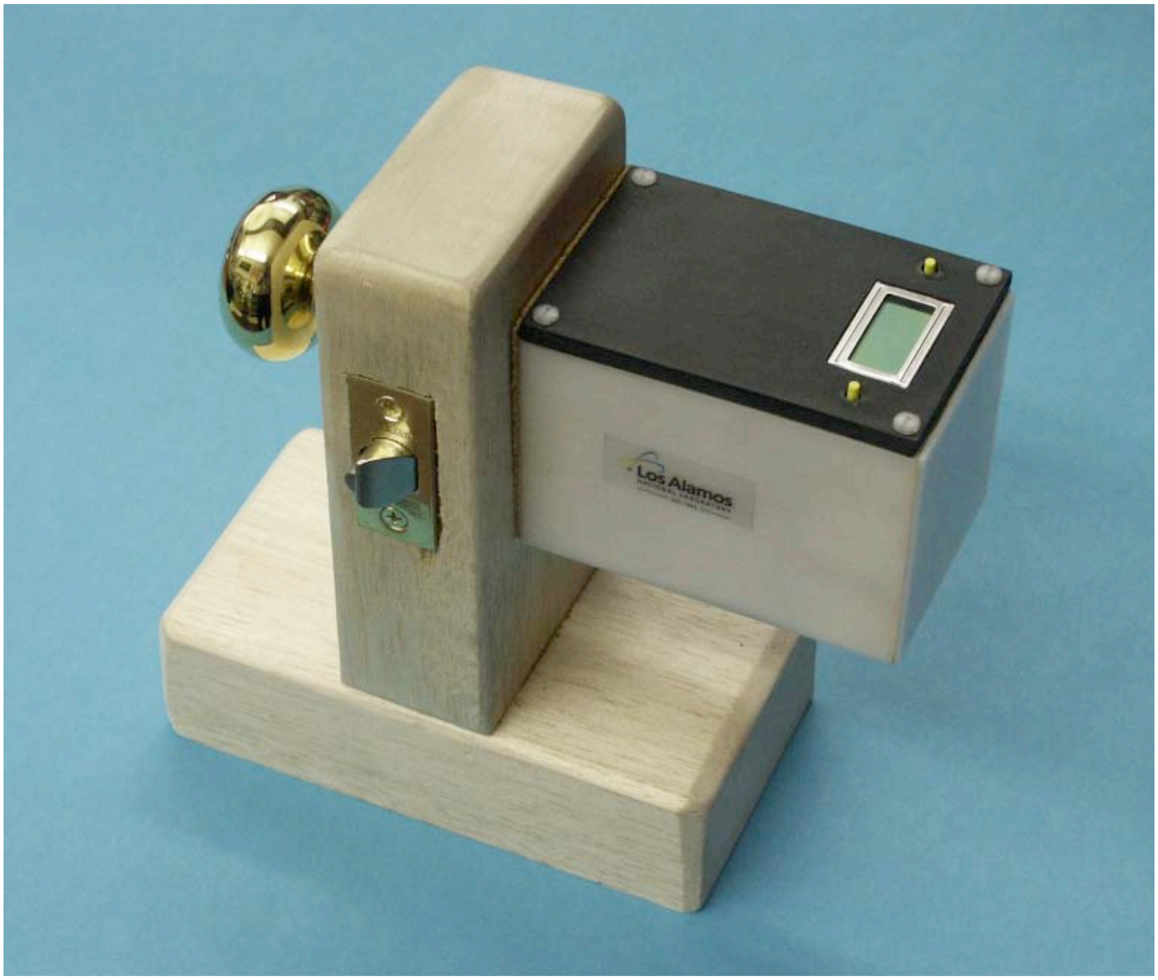

Fig 10 - A combination of the Tie-Dye Seal and Time Trap.
This box slips around the doorknob on the inside of a door. Any attempt to rotate the doorknob from the outside is irreversibly detected.

References

1. Colleen Mulcahy, “Product Tampering Explored”, *National Underwriter Property & Casualty--Risk & Benefits Management* **22**, p. 33ff, 5/29/1989.

2. Ian I. Mitroff and Ralph H. Kilmann, *Corporate Tragedies: Product Tampering, Sabotage, and Other Catastrophes* (Praeger, 1984).

3. PE Dietz, “Dangerous Information: Product Tampering and Poisoning Advice in Revenge and Murder Manuals”, *J Forensic Science* **33**(5), pp. 1206-1217 (Sept 1988).

4. “Foil The Malicious Tamperer: TE Devices Help Protect Your Products and Consumers”, *Food & Drug Packaging*, p. 14ff, 9/1/1992.

5. Park Dietz, “Product Tampering”, http://www.facsnet.org/tools/ref_tutor/tampering/prolif.php3

6. “The Pepsi Product Tampering Scam of 1993”, http://www.roadsideamerica.com/rant/pepsipanic.html

7. Kate Bertrand, “Making Tamper Evident”, *Food Processing **66**(12), pp. 38-41,* 12/1/2005.

8. Steve Ennen, “Food Security and the Facility: Foundation of Physical Plant Preparedness”, *Food Processing* **63**(5), pp. 64-66, 5/1/2002.

9. Roger G. Johnston, “New Research on Seals”, *International Utilities Revenue Protection Association (IURPA) News (*in press), Los Alamos National Laboratory Report LAUR-06-0940, February, 2006.

10. RG Johnston, “Assessing the Vulnerability of Tamper-Indicting Seals”, *Port Technology International* **25**, 155 (2005).

11. RG Johnston, ARE Garcia, and AN Pacheco, "Efficacy of Tamper-Indicating Devices", *Journal of Homeland Security*, April 16, 2002, http://www.homelandsecurity.org/journal/Articles/displayarticle.asp?article=50

12. RG Johnston, “The ‘Anti-Evidence’ Approach to Tamper-Detection”, *Packaging, Transport, Storage & Security of Radioactive Material* **16**, 135 (2005).

13. Johnston, R.G., Garcia, A.R.E., and Pacheco, A.N., “Improved Security via 'Town Crier' Monitoring”, *Proceedings of the Waste Management Conference* (WM’03), Tucson, AZ, February 23-27, 2003.

14. Johnston, R.G., Garcia, A.R.E., and Pacheco, A.N., “The 'Town Crier' Approach to Monitoring”, *International Journal of Radioactive Material Transport* 13, 117-126 (2002).

15. Honeywell SS94A1, http://catalog.sensing.honeywell.com/printfriendly.asp?FAM=solidstate&PN=SS94A1

16. Memsic, http://www.memsic.com/memsic/products/productselector.asp

17. Texas Advanced Optoelectronic Solutions (TAOS), http://www.taosinc.com/product_detail.asp?cateid=11&proid=12