How To Steal A Nuclear Bomb, Without Voiding Your Xbox Warranty

E. C. E. Michaud, I11 Industries LLC, eric@i11industries.com
J. E. H. Schwettmann, I11 Industries LLC, jamie@i11industries.com

Abstract

We will present the common elements and basic mechanisms of modern tamper-evident seals, tags, and labels, with emphasis on attack and circumvention. Adhesive seals, crimp seals, wire wraps, fiber optic seals, electronic, chemical, biological, and make-shift seals will be dissected, examined, and explained, with emphasis on their shortcomings and circumvention techniques. We will also present an overview of typical applications for tags, seals, and labels, including covert traps and uses ranging from consumer goods to loss reduction to government secrets.

I. Introduction

Tamper-evident devices have appeared throughout history in myriad forms, from a hair left hanging in a door jam to the wax seals and dignitary signets used on letters, scrolls, and official documents in ancient Rome. Today, while these ancient forms persist, many thousands of new devices have come into modern circulation, making a thorough study of the field a much larger endeavor than it once may have been, thereby leading to a great deal of confusion and misinformation about what constitutes a tamper-evident device, and what limitations and circumventions may exist when employing such. Fortunately, we can define it thus:

> **Tamper-evident device:**
> Any tag, seal, alarm or other indicator which can be employed to evidence unauthorized intrusion or alteration to a container, room, building, device housing, or other material. Materials secured by such such devices are often said to be “sealed”.

The advent of hyper-globalization and consumerism has resulted in billions of products being shipped around the world and across continents before reaching their final destinations in our homes and businesses. Coupled with advances in science, medicine, and technology, quality assurance has become an increasingly important focus of producers and consumers. Many governments have instituted regulatory measures requiring the use of tamper-evident devices for food and medical goods, as well as to verify taxes and tariffs, and many industries have self-adopted similar measures, often to the dismay of consumers. In fact, tamper-evident devices have found their way into the entire production chain, and several new ISO standards have recently been drafted in an effort to regulate the quality of the devices themselves.

Consider the production chain for a modern cell phone. At the factory where the boards are assembled, workers diligently slap stickers across key screws as they assemble the components into the housing, and then a glue may be used on the housing itself. The phones are often individually wrapped in plastic, with another sticker or glue sealing the wrapping, and then placed in a box which itself is marked with stickers across the opening flaps before it is shrink-wrapped with plastic. A carton or crate of these boxes may itself be wrapped again in plastic before being packed into a larger container, which is locked and tagged before it departs by air or sea. The section of the boat or plane it is placed into may have an alarm on the door as well. Each of these wrappings, stickers, tags, and alarms are designed to alert someone – whether it's the producer, consumer, shipping provider, insurer, or government agent – that the contents may have been altered.

An important distinction must be made between tamper-*evident,* tamper-*resistant,* and tamper-*proof* devices. In general, no device is tamper-proof, despite what manufacturers may claim. Tamper-evident and tamper-resistant often mean the same thing. Tamper-evident devices can further be distinguished from locks in that, unlike locks, they are generally designed and intended to be single-use, rather than opened with a specialized key and possibly resealed later.

Tampering cannot often be prevented, but it may potentially be detected. The security given by any tamper-evident device lies only in the potential knowledge that a material thus secured has been accessed or altered, and the diligence with which such knowledge is obtained. Thus, circumvention of tamper-evident devices relies primarily upon exploiting the limitations of an examiner to accurately detect that tampering has occurred.

Because of the involvement of an examiner to the process of exploitation, covert circumvention may not always require dealing directly with the supposed tamper-evident device. However, this paper will primarily cover the devices themselves. With this in mind, we will present first an overview of inspection techniques, followed by a general categorization of devices alongside direct circumvention strategies for each.

II. Inspection Techniques

Inspection techniques range from casual observation to detailed, scientific examination of devices.

Obviously anyone, regardless of training or tools, can tell when a piece of tape has been ruptured, a sticker has left behind bits of adhesive or perforated words such as “VOID”, or a pill-bubble has been broken. As such, simple observation is always the first line of defense in determining whether tampering has occurred. Here, the examiner will look for overt signs of tampering, such as breakage, leakage, tearing, staining, discoloration, dislocation of tabs and flanges, punctures, or recorded electronic evidence. Casual observation methods are the easiest to circumvent, as the examiner may simply overlook minute discrepancies.

If more thorough checking is required, a simple and important method often employed is **blink comparison**. With this method, the original sealer of the material will take a high-resolution photograph of the material and/or its seal, such that the examiner can take a second photograph and compare with the first for discrepancies. Depending on the level of security required and likely movement occurring during expected handling of the material, blink comparison can provide crucial information to the possibility that tampering may have occurred, even without an explicit tamper-evident device in place. Blink comparison is considerably more difficult to circumvent, since absolutely all changes will be observed, within the resolution limitations of the images. To covertly avoid detection from this method, it is important that any discrepancy can be rationalized by the examiner as “normal use”.

For yet more in-depth verification, a combination of blink-comparison and optical microscopic, X-ray, UV, IR, scanning-tunnelling microscopic, electron microscopic, proton emission scanning, or other imaging techniques may be combined. Examiners with access to such testing equipment often also have access to chemical testing, and possibly other high-tech methods, making covert circumvention nearly impossible. Any attack aimed at covertly passing such rigorous examinations must leave absolutely no trace.

III.Types of Devices and Circumvention Strategies

Although not the only categorization scheme available, we have chosen to divide the world of tamper-evident devices into four main categories: A) Adhesives, Inks, and Sealants, B) Wraps, Crimps, and Physical Barriers, C) Optical Seals, Electronic Devices, and Alarms D) Other Unique Devices. Many available devices are likely to be hybrids of these categories, and thus may not fall neatly into any one of them. Still, the circumvention methods outlined here should provide a comprehensive introduction to attack methods and limitations for most kinds of modern tamper-evident devices, given the type and degree of inspection that each device is likely to receive.

A. Adhesives, Inks, and Sealants

While it may not seem obvious that adhesives, inks, and sealants should be lumped together in the same family, in fact they have many striking physical similarities. Most notably, all of these tend to originate in a liquid or gel form, are typically applied to one or more layers of paper, plastic-film, and/or foil substrate(s), and leave evidence of overt tampering either through obvious visual indication of breakage or obvious visual indication of damage to the substrate(s), including residual material left behind after attempted removal.

Common examples include warranty-void stickers, auto registration and inspection stickers, wax seals, and signatures or designs inked across adjoining sections of the substrate material(s), such as postmark printing.

The trick to circumventing most of these is to find a suitable solvent or physical removal method (such as extreme temperature) for the tamper-evident material in question, which will not stain, dissolve, or mark the substrate material. This is certainly easier in principle than in practice, especially with recent developments in high-security ink and nano-bonding adhesives. (High-security versions of inks, adhesives, and sealants are more often used for forgery and fraud prevention than for tamper-evidence, but in some applications the distinction may be nominal.)

For example, a typical auto registration sticker has a strong adhesive on a plastic-film substrate which is applied to the uncoated inside of a glass windshield. The plastic of the sticker is perforated such that it becomes quite difficult to remove intact without leaving bits of the plastic-film behind. These devices are well-known to be defeatable with a hair dryer, a razor, and a steady hand. Wax seals are often circumvented similarly. Such seals are not likely to receive excessive scrutiny by examiners.

Inks, sealants, and adhesives applied to paper, such as in postage and shipping applications, present a different challenge for circumvention, since often the gel has bonded to the surface of the paper such that most kinds of removal would result in obvious damage to the paper. Here, alcohols, acids, water, or steam may be applied to aid in unbonding the adhesive or lifting the ink. The degree to which this must be accomplished covertly for inks depends heavily on the application. Official documents related to high-value items will likely receive considerably more examination than an ordinary postmark on an unimportant stamp.

Of course, if the goal of tampering is to insert a small amount of doping agent or remove a sample from the sealed material, often a thin-gauge hypodermic needle may be inserted covertly in an inconspicuous location, either through the seal or through the material itself, thus defeating the purpose of the tamper-evident device. This method of attack especially hinges upon the diligence of the examiner in searching the material for evidence of tampering, and requires significantly more examination to detect.

B. Wraps, Crimps, and other Physical Barriers

Wraps, crimps and physical barriers are also very similar types of devices. Crimps are employed as simply as their name implies, often by mechanically crimping a plastic or metal band (or wrapped wire) around a strap, wire, or other material to be tamper-evidenced, such that the strap or wire would need to be cut, or the band removed, in order to break the seal. Wraps are similar to crimps, though often no mechanical sealing takes place. Wraps may be sealed by electrostatic adhesion, an adhesive, or heat. Other physical barriers may include metal and plastic strap seals, bolt "locks", rivets, zip-ties, cable locks, plastic "padlock" seals, break-away seals, security caps, pull-tabs, dangle-tabs, cup seals, foil or plastic-film bubbles and tapes, perforated paper, and many others.

The unifying aspect of the devices in this category is that they must be *physically broken* or otherwise permanently removed to give evidence of tampering. Because of the likelihood that an examiner will make only a casual observation of a physical barrier device, most of them can be mechanically or thermally defeated, modified, covertly circumvented, or easily replaced. As such, nearly all physical barrier seals are subject to covert needle-based attacks (when sealing a material subject to such an attack) as described in the previous section.

The distinction between adhesive devices and physical barriers which employ adhesives is thin at best. Here, we distinguish the physical barrier as that which absolutely must be broken in order to evidence tampering, whereas the adhesive devices may leave behind residue or damage as evidence, even if the paper, foil, or film of the primary barrier is not broken. In this way, physical barriers employing adhesives may often be circumvented much more easily than adhesive devices, in that solvents are often not needed for removal and reattachment because the adhesive itself does not provide evidence of tampering. A simple magnifying glass is often all that is needed to tell whether a physical barrier secured by adhesive has been tampered with.

Crimps may often be circumvented by bending the crimp away from the strap or wire, and pulling such through the crimp. The crimp may then be re-crimped to reseal the device, and a heat gun may be employed in the case of any plastic discoloration. Conference wrist-ribbons attached with a metal band are a common example of crimp seals, and these often receive little scrutiny by examiners.

Wraps, on the other hand, must often be replaced if they are broken, as most cannot be reattached or reassembled in any form that resembles the original. The exception to this is a form of shrink-wrap which uses a thicker plastic-film and has minimal heat-crimping at the edges. Often these wraps can be carefully pulled apart, and reattached with minimal heat. Cigarette box wrappers provide an excellent example of such a film, and some pill-bubble foils may also be considered wraps in this context.

Strap seals, zip ties, plastic "padlock" seals, security caps, and some break-away seals (such as found on water and soda bottles) may often be defeated with a thin punch or chisel tool to bend, release, or remove the teeth holding the device together. Any marring of plastic resulting from bending can often be thermally corrected with a heat gun. Such modification may or may not be evidenced by blink-comparison, depending on the resolution and detail of the photos.

Cup seals have recently come into use for securing some of the most sensitive material in transportation and storage: fissile material and nuclear weapons. Often called "e-seals", these devices feature a nylon, carbon-fiber, or kevlar weave covering a woven steel cable which is sealed by a set of interlocking cups. These seals are often given a significant degree of scrutiny, possibly involving blink-comparison photos and examination beneath a magnifying glass, but there is still a possibility for mechanical defeat

by separating the cups and refashioning the end(s) of the cable.

Interestingly enough, the most secure seal discussed here is probably the soda can pull-tab, which today is found primarily as a dangle-tab which breaks away from the main can, but remains hanging within the open mouth. These physical barrier devices are especially genius in that the actual aluminum of the can must be breached in order to tamper with the contents. There is *no known covert attack* against this style of break-away tamper-evidencing device, and as such, most cans do not receive any scrutiny whatsoever.

C. Optical Seals, Electronic Devices, and Alarms

The characteristic feature of this category is the use of sensors and triggers, often optical, but possibly thermal, chemical, electrical, magnetic, gyroscopic, vibrational, atmospheric or barometric sensors to evidence a state change and imply the potential for tampering to have occurred. Electronic devices usually employ one or more of these sensors, and alarms generally include a visual or audio alert that a trigger has been tripped.

A common example of these are motion-detection units for use within a volume of space, which are usually triggered by a color, intensity, or pattern change in the ambient microwave, IR, or visible light level surrounding the sensor, and often result in recording beginning or ending, an alarm sounding, or other activation occurring. Beam-break sensors are another example, which rely upon a steady IR, visible laser, or fiber optic source to constantly impinge upon a receiver with expected optical characteristics. Piezo-electric, gyroscopic, and vibrational current generators are also often employed. These cause an electrical signal to be sent in the case that the secured material is shaken, tilted, or otherwise moved; and many others.

Because the inspection method for electronic devices is usually automated, there typically exists some inherent range of tolerance and sampling frequency. Would-be trigger events occurring within the tolerance range or outside the sampling frequency limitations will not be detected. Sometimes, the sensors themselves may be covertly bypassed physically or electronically, further allowing tampering to go unnoticed. Because of this, many manufacturers enhance their electronic tamper-evident devices themselves with tamper-evident sealants and barriers.

D. Other Unique Devices

Many additional types of tamper-evident devices exist which do not fit into any of the categories here, or even comprise hybrids thereof. A hair hanging in a door jam, a single colored thread woven into a fabric, a unique composition of particles surrounding a packed object, a piece of gum wedged into the back of a drawer, a hi-res photo of a circuitboard, an arrangement of leaves, the decoration on a cake... none of these find their way neatly into the other categories, but all may be considered tamper-evident devices.

IV. Designing and Using Tamper-evident Devices

As should be evident from the previous section, designing and using tamper-evident devices should involve more than simply following the manufacturer's instructions for application of stickers or tags. Rather, each application should be carefully considered and the risk and consequence of tampering appropriately weighed alongside the tamper-evident design. If significant risk is involved, and the consequence of covert unauthorized access is high, it only makes sense to choose tamper-evident

devices which will yield conclusive evidence with appropriate examination.

The blink-comparison method of examination is so often used because it is relatively easy, inexpensive, and can be used alongside a number of other evidencing devices and techniques. To be used effectively, however, the examiner must have knowledge and experience about what constitutes "normal use" of the material being secured, and how this will affect the examination. The requirement for this knowledge can be minimized by choosing tamper-evident materials which are less likely to be affected by handling. Hard plastics imbued with specific glitter, foil, or bubble patterns, or high-temperature glass with similarly imbedded features work fairly well across applications.

When choosing adhesives, inks, or sealants, it is also necessary to ensure that the gel used for tamper-evidencing is not easily removed from the material being secured. All too often, misuse of adhesives results in supposed tamper-evident devices being easily removed and replaced without any tools or experience, thus leaving these defeated by design.

The placement and specific implementation of tamper-evident devices is also of utmost importance, since an ill-placed device will simply inspire tampering of the "sealed" material elsewhere. At best, improperly used devices will provide inconclusive information regarding intrusion, and at worst, they will provide absolutely none.

V. Conclusion

A full discussion of the applications and intricacies of tamper-evident devices would require much more space than is allowed in this short paper, and indeed, may constitute volumes of future work. The information contained here should be sufficient for a basic general-purpose understanding of the nature of tamper-evident devices, including common applications, inspection techniques, and circumvention strategies. The importance of these devices, and an understanding of their risks and limitations will only increase as our global economy becomes more complex and intertwined, and the new standards are not likely to be as reliable as careful consideration and examination in determining which tamper-evident devices and methods will be best for which products and situations. With this information in hand, however, sound decisions involving tamper-evident devices can easily become an inexpensive and important part of any security policy.