How to Choose and Use Seals*

Roger G. Johnston, Ph.D., CPP and Jon S. Warner, Ph.D.
Vulnerability Assessment Team
Argonne National Laboratory

Introduction

Tamper-indicating seals have been in use for well over 7,000 years.[1,2] Today, seals are widely used for a variety of applications including cargo security, nuclear safeguards, counter-intelligence, theft detection, loss prevention, records security, employee drug testing, and election integrity.[3-11] They protect money, transportainers, footlockers, courier bags, filing cabinets, utility meters, hazardous materials, instrument calibrations, drugs, weapons, computer media, warehoused goods, and other critical items. Despite their antiquity and widespread modern use, there remain quite a few misconceptions, poor practices, and misleading terminology when it comes to seals and seal use.[12-16] This article is a brief primer on how to choose and use seals, and is based on two decades of research by the Vulnerability Assessment Team at Argonne National Laboratory.[17-22]

It's important first off to be clear on what a seal is and what it is not. (See figure 1 for an example of seals.) Unlike a lock, a seal is not intended to delay or discourage unauthorized entry (except possibly in some vague psychological sense). Instead, a seal is meant to leave behind unambiguous, non-erasable evidence of unauthorized access. Complicating the issue is the fact that there are "barrier" seals—devices that are part lock and part seal. Barrier seals have their uses, but the downside is that they cause a lot of confusion in users, and the devices tend to be a compromise, being neither the optimal lock nor the optimal seal for a given application.

Barrier seals are sometimes misleadingly called "security seals" or even "high security seals" in contrast to "indicative seals", but this is sloppy terminology. (All seals have a role to play in security, and "high security" is a value judgment, not a product attribute!) Other terminology to avoid include "tamper-proof seal" and "tamper-resistant" seal. There is no such think as a seal that cannot be spoofed, and the idea of "tamper resistance" applies more properly to locks, not seals.

Unlike a lock, cutting a seal off a container is not defeating it because the fact that the seal is damaged or missing will be noted at the time of inspection. "Defeating" or "spoofing" a seal means to open the seal, then reseal the container it is used on, <u>but without being detected</u> by the inspection process in use.[18-22] "Attacking" a seal means undertaking a sequence of actions intended to try to defeat the seal.

Seal manufacturers, vendors, and users typically over-estimate the difficulty of defeating their seals. There are at least 105 different generic methods for potentially defeating a seal.[23] These include, for example, picking the seal open without leaving evidence,

---

*Editor's Note: This paper was not peer reviewed. It originally appeared in *Army Sustainment* ***44****(4), 54-58 (2012).*

counterfeiting the seal, replicating the seal at the factory, changing the serial number, tampering with the database of seal serial numbers, drilling into the seal to allow interior manipulation then repairing the hole, cutting the seal and repairing the damage, not installing the correct seal in the first place (then later replacing it with the correct seal), etc. Full counterfeiting is usually not the most likely attack on a seal unless perhaps the adversary is attacking a large number of seals, or has very limited access time at the seal and its container.

A fundamental fact about tamper detection is that a seal is no better than its "seal use protocol".[1-6,10-12,18] This is the official and unofficial procedures for seal procurement, shipping, storage, check out, installation, inspection, training, reporting, disposal, securing the seal data (such as the recorded seal serial numbers), and securing the seal reader, if there is one. (Typically, 15 seconds of access to either the seal database or the seal reader allows an adversary to defeat 1 or many seals in one quick effort.) Modest seals used with a good seal use protocol can potentially provide good tamper detection. Sophisticated seals used poorly will not.[2,13,19-22]

Choosing & Procuring Seals

In choosing a seal, it is important to realize that there is no such thing as an unspoofable seal (any more than there is an undefeatable lock). There is also no one "best" seal. The optimal choice of a seal depends on details of your security goals, threats, adversaries, personnel and their training, as well as the nature of your containers, doors, hasps, physical facilities, and time and budget constraints.

Generally, seals that are complex, difficult to use, or that present significant ergonomic problems will be resisted by seal installers and inspectors and will not provide good security.

All seals need a unique identifier, such as a serial number, so that an adversary cannot easily swap one seal for another. Independent parts of seal should have (ideally the same) serial number. Serial numbers should not be easy to erase, dissolve, or buff out (though they often are).

Seal vendors and manufacturers (ideally) should contractually agree not to sell duplicate serial numbers or replicate logos to anybody (even within your organization!) who are not on your organization's short list of authorized seal buyers. Seal users should test if this agreement is honored. Often it is not.

If the seal is frangible, be sure to consider environmental conditions and any rough handling the seal may be receive. Also bear in mind that robust seals on moving containers can be a safety hazard in that they can gouge eyes or skin, or entrap clothing.

Seals should not be chosen based solely on unit cost. There are often much higher costs associated with seal installation, inspection, removal, and training. With reusable (typically electronic), seals, be sure to factor in the cost of unit failures, battery replacement, and theft/loss/vandalism of the seal, as well as the costs of protecting and returning the seals for re-use (if necessary).

Seal Installation

Unused seals must be carefully protected prior to use, not just left lying around a loading dock, for example. Seals should be assigned to specific individuals who are responsible for protecting and returning unused seals. Unused seals are potentially very useful to an adversary for practicing attacks, or for use in an attack.

Prior to installation, a seal should be checked for manufacturing defects and for evidence of pre-installation tampering (a "backdoor attack") which can make it easier for an adversary to open the seal later without leaving evidence.

The door, hasp, or locking mechanism, as well as all sides (and top and bottom) of the container must be inspected. It makes little sense to seal a container with gaping holes in it, or to apply a seal to a door, hasp, or locking mechanism that is faulty. (You'd be surprised, however, how often people do this!)

Seals should not be used in sequential order. Adversaries must not be able to guess a seal serial number in advance, or even a narrow range of serial numbers!

Seal Inspection & Removal

The common misconception that a seal will either be missing or blatantly smashed open, or else there has been no unauthorized access or tampering couldn't be more wrong.[9,14,21] In fact, even amateurs can attack seals in a way that leaves little (and sometimes no) evidence.[9,14,20] Only if the seal inspector has some idea of the most likely attack scenarios and knows what specifically to look for on a given seal can she detect tampering with full reliability. Simply checking to see if the seal is intact and maybe has the right serial number is of limited usefulness, unless you are sure there is no potential adversary with an interest in attacking surreptitiously. (A seal is called a "flag seal" when there is no concern about a surreptitious attack. A flag seals is often used to signal an employee not to unnecessarily reprocess a container. It differs from a "tamper-indicating seal" which is meant to deal with covert tampering or intrusion attempts.)

Seal inspectors should have training on the vulnerabilities and most likely attack scenarios for the seals they are using in the context they are using them. They should have hands-on practice detecting seals attacked both blatantly and subtly. Without this training, they cannot do the best job of detecting tampering.

A seal must be inspected carefully before it is removed, as well as after. Before removing the seal, the seal inspector should also check that the seal displays the right amount of movement or "play" between any 2 mated parts.

Seal inspectors should always compare a seal side-by-side with a protected, unused ("control") seal of the same kind. See figure 2. (This is true even for seals read at a distance with an automated reader.) People are fairly proficient at side-by-side comparisons but not very good at remembering exact details, even for familiar objects.. The seal inspector should

compare the seal color, gloss, surface finish, size, and morphology, and also check the serial number size, font, feel, and character alignment.

Seals should be inspected for evidence of repair or cosmetic coverups of holes or cuts. Smelling the seal—especially as it is being opened—is often remarkably effective in detecting the presence of epoxies, adhesives, paints, inks, solvents, or coatings that have been applied to the seal (even months earlier) by an adversary to hide an attack. Alternately, relatively inexpensive, hand-held electronic sensors can detect many of the same chemicals. If there is time during the inspection, rubbing the seal with a wire brush and/or solvent can be very effective at detecting certain kinds of counterfeit seals or seals that have been repaired.

The door, hasp, or locking mechanism of the container, as well as its sides, top, bottom, and ideally insides must be inspected as well to reliably detect tampering.

After a seal is removed, used seal parts must be protected or thoroughly destroyed so that they cannot be used by an adversary for practicing or executing seal attacks. Ideally, the used seals and seal parts should be saved for some period of time to allow a forensics examination should questions arise.

The best seal inspectors seem to have an uncanny sense that something is suspicious about a seal without necessarily knowing what. Such intuition should never be discounted. Security managers should also make sure that seal inspectors are not hesitant to report their concerns. Sometimes the consternation and delays that a suspicious seal creates for superiors, security personnel, and logistics managers makes front-line employees hesitant to raise their concerns.

Seal inspectors should be occasionally tested with deliberately attacked seals, then heartily rewarded if they detect them. This should include both seals blatantly attacked, and seals attacked with more subtle methods.

Pressure Sensitive Adhesive Label Seals

After having studied hundreds of such seals, we have concluded that pressure sensitive, adhesive label seals do not generally provide reliable tamper detection. People like using these "sticky labels" because they are inexpensive and appear superficially to be easy to install and inspect. They are, however, typically easy even for amateurs to defeat.

If you insist on using adhesive label seals anyway, here are some suggestions:

1. Match the type of adhesive to the surface. The best adhesive for bare metal is not necessarily best for painted metal, plastic, wood, cardboard, paper, or glass.

2. Feel the surface that the seal will be applied to so that you can detect any substances the adversary has added to reduce adhesion. Pre-cleaning of the surface with a solvent or detergent water is strongly recommended. Residue from previous adhesive label seals must be fully removed.

3. The surface should not be cold, wet, corroded, or peeling.

4. Full adhesion requires more than 48 hours. This often makes it easy for the first 2 days to lift the seal without causing damage or evidence of tampering. Heat can help speed up the adhesion process. (For safety reasons, be careful not to heat any cleaning solvent that has not yet fully evaporated!)

5. Ideally the adhesive, substrate, and ink should be made of the same material, or at least they should dissolve in exactly the same solvent. (Few, if any, adhesive label seals are designed this way.)

6. Consider covering the label seal with a plastic protective sheet or clear protective spray while it is in use.

7. During seal inspection, carefully examine the surface area outside the perimeter of the seal to look for evidence of attack.

8. The best way to detect tampering with an adhesive label seal is to observe (and smell) as the seal is being removed. The seal inspector, however, must understand how the seal is supposed to behave (and smell) ordinarily.

9. A blink comparator used with a kinematic mount (to exactly re-position the camera without any necessary adjustment) is an excellent way to compare before and after images of seals to look for tampering. Contact the authors for more information.

10. Manufacturers and vendors often emphasize the unique features of adhesive label seals that they claim are difficult or impossible to replicate. This is usually quite untrue in our experience, but it doesn't usually matter since most adhesive label seals will be attacked by reusing the original seal, perhaps with some artistic, cosmetic, or repair work.

11. Seals that reveal words like "OPENED" or "VOID" or show patterns when removed from a surface are largely gimmicks that do not represent serious challenges to an adversary. (On the other hand, this feature can be quite effective for flag seals.)

ISO 17712

In our view, existing standards for tamper-indicating seals are not very helpful. We believe that ISO 17712, the new international standard for freight seals [24], does a particularly serious disservice to effective tamper detection. ISO 17712 formalizes flawed concepts, encourages misleading terminology, over simplifies critical seal and vulnerability issues, and compromises cargo and homeland security. We are preparing a detailed critique of this standard but our advice in the meantime is not to be overly confident about seals that meet the ISO 17712 standard.

Better Seal Training

The best advice and training for tamper detection is specific to the relevant seals and the security application of interest. The authors are available to provide seal and cargo security advice for legitimate organizations that face security and tampering issues.

Conclusion

If used effectively (i.e., with a good use protocol) and with a realistic understanding of their capabilities and vulnerabilities, seals can provide fairly reliable tamper detection. But they are not a simple-minded, silver bullet for tamper detection or logistics security. We also believe that much better seal designs are possible.[2,5,11,17]

Disclaimer

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

About the Authors

Roger Johnston, Ph.D., CPP and Jon Warner, Ph.D. are part of the Vulnerability Assessment Team (VAT) at Argonne National Laboratory.[15,17] The VAT has provided consulting, training, vulnerability assessments, and security solutions for over 50 government agencies and private companies. Johnston and Warner have conducted vulnerability assessments on hundreds of different seals, and demonstrated easy-to-exploit vulnerabilities (but also effective countermeasures) for many other physical security devices and systems including locks, tags, access control and biometrics devices, GPS, RFIDs, nuclear safeguards, and electronic voting machines.

Dr. Johnston and Dr. Warner have published more than 170 technical papers, given over 90 invited talks (including 6 Keynote Addresses at national and international security conferences), and hold 10 U.S. patents.

References

1. RG Johnston, DD Martinez, and ARE Garcia, "Were Ancient Seals Secure?", *Antiquity* **75**, 299-305 (2001).

2. RG Johnston, "Tamper-Indicating Seals", *American Scientist* **94,** 515-523 (2005).

3. NAVFAC, "Department of Defense Lock Program: Security Seals", https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_nfesc_pp/locks/SEALS_INFO/TAB_SEALS_INTRO.

4. RG Johnston, "The Real Deal on Seals", *Security Management* **41**, 93-100 (1997).

5. RG Johnston, "The 'Anti-Evidence' Approach to Tamper-Detection", *Packaging, Transport, Storage & Security of Radioactive Material* **16,** 135-143 (2005).

6. RG Johnston, "New Research on Tamper-Indicating Seals", *International Utilities Revenue Protection Association News*, **16**(1), 17-18 (2006).

7. L Tyska, Editor (1999), "Seals" in *Guidelines for Cargo Security & Loss Control*, (National Cargo Security Council, Wash, D.C.), Chap 4 (29-38).

8. U.S. Nuclear Regulatory Commission, "Pressure-Sensitive and Tamper-Indicating Device Seals for Material Control and Accounting of Special Nuclear Material", Regulatory Guide 5.80, December 2010, http://pbadupws.nrc.gov/docs/ML1018/ML101800504.pdf

9. AW Appel, "Security Seals on Voting Machines: A Case Study", *ACM Transactions on Information and System Security*, 14(2), September 2011, http://dl.acm.org/citation.cfm?id=2019603&CFID=63720906&CFTOKEN=32687086

10. RG Johnston, EC Michaud, and JS Warner, "The Security of Urine Drug Testing", *Journal of Drug Issues*, **39**(4) 1015-1028 (2009).

11. RG Johnston, "Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management", *Science and Global Security* **9,** 93-112 (2001).

12. RG Johnston, "Tamper Detection for Safeguards and Treaty Monitoring: Fantasies, Realities, and Potentials", *Nonproliferation Review* **8**, 102-115 (2001).

13. RG Johnston and JS Warner, "The Doctor Who Conundrum: Why Placing Too Much Faith in Technology Leads to Failure", *Security Management* **49**(9), 112-121 (2005).

14. AW Appel, "The Trick to Defeating Tamper-Indicating Seals", https://freedom-to-tinker.com/blog/appel/trick-defeating-tamper-indicating-seals

15. P Rogers, "Most Security Measures Easy to Breach", http://www.youtube.com/watch?v=frBBGJqkz9E

16. JS Warner and RG Johnston, "Why RFID Tags Offer Poor Security", *Proceedings of the 51st Annual INMM Meeting,* Baltimore, MD, July 11-15, 2010.

17. Argonne National Laboratory, "Vulnerability Assessment Team", http://www.ne.anl.gov/capabilities/vat.

18. 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

19. RG Johnston and ARE Garcia, "Vulnerability Assessment of Security Seals", *Journal of Security Administration* **20**, 15-27 (1997).

20. RG Johnston, "Effective Vulnerability Assessment of Tamper-Indicating Seals", *Journal of Testing and Evaluation* **25**, 451-455 (1997).

21. RG Johnston, ARE Garcia, and WK Grace, "Vulnerability Assessment of Passive Tamper-Indicating Seals", *Journal of Nuclear Materials Management* **224**, 24-29 (1995).

22. RG Johnston, "Assessing the Vulnerability of Tamper-Indicting Seals", *Port Technology International* **25**, 155-157 (2005).

23. RG Johnston and ARE Garcia, "An Annotated Taxonomy of Tag and Seal Vulnerabilities", *Journal of Nuclear Materials Management* **229**, 23-30 (2000).

24. International Standards Organization, "Freight Containers – Mechanical Seals", ISO 17712, September 1, 2011.

Figures

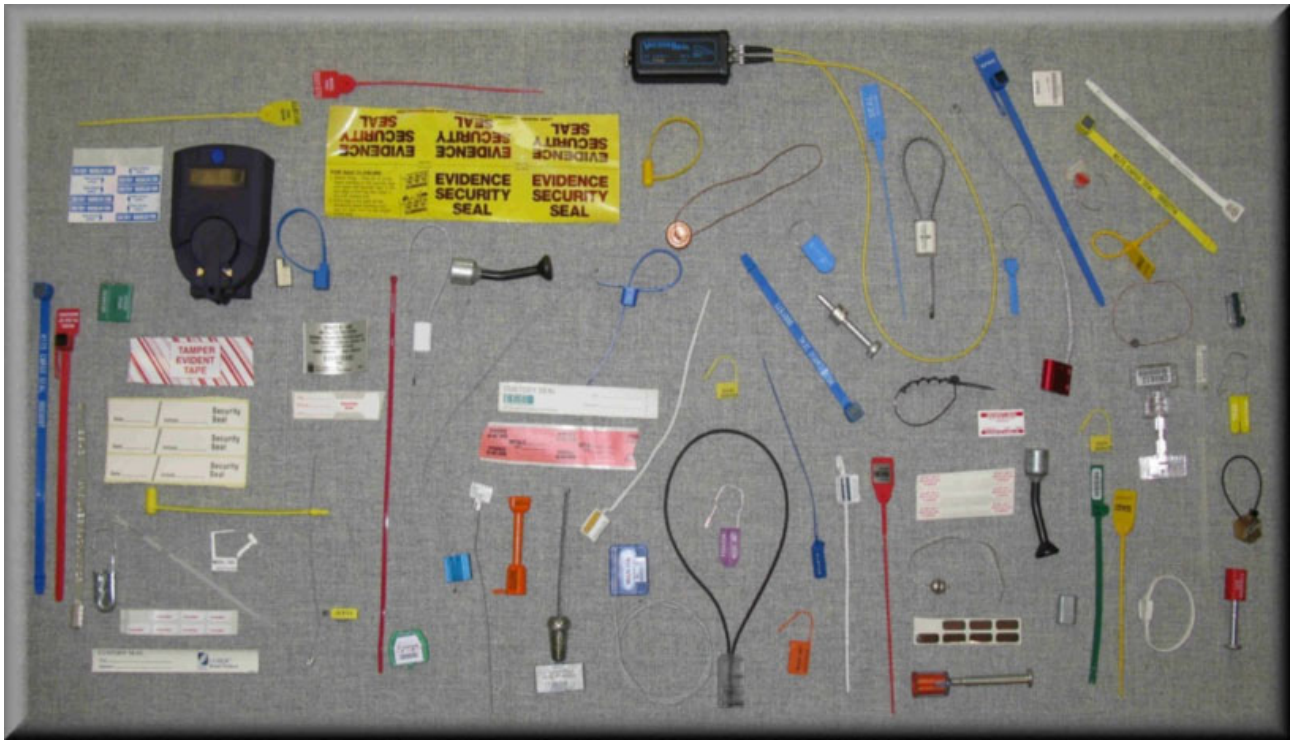

Figure 1 - Examples of the more than 5,000 tamper-indicating seals that are commercially available. Some are based on supposedly irreversible mechanical assemblies. Others are frangible or use electronic or optical means to detect physical intrusion or seal opening. Adhesive label seals typically attach to an object or container using a pressure-sensitive adhesive.

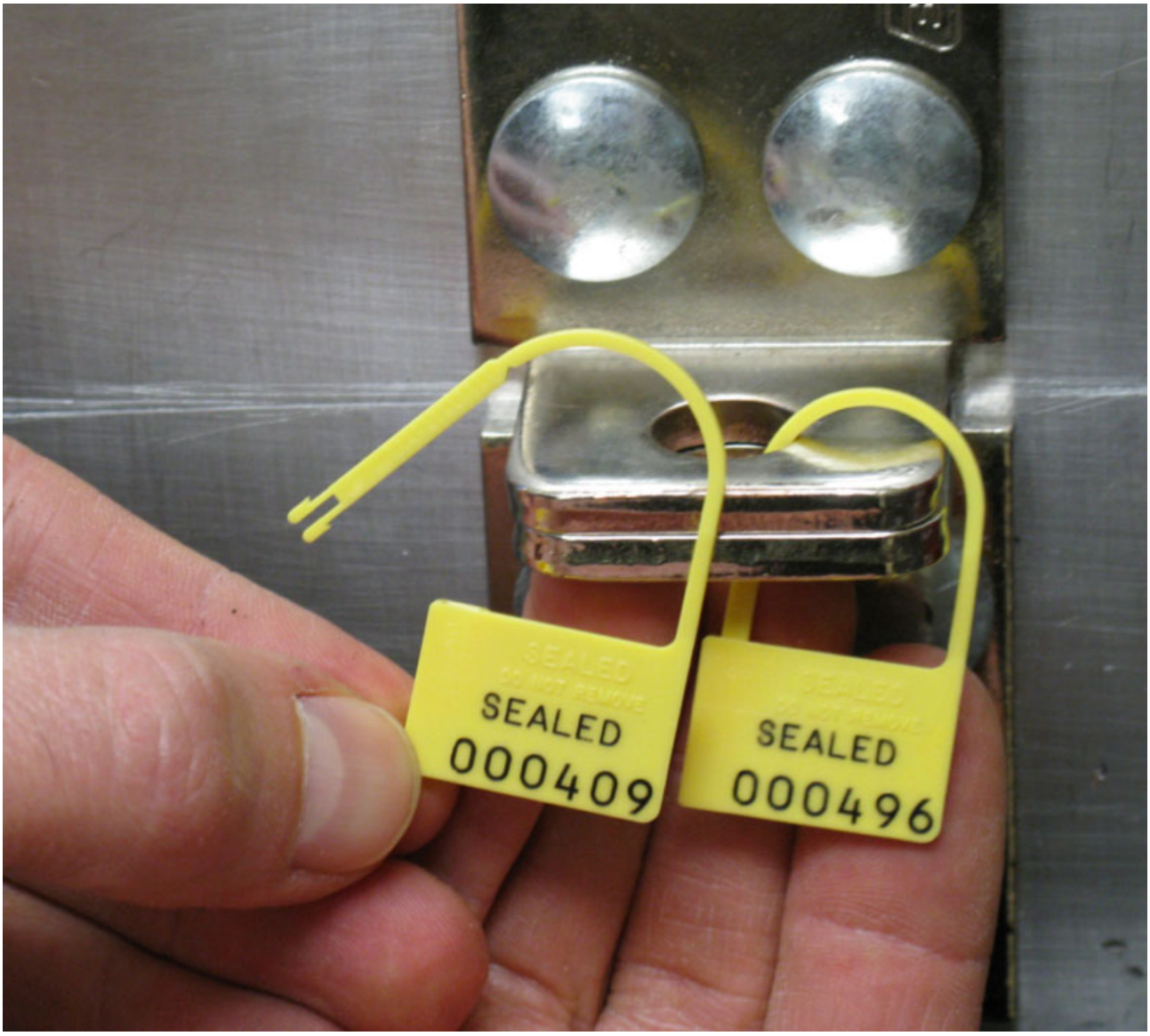

Figure 2 - At inspection time, a seal should be compared side-by-side with a similar, unused seal that has been protected from tampering.