sealock

White Paper

Protecting the Supply Chain From Covert Attacks: A Cost-Effective, Industry-Proven Solution

About This Paper

Cargo containers are an attractive target for thieves and other enemies of the state, both for the value of the goods they carry and their potential for use as a Trojan horse. Yet the most widely adopted methods for securing cargo containers—the bolt seal and single-loop cable seal—can be bypassed quickly without leaving telltale evidence. This paper explains the most common of the many methods by which criminals circumvent conventional cargo seals, and introduces a cost-effective, industry-proven solution to prevent these covert attacks.

About Sealock

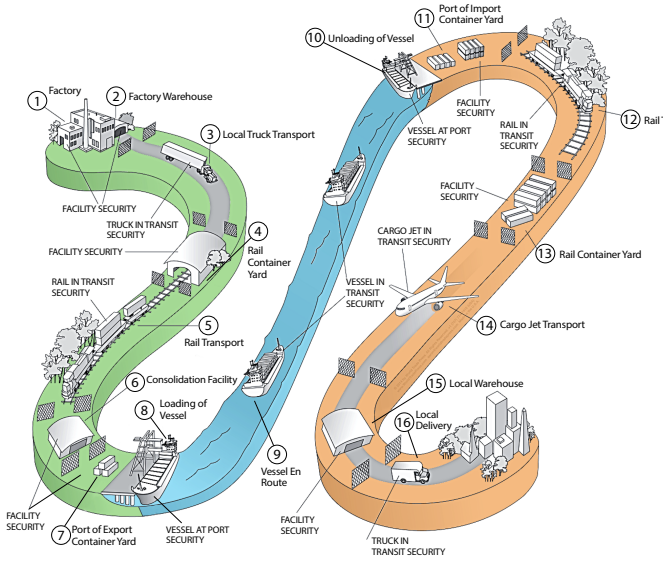
Sealock Security Systems, Inc. has a 23-year history of successful product development in the cargo security industry. Since its founding in 1996, Sealock has grown into a company that provides cargo security devices to some of the largest movers of freight in the world. Key customers include Wal-Mart, Target, IKEA, Starbucks, Pfizer, and Red Bull, to name but a few.

Introduction

How the Seal *Should* Work: A Quick Means of Ensuring Shipment Integrity

The global supply chain is an extremely complex system, with multiple, independent, unrelated entities working in unison to move goods across great geographic distances. Just as in a physical chain, each link in the supply chain must perform its role properly for the entirety to function.

Incredibly, the system typically functions without central coordination. Each of the system's constituents, all interconnected but operating independently, carries out its functions and relies on the others to do the same. Many of these parties will never communicate with each other directly, and yet the vast majority of the time the system functions as expected and goods reach their intended destination intact and undisturbed.



The global supply chain is almost impossibly complex. Image source: C-TPAT Importers Minimum Security Criteria Update Workbook 2018

As goods move through exchange points within the chain, from different modes of transportation to various types of processing facilities, numerous intermediate recipients take temporary custody of, and responsibility for, the goods. But before assuming such liability, these intermediaries first seek to satisfy themselves that the goods remain in their intended, original condition. To facilitate this process, a simple means of communicating the integrity of the shipment has become convention: the traditional cargo seal.

From the very start of the chain, numerically-sequenced cargo seals are applied to the handle of the right-hand door on the back of cargo containers after the goods have been loaded. So applied, the seal is intended to provide an inexpensive way to quickly check the integrity of the container. At each handoff, the new recipient notes the number that appears on the seal against the one reported on the shipment's manifest; if the numbers match, the seal's continued presence on the back of the container allows the recipient to presume the container has not been opened while in the delivering party's possession, and the flow of commerce may continue.

Conventional cargo seal in right-hand door handle

On the other hand, a seal that is missing, or a seal that is present but with incorrect numbers, quickly indicates to the recipient that something is amiss. Delivery may then be refused, and the supply chain halted for investigation to begin—crucially, *before* liability passes to the next recipient. In this way, the humble cargo seal takes on an outsized role in securing the entirety of the supply chain.

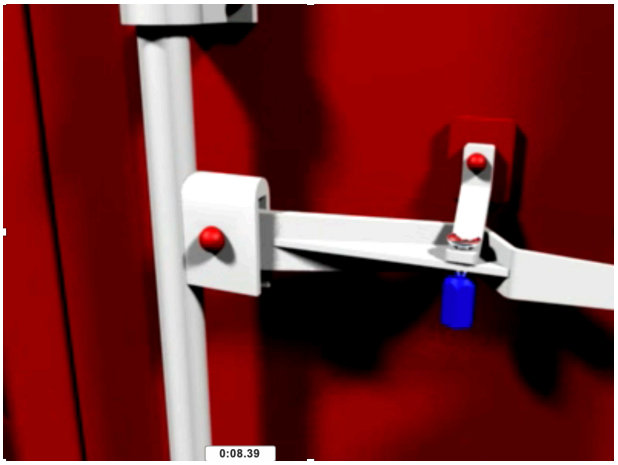
At least, that is how the common cargo seal is *intended* to function. All too often, unfortunately, these seals may appear intact, when in fact they have been defeated while in the other party's possession. And during such defeat, goods and merchandise may have been removed by thieves, or contraband inserted, illegal aliens stowed, even weapons of mass destruction hidden inside.

Millions of Jobs.
Billions of Products.
Trillions of Dollars.
It All Rests on One Seal.

Problem

Circumvention of Conventional Seals: The Worst-Kept Secret in Cargo Security

The current generation of bolt and single-loop cable seals can be defeated quickly and the evidence of defeat hidden easily, in a variety of ways.[1] Common bolt seals and single-loop cable seals are applied only to the handle of the right-hand door of the container, to prevent turning of the handle and thereby prevent unlocking of the right-hand door. But various techniques exist whereby this method of sealing can be quickly circumvented—leaving the seal undisturbed and intact while the container doors may be opened and closed freely. By only sealing one door instead of physically binding both doors together, the common bolt seal is inherently flawed in its design.



A conventional seal applied to the right-hand door

The key issue with all traditional bolt seals is that they do not seal the container; they seal the container's handle to the door. As depicted immediately above, a bolt seal is usually affixed only to the handle of the innermost bar on the right-hand door. Once the seal is in place, the handle cannot be turned, and the door (in theory) remains locked as the bar is engaged with the locking mechanisms at the top and bottom of the container.

However, criminals have known for decades that the handle itself can be attacked in less than a minute, while leaving the bolt seal entirely undisturbed. As depicted in the following image, with the use of something as simple as a battery-operated household drill or even a basic chisel, the rivet attaching the handle to the bar can be removed and destroyed. Just by removing this single rivet, the handle can be disengaged from the locking bar and the entire locking mechanism disassembled—while the seal remains completely in place undisturbed. Note the seal itself could be an expensive, tech-enabled device, with GPS tracking, and still be circumvented by this simple method.

Removing a single rivet circumvents the "seal"

With the rivet removed, the door can be swung open as it normally would, merely by rotating the locking bar, and all the while ignoring the "sealed" handle. Finally, a new rivet can be applied, reattaching the handle to the locking bar.

This key vulnerability of the common cargo seal significantly reduces its reliability as a tamper-indicative measure. The vulnerability arises because the seal only seals the handle shut; it does not lock the two container doors together. Most concerning, as the minimum standard promulgated by the Federal government, this flawed approach to cargo security is nearly universally adopted, even though the vulnerabilities are widely known by criminals. Fortunately, there is a simple, cost-effective solution.

What good is a seal that can be bypassed entirely, with no telltale evidence?

[1] Although only one is discussed here, numerous methods exist allowing for the covert entry into a container without attacking the conventional seal directly. Informative videos depicting these attacks are freely available online. For additional information, please visit: https://www.youtube.com/watch?v=wqz99bFYENY. Moreover, a 15-second video demonstration of the rivet attack discussed here is available online at https://www.youtube.com/watch?v=qzwPQ5hSzH8. (Both links last accessed October 2, 2019).

Pictured: Sealock Model SL-C dual-function, hybrid sealing-and-locking cable seal.

Solution

A Dual-Function, Hybrid Device that Simultaneously Seals *and* Locks

Attacks such as the one previously discussed can be prevented by using a dual-function, hybrid device which simultaneously seals and locks the container doors together, such as the cable seal pictured here. Dual-function, hybrid devices like this cannot be circumvented by the means previously discussed because the container doors cannot move independently of each other: they are physically locked together by the same device that is sealing the right-hand door handle.

Even if the rivet is removed, the right-hand door cannot open independently of the left, because the two doors are bound together by the same length of cable that is also sealing the handle. So the previously demonstrated rivet attack fails when a dual-function, hybrid device is used. Indeed, *all* of the other commonly deployed covert attack methods fail against such a device.

These dual-function devices succeed because, in order to open either door, the entire device must be destroyed—leaving telltale evidence of the intrusion. Finally, the cargo seal is able to fully achieve its intended function: providing a reliable means of quickly confirming the integrity of the shipment. Because such dual-function, hybrid sealing-and-locking all-in-one devices cannot be surreptitiously circumvented, supply chain intermediaries receiving these shipments can reasonably rely on the presence of the device as evidence the cargo remains intact, in the same condition as at origin—which is exactly what the supply chain expects and requires of its seals.

Results

Real-World Success Stories Prove Out the Approach

The ability of dual-function, hybrid devices to address covert attacks is not just theoretical: leading shippers around the world have adopted these devices as the preferred approach for securing their supply chains, and have witnessed firsthand improvements in their security. From big box retailers, to pharmaceutical giants, to precious metal traders, and many more, Sealock's dual-function cargo seals have solved real-world cargo crime issues.

"We have seen as near a 100 percent abatement of the shrink-pilfering problems."
—Allen M. Perkins, Fleet and Compliance Specialist, Alter Trading Corporation

> **The IKEA supply chain is an extensive, far reaching organism that is growing constantly. As one of the more recognized brand names, IKEA's supply chain is a constant target for criminals looking to take advantage of its name and reputation. In recent years IKEA has become aware of the need to increase security in the over-the-road, cross-border shipments from Mexico and ocean shipments from South America. After benchmarking with other major importers and being referred to Sealock, the decision was made to mandate all IKEA suppliers utilize Sealock cable seals on shipments from high risk countries in the Americas. All suppliers in these high risk countries are using these seals and there has been a notable decrease in attempts to contaminate the IKEA shipments with contraband, which has allowed IKEA to successfully mitigate these risks and keep its CTPAT Tier 2 status.**
> ***—Mark Moss, Customs Compliance Security Specialist, IKEA***

For example, when one of the United States' leading scrap metal recyclers, Alter Trading, began experiencing mysterious losses of cargo, it turned to Sealock to address the problem. Reflecting on the company's success, Alter's Fleet and Compliance Specialist, Allen M. Perkins, notes: "**Since we began the program employing Sealock's SU-2009 and SU-2013 barrier seals, we have seen as near a 100 percent abatement of the shrink-pilfering problems as any shipper may desire. This improved condition has held for the past 8 years while our volume of shipments has steadily increased.**" Alter's positive experience is typical for companies adopting dual-function, hybrid sealing-and-locking devices in response to mysterious cargo losses.

After world-recognized home furnishings brand IKEA became aware of regional security issues in Central and South America, the company realized supply chain security improvements were warranted. Mark Moss, IKEA's Customs Compliance Security Specialist, writes: "**After benchmarking with other major importers and being referred to Sealock, the decision was made to mandate all IKEA suppliers utilize Sealock cable seals on shipments from high risk countries in the Americas. All suppliers in these countries are using these seals and there has been a notable decrease in attempts to contaminate the IKEA shipments with contraband**."

Recognizing the benefits gained by shippers such as IKEA and Alter Trading, marine insurers likewise encourage, and at times even require, the use of these products. Gregory J. Kritz, a marine underwriter and Lloyd's Coverholder with over thirty years of experience, writes: "**For selected risks, I and many of my underwriter peers specifically require the use of a Sealock seal as a condition of insurance. I've personally required use of Sealock products for over twenty years. Years of data indicates that the use of Sealock reduces, and in many cases eliminates, pilferage on truck loads and shipping containers.**"

The adoption of dual-function devices by shippers and their requirement by insurers suggests that there is real value in using these hybrid devices to enhance supply chain security. That inference is further supported by cost-benefit analysis, as the following section shows.

Cost-Benefit Analysis

Effective Security Achieves at Least 2-10x Return on Investment

Cargo theft losses are notoriously difficult to quantify. Shippers are reluctant to share loss rates, for fear of diminishing their reputation. Furthermore, there is no comprehensive central repository of data. For example, although the FBI compiles cargo theft

"Years of data indicates that the use of Sealock reduces, and in many cases eliminates, pilferage on truck loads and shipping containers."
—Gregory J. Kritz, Principal, World Insurance Services, Inc.

statistics, only 22 of 50 states submit data—and notably, many of the most populous states (California, Georgia, Illinois, Massachusetts, New Jersey, New York, North Carolina, Pennsylvania, etc.) do not participate. Consequently, industry groups believe cargo losses may be widely underreported.[2]

Nonetheless, the limited data that is available can be used to draw some conservative conclusions as to the financial impact improved cargo security devices may offer. The FBI counted 649 number of container thefts in 2018.[3] Given that jurisdictions participating in the FBI survey represent approximately only 41% of the U.S. population, we can roughly adjust by population to estimate the total U.S. gross cargo theft incidences at 1,583. Taking into account that estimated overall container movement entering and leaving the U.S. in the same period was 37.4 million,[4] we can assume a per container loss rate on average of 1,583 incidents / 37.4 million containers = 0.00423%. (Note this only accounts for losses sustained within the U.S., in accordance with the data collected by the FBI. The overall rate globally will be higher.)

The per container loss rate can be multiplied by the average loss value to derive a break-even point for per container cargo security spending. Assuming the 0.00423% loss rate, and taking into account a reported $143,949 average loss value,[5] the average break-even point for effective security spending per container is $6.09/container (0.00423% x $143,949). Given that the dual-function, hybrid cable seals discussed here can retail below $3.00 per unit at large volume, and in customers' experiences have been near 100% successful in eliminating common covert container theft, **companies can expect at least a 2x return on investment when utilizing these devices. And for companies that routinely move containers with values in excess of the $144,000 average, the rate of return could be significantly higher**.

Finally, these returns are likely to be conservative, given the fact that container thefts are known to be widely underreported, and the true cost of a particular incident will likely exceed the gross value of the reported loss. For example, although average reported loss may only be approximately $144,000, this is typically only an indication of the retail value of the stolen product. In fact, the actual losses suffered will be multiples higher than this reported retail value due to indirect costs consequent to the incident. **In certain industries, the total cost could well exceed 3 to 5 times the reported retail loss,[6] in which case the break-even point for spending, and the expected return on investment, would increase accordingly. For these industries, return on investment could easily exceed 10x**.

Stakes
Countless Dollars, Priceless Lives

While the economics support adoption of these enhanced cargo security measures, equally if not more important in the calculus is securing the supply chain against terrorism. Cargo containers are not just an attractive target for thieves: their potential for use as a Trojan horse makes them susceptible to corruption by terrorists looking to move supplies or, in a worst-case scenario, weapons of mass destruction. The disturbing ease with which a terrorist could infiltrate a container to smuggle destructive weapons is a real concern that should not be ignored.

Global supply chain security is of paramount importance to the safety of the American people, and improving the efficiency of the flow of international commerce is essential to the wealth of the nation. Yet this glaring weakness in a linchpin of cargo security threatens to

---

[2] Bill Turner (September 5, 2018), *Cargo Theft Statistics: Unreported Incidents May Greatly Understate the Numbers*, Loss Prevention Magazine, https://losspreventionmedia.com/unreported-cargo-theft-incidents-make-it-difficult-to-grasp-scope/ (last accessed October 2, 2019).

[3] The U.S. Department of Justice, Federal Bureau of Information's Uniform Crime Reporting Program, *2018 Crime in the United States, Table 1 (Cargo Theft by State),* https://ucr.fbi.gov/crime-in-the-u.s/2018/crime-in-the-u.s.-2018/additional-data-collections/cargo-theft/table-1.xls/view (last accessed October 2, 2019).

[4] Eric Johnson (May 31, 2019), *Tariff Tremors Test Top 100 US Importers, Exporters,* JOC.com, https://www.joc.com/maritime-news/tariff-tremors-test-top-100-us-importers-exporters_20190531.html (last accessed October 2, 2019).

[5] Eboni Thomas (2018), *Third Quarter 2018 Cargo Theft Trends Analysis,* Cargonet.com, https://www.cargonet.com/news-and-events/cargonet-in-the-media/third-quarter-2018-cargo-theft-trends-analysis/ (last accessed October 2, 2019).

[6] Dr. Marvin Shepherd (March 2015), *Pharmaceutical Cargo Theft: Uncovering the True Loss*, Vigilant e-Magazine, https://www.tapa-global.org/fileadmin/public/downloads/vigilant/2015/TAPA_EMEA_Vigilant_e-Magazine_-_March_2015.pdf (last accessed October 2, 2019).

undermine the entire system, and implicates numerous core missions of the US Department of Homeland Security (DHS). Ensuring the integrity of cargo containers is vital to DHS's mission to prevent terrorism and enhance security, due to containers' potential for use in smuggling contraband (including weapons of mass destruction). And DHS's mandate to secure and manage the country's borders is directly affected by the quality and reliability of port security, of which cargo security is a key component.

Despite these unmatched stakes, the vast majority of the millions of cargo containers entering U.S ports each year rely on demonstrably deficient devices to secure their contents—thereby threatening the entire system.

Conclusion

Covert Attacks Can Be Avoided, and the Solution is Cost-Effective and Industry-Proven

The global supply chain is an almost unimaginably complex system, with parties around the globe working remotely and independently to move goods across great geographic distances. Underpinning it all is the humble cargo seal. A reliable seal allows these various parties to carry out their roles within the system in confidence.

Yet the most common seal used to support this intricate system is widely known to be susceptible to covert attacks. The conventional bolt seal and single-loop cable seal can be (and regularly are) bypassed quickly and easily by criminals without leaving telltale evidence, thereby undermining the integrity of the entire system.

Fortunately, there are industry-proven, cost-effective means to secure the supply chain and fulfill the crucial role of the cargo seal. Prominent, forward-thinking shippers and insurers have already begun adopting these devices with real-world success. But the overwhelming majority of containers entering and leaving the U.S. each year continue to be sealed by insufficient devices.

And the stakes could not be higher. The security of the global supply chain is not only essential to the flow of commerce: cargo containers' potential for abuse as a Trojan horse makes them another weapon in the arsenal of terrorist and other enemies of the state. Supply chain vulnerabilities threaten not only wallets, but lives.

Despite the widely known risks of using these flawed devices, U.S. Customs and Border Protection, through its Customs-Trade Partnership Against Terrorism, continues to validate their use as a minimum standard. Although the positive, impactful return on investment will continue to drive leading shippers and insurers to address these vulnerabilities with dual-function, sealing-and-locking cargo seals, only until top-down leadership from the Federal government adopts such measures for its own use will the laggards finally follow suit. Until then, the vast majority of containers will continue to move through the system with a fatally flawed false sense of security. Hopefully, change will come—*before* a tragedy necessitates it.

sealock

Sealock Security Systems, Inc.
11350 NW 36th Terrace
Miami, Florida 33178
USA
1-305-418-7603
www.sealock.com