



Seal launch

Glen Carroll of SecurTrack presents the case for electronic seals

On 15 October 2008, a mandate issued by the **United States Customs Border Protection (CBP)** became effective requiring all US inbound maritime containers to be secured with an **International Organization for Standardization ISO/PAS 17712** bolt seal. The genesis of this mandate can be traced back to the interpretation of the *SAFE Port Act* of 2006, which called for the **United States Department of Homeland Security (DHS)** to develop minimum container security standards by March 2007. The DHS was to determine whether electronic container security devices (CSDs) were technically feasible and should be included in the standards, but was given the option of not including CSDs if they were proven not to be effective and reliable. A default provision was added to the *9/11 Implementation Bill* requiring the DHS to issue a standard for bolt seals by 15 October 2008 if no CSD standard was in place by mid-April 2008.

Because many of the CSDs that were available at that time proved to be anything but effective and reliable, the DHS decided not to mandate electronic CSDs and instead mandated the bolt seal. According to a statement issued by the former DHS Secretary, Michael Chertoff, in December 2007: 'CSDs have not proven effective enough in an operational environment, and industry is concerned about the cost of the equipment, logistical challenges such as installing radio frequency identification (RFID) readers, returning reusable units, and delays resulting in Customs responding to alarms.' He went on to say that although the *SAFE Port Act* and the *9/11 Act* encouraged the DHS to develop and implement CSDs 'neither law prescribes a clear path for their development and use'.

However, the ISO did prescribe a clear path to aid in the development of electronic seals (e-seals) by issuing a set of standards in early 2007 (Series 18185). The standards include communication protocols, application requirements, environmental characteristics, and data protection. While this helped in the technical development of e-seals, there

seemed to be confusion on how and when to apply them in the supply chain. Meanwhile, containers still arrived at ports around the world unsecured.

In April 2008, the **US Government Accountability Office (GAO)** published a report on Supply Chain Security (*GAO 08-240*) in which it reviews the progress of supply chain security from late 2001 to early 2008.

The GAO report stated: 'Every time the responsibility for cargo in containers changes hands along the supply chain, there is the potential for a security breach; thus, vulnerabilities exist that terrorists could exploit by, for example, placing a weapon of mass destruction (WMD) into a container for shipment to the United States or elsewhere.' In 2002, **Booz Allen Hamilton** sponsored a simulated scenario in which the detonation of weapons in cargo containers shut down all US ports for 12 days. The estimated loss of revenue to the US economy was \$58 billion, along with significant disruptions to the movement of trade.

While there is no record of a WMD being transported into the US yet, criminals have exploited containers for other illegal purposes like smuggling weapons, people and drugs. But criminals aren't just putting things into containers, they are also taking cargo out of them. The **Federal Bureau of Investigation (FBI)** has estimated that the cost of cargo theft to the US is between \$15 billion and \$30 billion a year.

Recent surveys show that many executives from the supply chain and logistics industry consider cargo theft as the main challenge to supply chain security, while safeguarding against a terrorist attack is slightly less important. This reflects an attitude that, despite a growing number of government regulations that suggest terrorism is still a relevant threat, shippers are mainly worried about theft of their cargo.

While there is ample data attesting to the benefits of securing intermodal-shipping containers, little has been done. Theft from containers has been an issue since there have been containers, and use of containers to smuggle contraband,

Glenn Carroll is the CEO of SecurTrack, based in Fairfax, California.

Contact:
Glenn Carroll
Tel: +1 415 457 2584
Email: Glen121@comcast.net





including humans, increases every year. The events of 9/11 brought into focus the glaring vulnerabilities of our ports and supply chain, but the response to these vulnerabilities has been slow and fragmented. The main reason for this lethargic response mainly centres around the cost of implementation, but secondarily there has been little consensus on what to implement.

While there have been improvements in the security of many of the world's ports and terminal facilities, very little has been done in terms of securing individual intermodal containers. The mandate by the US government of the ISO 17712 bolt seal does not represent a step forward in container security. Many shippers and container carriers have been using these bolts for years with no appreciable effect. These seals are easily counterfeited, and their main advantage seems to be that they are inexpensive.

The debate over using e-seals is ongoing; however, the continued use of low-tech mechanical devices has proven ineffective for detecting or preventing the breach of container doors. The technology is available now to develop a single-use, disposable, inexpensive, versatile and reliable e-seal. Part of the argument put forward by the DHS for not using e-seals is the concern by both government and industry about the costs of the e-seals, the costs of an extensive and expensive RFID infrastructure, the logistics of returning reusable e-seals and responding to 'false positive' alarms caused by defective and unreliable e-seals.

In response to these issues and concerns **SecurTrack**, working in partnership with **Innovative Labs** of Santa Rosa, California, has developed an e-seal, the *SEMA-4 C-3000*, that will address many of the current concerns. First, this unit is disposable. Because of the way containers move around the globe, this feature was imperative. The shipper attaches the unit at the point of origin, then at the destination the unit is removed. The batteries that power the unit are easily removed for proper disposal. The C-3000 protects both doors of the container since it attaches to the right side door handle



'The technology is available now to develop a single-use, disposable, inexpensive, versatile and reliable electronic seal'

and, using an adjustable arm, reaches across the door seam and attaches to the left door locking rod.

One of the most difficult problems encountered by attaching an electronic device to a container is the brutal environmental conditions the container travels through. These conditions have caused malfunctions and thus the 'false positive' alarms on many of the earlier e-seals that were tested.

However, the C-3000 e-seal is made of durable ABS plastic, and the critical interior electronics are double sealed against moisture, temperature variations from -50°C to +80°C and isolated from vibrations and jolts. Extreme care was taken to assure the reliability of this unit.

The basic purpose of any e-seal is to detect, display and record any unauthorised opening of the container doors. The C-3000 does this in a unique way. By using several sensors located throughout the unit and the arm, it can detect any tampering with the unit itself or the opening of the doors. On the front of the unit is a large colour display screen and a flashing high intensity green light-emitting diode (LED). The screen and the LED remain green until they are triggered by a sensor, then the screen turns red. The green LED shuts off and a high intensity red LED begins to flash. Once the displays have changed, they cannot be reversed. The unit contains a timer and any breach event is recorded in

the database.

The colour display screen, the LEDs and the serial number, which is also printed in bar code, can be easily read by the high resolution video cameras and optical character recognition (OCR) cameras that are used at most of the major container terminals. Because the serial number and the security status can be determined quickly and accurately, it will greatly aid in container velocity through the terminals.

The C-3000 has a microprocessor that can be programmed and interrogated by readers at any time after the unit is powered up. This gives shippers and carriers the option of inputting and retrieving data. In the event of a breach, the data can be used forensically to determine where in the chain of custody the breach occurred. The C-3000 uses a passive RFID system and can be accessed by readers up to six metres away but the architecture is designed to accommodate active RFID as fixed readers come on line.

The SecurTrack C-3000 is a rugged, versatile and inexpensive electronic seal that is nearly impossible to counterfeit. Because the security status of a container can be determined visually, this system can be adopted now without waiting for expensive fixed RFID reader infrastructure. Handheld RFID/ Bar Code readers can programme and retrieve data where and when it is needed, and the electronic architecture is designed to be versatile and flexible. The SecurTrack C-3000 was recently awarded a citation for 'Best in Show' at the *US Maritime Security Expo 2008*, which took place in Long Beach in last November.

The C-3000 addresses the main concerns of government and industry regarding disposability, costs, and reliability. The bolt seal is a remnant of the past; the SecurTrack C-3000 is the future of container security.

