

# Evaluating and Improving the Security of RFID tags in eSeals at the L.A. and L.B. Ports



---

**Burkhard Englert**

Dolgorsuren Byambajav

Aniketh Parmar

CSULB

NUF Conference 2007

December 7

Long Beach CA

METRANS 06-01



# Outline

---

- Introduction and Motivation.
- RFID Systems.
- RFID Security.
- Active Tags at the ports - eSeals
- Recommendations.



# Smart & Secure Tradelanes 2003

---

- Initiative of the strategic council on Security Technology.
- Phased, industry driven initiative using an open technology platform in coordination with U.S. Customs, the Transportation Security Administration, Operation Safe Commerce, C-TPAT (Customs Trade Partnership Against Terrorism) (US C-TPAT) and the Container Security Administration.



# Incentives to participate in C-TPAT

---

- Fewer inspections of inbound cargo.
- "green lanes" to speed up handling of compliant cargo.
- "restart priority" in the event of port closure due to disaster.
- paperless information exchange.



## So far....

---

- Only reduced cargo inspections implemented.
- only about 4,000 out of about 50,000 U.S. importers have applied to join C-TPAT.
- What if ... it can be shown that an investment in cargo security is contributing to supply chain efficiency.



# Goal

---

- Analyze the security implications of the proposed technologies.
- Focus on SST application and the proposed use of Radio Frequency Identification (RFID) technology.

# RFID Systems - main components

- RFID tag or transponder - the data carrier in the RFID system.



- RFID reader or transceiver - able to read data from tags and possibly write data to them.



- Data Processing subsystem or back-end database - processes the data received from the transceiver in some useful manner.



# RFID tag or transponder

---

- read-only, write-once read-many, or fully rewritable.
- Source of power: active, semi-passive or passive.
- Frequency used: Ultra-High Frequency (UHF) 868-956 Mhz or 2.45 Ghz, High-Frequency (HF) 13.56 Mhz, low-frequency (LF) 120-140 Khz.



# RFID security - Risks and Threats

---

- Privacy attacks.
- Physical Attacks.
- Counterfeiting.
- Spoofing.
- Eavesdropping.
- Skimming Attacks.
- Denial of Service.
- Traffic Analysis.



# RFID Security solutions

---

- Kill command.
- Tag shielding and isolation.
- Active jamming.
- Blocker Tags.
- Silent Tree walking.
- Cryptography (e.g. Anonymous ID's, Challenge -response, Public Key Cryptography).



# RFID Security Solutions

---

- Hash functions.
- Pseudo Random Function.
- Tree-based Private Authentication.
- Human Protocols.
- **But:** most cryptographic schemes are not yet feasible for RFID tags or have not yet been tested enough to justify confidence in their security.



## Active tags at the ports - eSeals

---

- provide efficient, instant notification of container security breaches.
- provide automatic notification of tampering by going "silent".
- requires systems that can constantly log and monitor all container seals in a given geographical area so that any that suddenly stop responding can be flagged for action.



# ESeal Threats

---

- RFID readers broadcast RFID tag data over long distances, up to hundreds of meters away.
- Eavesdropper with an antenna and some basic receiving equipment can gather the same RFID tag information that is compiled by the reader at the port.
- Eavesdropper may also be able to physically tamper with a container seal and hide this intrusion by creating a signal that impersonates that of the original RFID tag.



# ISO 18185 eSeal standard

---

- Ratification of standard had been delayed because of concerns about RFID security.
- Now ratified, but ignored concerns.
- eSeal communication is performed in cleartext.
- Only physical but no electronic authentication.



# Savi Tag St-656

---

- Active tags based on patented EchoPoint technology.
- EchoPoint uses a multi-frequency design and a three-element system architecture that includes Signposts that notify tags of their location.
- ST-656 designed to withstand severe conditions.
- Tag includes an onboard processor, memory and radio transmit and receive capability. Possible to write to the tag while in transit and to capture data about the shipment from mobile readers.
- Cost: \$100 per tag, not including readers, signposts and operating software.



# Savi ST-656

---





# Status

---

- Lack of interoperability, standards and a perceived lack of security led many companies to question any potential return on investment into this new technology.
- Only agents such as the US military that have a large amount of control over their supply chains -that can enforce interoperability by simply changing all their systems - were early adopters.
- Several large scale demonstrations recently executed.



# Savi Tags and ISO 18185

---

- ISO 18185 standard for eSeals (April 2007) is based on Savi's active RFID technology.
- All eSeals based on ISO 18185 require the use of Savi in electrode property (ISO 18185-4).
- Users need to obtain a license for the use of Savi's IP that implements the tag-to-reader communication requirement in ISO 18185.



## Eseals at the LA and LB Ports

---

- Currently no widespread use of eSeals at the ports of LA and LB.
- Expected to change in the near future.



# Reasons for delay

---

- Technology has not yet matured sufficiently. Eg. Reliability issues.
- Interoperability problems have not yet been addressed.
- Until recently a complete lack of eSeal communication standards.
- Concern about the security of eSeals.
- Perception of a non existent or very low return on investment in an eSeal RFID system.



# ESeal security

---

- Encryption techniques not yet ready for implementation.
- Battery power limiting factor.
- Cryptographic protocols need to be hardwired on tag.
- Lack of confidence in their correctness.
- Progress may need to be motivated by the non private sector.



# Recommendations

---

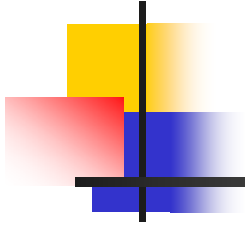
- Tag transmissions should be shielded whenever tags are not currently read by a reader.
- Tag signals should be continuously jammed while the tag and the container that contains it are in transit to a US port.
- AutoID scheme should be used to provide an additional amount of security.
- Readers should be installed only in the interior of the port (and terminal) areas.



## Recommendations cont.

---

- Tag shielding devices should be tamper proof. All personnel with access to the ports should be subject to thorough security checks so that only trusted personnel has access to the read range of the used active tags.



---

Thank You!

Questions?