Secure and Transparent Cargo Supply Chain: Enabling Chain-of-Custody with Economical and Privacy Respecting Biometrics, and Blockchain Technology
Project Team Profile

- **PI**: Larry Shi, University of Houston
- **Project Start Date**: July, 2017
- **Anticipated End Date**: June, 2019
- **Project personnel**:
  - Eleftherios Iakovou, Ph.D. Lead for Texas A & M University sub award (logistics and supply chain).
  - Lei Xu, Ph.D. co-PI (protocol design to support supply chain security).
  - Jeffrey Baldwin Sr. Senior personnel (expertise managing and directing CBP field operations).
The project addresses the need of chain-of-custody in maritime supply chain security. It enhances best practices for securing cargo release/pickup by trusted maritime transportation workers, deters cargo fraud/theft, and strengthens supply chain resilience against cybercrimes and insider threats.

It leverages recent advance in mobile biometrics/authentication and blockchain as enabling technology to achieve its goals.
Beneficiary / End User Profile: Jobs

- CBP partners from trade community: customs warehouses, logistic brokers, shippers, freight forwarders, etc.
- Marine port authorities and terminal operators.
- Technology companies developing solutions to facilitate cargo movement and ensure compliance.


Deliveries / Cargo Pick-up – verify driver identity against list and photo provided by carrier; issue temporary visitor badges; record driver’s ID, truck number, seal number, container number; verify at second access gate; verify pick-up appointment times; scan and store images of documentation tendered; on driver departure verify container / trailer, seal and documentation against information in the database; flag discrepancies.
Beneficiary / End User Profile: Desired Gains

- Improved **cargo security** to deter trafficking of illegal goods, cargo fraud and thefts.

- **Chain-of-custody** and supply chain visibility.

- Assurance of cargo handling by trusted maritime transportation workers using commercially available mobile biometrics enabled solution.

- Resilience against **cybercrimes**.

- Reduced risk of tampering and **insider threats**.

- Documentation of **compliance**, evidence of implementation, and improved **auditability**.
Beneficiary / End User Profile: Pain Points

- Lack of transparency and visibility.
  - Long persistent challenge in global supply chain and cargo industry.

- Disconnected information (lack of data consistency and harmonization).
  - Exposure to frauds, thefts (e.g., fictitious pickup), and trafficking of illegal goods.

- High cost for managing credentials.
  - ~$17K per card reader, total ~$300M - $400M deploying TWIC.

- Cybercrime and insider threats.
  - Growing risks of cybercrimes and insider threats as the industry increases reliance on IT and Internet.
# Products & Services

<table>
<thead>
<tr>
<th>Products &amp; Services</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology</td>
<td>Design of secure cargo release/pickup process to enhance chain-of-custody by leveraging state-of-the-art <em>mobile biometrics/authentication</em> and <em>blockchain</em> technology.</td>
<td>Under development.</td>
</tr>
<tr>
<td>Software &amp; Tools</td>
<td>Prototype facilitating secure cargo release/pickup for commercial customs stakeholders and CBP partners from global trade community.</td>
<td>Reducing time-to-transition: partnership, lessons learned from early adopters.</td>
</tr>
</tbody>
</table>
# Gains Created: Don’t Trust, Verify!

<table>
<thead>
<tr>
<th>Before</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information Sharing and Collaboration</strong></td>
<td>Isolated and fragmented systems.</td>
</tr>
<tr>
<td><strong>Carrier and Trucker Vetting</strong></td>
<td>Isolated IT system, vulnerability to frauds, forgery, high cost.</td>
</tr>
<tr>
<td><strong>Cargo Release Process</strong></td>
<td>Vulnerability to frauds, forgery, and tampering.</td>
</tr>
<tr>
<td><strong>Cybercrimes</strong></td>
<td>Single point of failure.</td>
</tr>
<tr>
<td><strong>Insider Threats</strong></td>
<td>Isolated systems and information silos.</td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
<td>Lack of documentation of compliance.</td>
</tr>
</tbody>
</table>
## Pains Alleviated

<table>
<thead>
<tr>
<th>Lack of transparency and visibility</th>
<th>Enhanced information sharing environment for robust detection and deterrence of cargo fraud, theft, trafficking, and breaches of security in cross border supply chain and logistics.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data consistency and harmonization</td>
<td>Improved data harmonization and as a result, efficiency for moving cargo &amp; containers (e.g., faster driver verification, less trouble tickets at terminals)</td>
</tr>
<tr>
<td>Cost</td>
<td>Virtual TWIC by leveraging commercial off-the-shelf mobile biometrics/authentication.</td>
</tr>
<tr>
<td>Cybercrime and insider threats</td>
<td>No single point of failure, resilience against cyber exploits/DOS, tamper resistance against insiders.</td>
</tr>
<tr>
<td>Compliance Verification</td>
<td>Documentation of compliance. Transactions are stored on immutable database. Improved auditability for compliance and non-compliance, and enhanced capability of post incident analysis.</td>
</tr>
</tbody>
</table>
Key Accomplishments

- Creation of a testbed environment.

- Requirement analysis and survey of terminal operation process, C-TPAT supply chain security criteria, and cargo security best practices.

- Initial design of protocols for showcasing a solution that not only realizes but exceeds C-TPAT criteria and industry practices in physical and IT security for cargo release/pickup.

- Understanding operational environments.
Key Accomplishments – Cont’d

Related publications


- One journal submission based on the conference paper.


Certify and validate partners.

Ensure compliance, evidence of implementation.

New technology capabilities for improving physical and IT security for potential upgrade of security and best practice standards.

Team: hub of innovations

Partnerships.

Technology solutions compliant with CBP security criteria and best practices.

Industry and technology partners: integration.

Transition Engagement

- **C-TPAT and Houston Field Office.**
  - Shared project information and established POCs by the team on air and maritime cargo security.
  - Houston: one of the six C-TPAT field offices in the nation.

- **Commercial customs stakeholders.**
  - Port of Houston – CIO: further meeting planned early next year.
  - Logistics providers.

- **Industry alliances on supply chain security.**
  - Cargo Security Alliance (CSA) – on C-TPAT compliance and industry best practice integration for secure cargo release/pickup.

- **Partnership on technology.**
  - T-mining, Blocklab, and Accenture Labs on technology integration, standardization and customization.
Transition Challenges

- Commercial customs stakeholders and partners of CBP.
  - Trust and understanding by stakeholders of our research mission.
  - Reluctance and fear to change.
  - Unfamiliarity with new technology.
  - Complexity of supply chain/cargo industry.

- How to overcome challenges?
  - Work with early adopters.
Conclusions

- **Objective:** Achieving chain-of-custody and strengthening supply chain security by enhancing both physical and IT security of maritime cargo release/pickup process.

- **Challenges to be solved:**
  - Lack of transparency and visibility.
  - Lack of data consistency/harmonization.
  - High cost for managing cargo handler credentials.
  - Cybercrimes and insider threats.

- **Approach:** Leveraging mobile biometrics/authentication, and blockchain as enabling technology.
Disclaimer

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2015-ST-061-BSH001. This grant is awarded to the Borders, Trade, and Immigration (BTI) Institute: A DHS Center of Excellence led by the University of Houston, and includes support for the project “Secure and Transparent Cargo Supply Chain: Enabling Chain-of-Custody with Economical and Privacy Respecting Biometrics, and Blockchain Technology” awarded to the University of Houston. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.