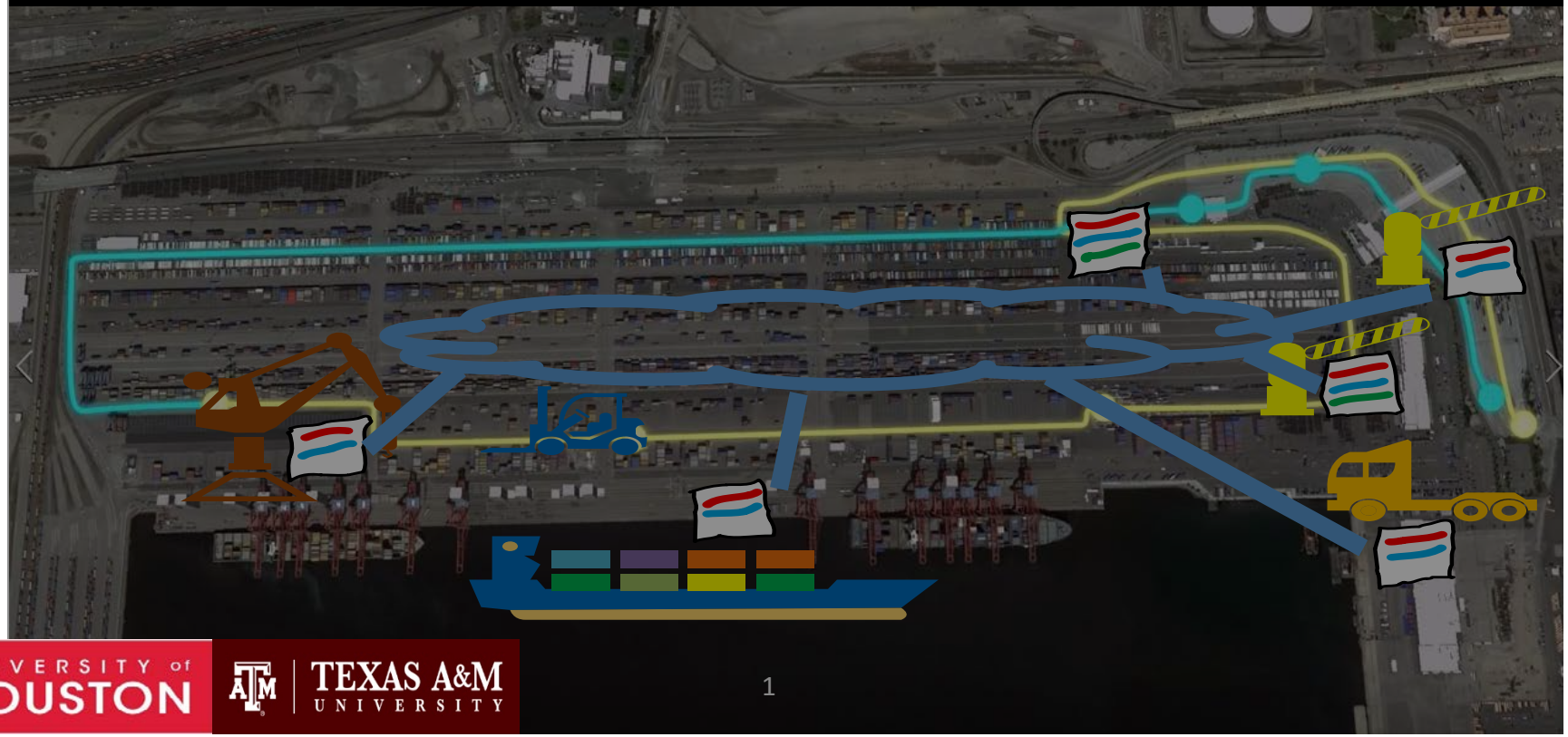
Secure and Transparent Cargo **Supply Chain**: Enabling **Chain-of-Custody** with Economical and Privacy Respecting Biometrics, and Blockchain Technology

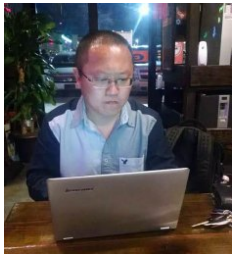


UNIVERSITY of HOUSTON | TEXAS A&M UNIVERSITY

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).

Problem Statement

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.

Cargo Theft by Fictitious Pick-up

Walt Beadling, Managing Partner, Cargo Security Alliance
Keith Lewis, Vice President of Operations, CargoNet

Executive Summary

Cargo theft by fictitious pick-up is a growing threat to supply chain security. A proliferation of information technologies enable thieves to defraud shippers and carriers at multiple points across the supply chain. This paper seeks to better define the terms and scope of this new and rapidly evolving brand of "supply chain cybercrime", and recommends *7 Best Practices* that can help prevent it.

In a fictitious pick-up, criminals fool companies into willingly turning over loads to them. They use on-line load posting sites to win transportation bids, or simply show up as drivers with fake credentials, claiming to be assigned to a load. Variations of this scam include a recently terminated driver arriving in

More action needed to prevent cargo theft, says International Union of Marine Insurance

Published on: Thu, 09/17/2015 - 09:24

The International Union o
has said that more m
cargo theft, after an in
and annual losses worth

IUMI, which is currer
conference in Berlin, h
paper that notes cargo t
to high-value goods, and

Maritime industry is easy meat for cyber criminals

May 22, 2015

Merchant vessels are continuously becoming bigger and getting more electronic systems. Seafarers often depend on technology data more than their own skills, knowledge, and senses. Crews are becoming smaller as computer systems are being used for navigation, as well as for rapid unloading, handling, and tracking of goods at ports. Unfortunately, these systems are also highly vulnerable to cyber threats.

Beneficiary / End User Profile: Jobs

- CBP partners from trade community: c*ustoms warehouses, logistic brokers, shippers, freight forwarders, etc.*
- Marine port authorities and terminal operators.
- COAC – Emerging Technologies Work Group.
- Technology companies developing solutions to facilitate cargo movement and ensure compliance.

C-TPAT on Physical Security Best Practices: ***establish and maintain Chain-of-Custody*****.**

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.*

Drayage delays are costing $348 million, 14 million hours, and 9 million gallons of fuel annually, and emitting 103,000 tons of GHGs

Scenario	Hours (million)	Fuel (million gal)	C02 (tons)	Pollutants (tons)	Cost (million)
2012 National Estimate	45	80	891,052	11,309	$ 1,640
30 vs. 40 Minute Terminal Time	4	2	17,821	253	$ 90
10 vs. 20 Minute Queue Time	3	2	24,949	355	$ 79

Products & Services

Analysis/ Report	Analysis of feasibility and benefits, report of lessons learned using *commercially available off-the-shelf mobile devices* and *blockchain* infrastructure for strengthening cross border supply chain and cargo security.	Under preparation.
Technology	Design of secure cargo release/pickup process to enhance chain-of-custody by leveraging state-of-the-art *mobile biometrics/authentication* and *blockchain* technology.	Under development.
Software & Tools	Prototype facilitating secure cargo release/pickup for commercial customs stakeholders and CBP partners from global trade community.	Reducing time-to-transition: partnership, lessons learned from early adopters.

Gains Created: Don’t Trust, Verify!

	Before	After
Information Sharing and Collaboration	Isolated and fragmented systems.	Over shared blockhain database, carrier provides in advance unique cargo release appointment and related information.
Carrier and Trucker Vetting	Isolated IT system, vulnerability to frauds, forgery, high cost.	Robust verification of carrier and trucker (multiple anchors: whitelist, TWIC, commercially available mobile biometrics, employee database).
Cargo Release Process	Vulnerability to frauds, forgery, and tampering.	Security enhanced cargo release/pickup process based on smart contracts & robust validation process.
Cybercrimes	Single point of failure.	Improved resilience against cyber exploits.
Insider Threats	Isolated systems and information silos.	Redundancy and immutable records, smart contracts based, and tamper resistance.
Compliance	Lack of documentation of compliance.	Documentation of compliance, evidence of implementation.

Pains Alleviated

Lack of transparency and visibility	**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.
Data consistency and harmonization	**Improved data harmonization and as a result, efficiency** for moving cargo & containers (e.g., faster driver verification, less trouble tickets at terminals)
Cost	Virtual TWIC by leveraging **commercial off-the-shelf mobile biometrics/authentication**.
Cybercrime and insider threats	No single point of failure, **resilience** against cyber exploits/DOS, **tamper resistance** against insiders.
Compliance Verification	**Documentation of compliance**. Transactions are stored on immutable database. Improved auditability for compliance and non-compliance, and enhanced capability of post incident analysis.

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 peer reviewed conference publication: "***CoC: Secure Supply Chain Management System based on Public Ledger.*" 1st Workshop on Privacy, Security and Trust in Blockchain Technologies in conjunction with The 26th International Conference on Computer Communications and Networks, 2017.
- **One journal submission based on the conference paper.**
- **One under review.** "*Chain-of-Custody: Blockchain based Supply Chain Security*". IEEE *Symposium* on Technologies for Homeland Security, 2018.

Transition Pathways

CBP
TSA

CTPAT™ YOUR SUPPLY CHAIN'S STRONGEST LINK.

Guidance.

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

Team: hub of innovations

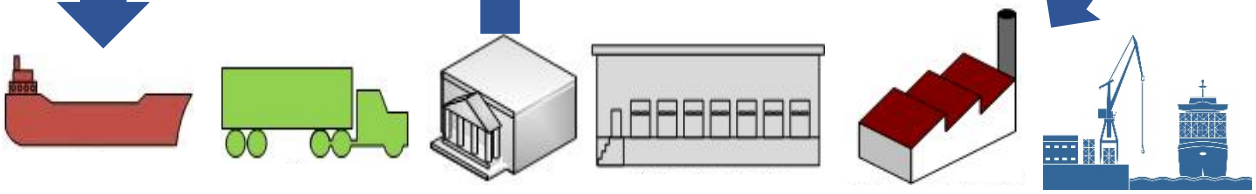
Set Forth Security Criteria and Best Practices for Supply Chain Security: Physical Security and IT Security. Tiered Benefits Structure.

Certify and validate partners.

Ensure compliance, evidence of implementation.

Partnerships.

Technology solutions compliant with CBP security criteria and best practices.



10 Business Entity Types: Importers, Air Carriers, Highway Carriers, Mexico Long Haul Highway, Carriers, Rail Carriers, Sea Carriers, Foreign Manufacturers, Customs Brokers, Port Authorities/Terminal Operators, Third Party Logistics Providers (3PLs).

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.