
March 17, 2009

Michael Orosz, Ph.D.
Information Sciences Institute (ISI)

N. Onur Bakir, Ph.D.
Post-Doctoral Research Associate

Anthony Barrett, Ph.D.
Post-Doctoral Research Associate

Jennifer Chen
Information Sciences Institute (ISI)

Petros Ioannou, Ph.D.
Professor and Director, Center for Advanced Transportation Technologies (CATT)

Isaac Maya, Ph.D., P.E.
Director of Research

Viterbi School of Engineering
University of Southern California
Los Angeles, CA

Research Assistants

Carl Southwell
Planning and Development Studies
School of Policy, Planning, and Development
University of Southern California
Los Angeles, CA

Afshin Abadi
Electrical Engineering

Mithun Baphana
Electrical Engineering (Computer Networks)
Viterbi School of Engineering
University of Southern California
Los Angeles, CA
The Problem

- Ports and similar operations are composed of many different components (e.g., terminals, bridges, inspection points, etc.), agencies, and interactions between these "systems"
  - The complex operations and interactions within and between these components make risk assessment and management difficult.
  - These are “system of systems” problems which are difficult to model and analyze

- These "system of systems" are dynamic - constantly changing both day-to-day and long-term.
  - There are tactical risk-based decisions that influence strategic planning and vice versa
Port Security Risk Management and Resource Allocation Project

1. Develop and apply systems-based risk management methodology and tools for assessing risk and evaluating alternative technology-based solutions and resource allocation policies.
   - Develop a useful port/terminal risk evaluation tool
     • Security officer
     • Resource analyst
   - Develop methodology for countermeasures/technology evaluations and resource allocation evaluations

2. Demonstrate benchmark case
   - Port boundary protection resource allocation (From among the 13+ security agencies at the POLA/POLB complex)
   - Strategic resource allocation trade-off example TBD
PortSec Risk Analysis Methodology

Risk Assessment

Threat Assessment → Vulnerability Assessment → Consequence Assessment

Prevent/Avoid/ Monitor → Protect/Countermeasure → Respond/Recover

Economic Assessment

Assessment of Direct Econ. Consequences → Assessment of Indirect Econ. Consequences → Cost-Benefit & Decision Analysis

Risk Management
PortSec Approach

1. Research and understand the problem
   – Pre-existing scenarios reviewed and accepted by port community
   – Define attackers, modes, targets, conditions, probabilities
   – Define resources available, possible allocations, tradeoffs

2. Develop/refine technical solutions that address the problem
   – Scenario risk: Threat \times Vulnerability \times Consequence
   – Incorporate best available data
   – Reflect best Port estimates
   – Calculate based on developed/benchmarked models

3. Incorporate external inputs when and where available
   – MSRAM
   – FSIVA: HLD-ECAM (M/D-SHARPP, Criticality)
   – Port self-assessments

4. Demonstrate and collect stakeholder feedback

5. Repeat steps 1 through 4 as necessary

6. Deploy technology
Analysis Begins with a Scenario:
e.g., Conventional Truck Bomb at Single Terminal

Vulnerability: Low percentage of containers are currently adequately screened

Threat: Conventional bomb packed in a container

Countermeasures: ID checks, physical screening, chemical sniffers, dogs

Consequences: 25 Injuries, 10 Deaths, $45 million in Property Damage, $449 million in Business Interruption and Indirect Costs, Total Costs of about $866 million
Resources Engaged in Port Security

- Example of agencies that provide security resources in and around the port complex:
  - Los Angeles Port Police
  - Port of Long Beach Harbor Patrol
  - Los Angeles Police Department Harbor Division
  - Long Beach Police Department
  - California Highway Patrol
  - U.S. Coast Guard
  - U.S. Customs and Border Protection
  - Los Angeles County Fire Department
  - City of Long Beach Fire Department
  - City of Los Angeles Fire Department
  - U.S. Immigration and Customs Enforcement
  - Los Angeles County Sheriff’s Department
Identify Potential Countermeasures for Reducing Terrorism Risk

Potential countermeasures to improve physical security in and around the port complex could include:

- Patrol cars
- Patrol boats
- Motion/vibration/heat detectors
- Security fences
- Waterborne barriers and gates
- Underwater surveillance systems
- Radar surveillance systems
- Pipeline protection systems
- Unmanned aerial vehicles
- Fixed and portable lighting systems
- Car checkpoints
- Gate inspections
- Portable rad/nuke sensors
- Biometric identification cards
- Divers
- Cameras
- Automatic Identification Systems
PortSec Software – Users

- Port Security Officer – tactical responsibility for daily security arrangements, has limited additional resources that can be reasonably reallocated on an as-needed basis.

- Port Security Analyst – strategic analysis of potential long-term resource allocation investments for port security.
PortSec Software – Approach

• Develop generalized “infrastructure” security software – support multiple domains

• Tailor generalized “infrastructure” security software for the port environment
Software Architecture

Domain-Specific Configuration Parameters

Port Sec User Interface

Parameters

Middleware

Port Security Risk Modeling Infrastructure

Parameters

Dynamic Data

Model Parameters

Parameters

Port Resource Allocations

Port Operating Environment

Internally maintained databases

Externally maintained databases

# of patrol cars, patrol boats, inspection stations, cameras, etc.,

ACTA, e-Modal, PierPass, Marine-Exchange, AVL, ATMIS, Sonar/Radar Info

# of ships in berths, events, auto traffic conditions, etc.
Potential PortSec Interface in JCCC

- Video Systems
- ACC
- Analytics
- SMP
- Sonar/Radar
- PortSec User Interface
- PortSec Middleware and Modeling Infrastructure
- PortSec Internal Data Sources
- External Data Sources

ACTA, eModal, PierPass, Marine-Exchange, ATMIS, AVL

Direct access to data (or through SMP)?

PortSec Software
Existing JCCC system components
Internally maintained databases
Externally maintained databases
Tactical Usage: Port Security Officer

- List of Available/Used Countermeasures/Resources
- Calculated Risk for the Highlighted Region
- Resources Assigned to the Highlighted Region
- Resource Allocation Options
- Critical Regions Color Coded to Reflect Calculated Risk
- Optimize Available Here
Strategic Usage: Port Security Analyst

- Rail Line
- Surveillance Station
- Cargo Truck
- Crane
- Highway/Street (Movement)

Available Resources

Results from Run:
- Throughput: 100 TEUs/hour
- Cost: $400/TEU
Strategic Usage: Port Security Analyst

Available Scenarios For “What-if” Comparisons

Scenario Performance Parameters

Scenario A:
Perf: 45 TEUs/hour
Implement Cost: $10M
Maint Cost: $1M/yr
Est. Loss: $3B

Scenario C:
Perf: 38 TEUs/hour
Implement Cost: $15M
Maint Cost: $2M/yr
Est. Loss: $3B
Near Real-time Marine and Land Traffic

Marine Traffic

Vehicle Traffic
Port Operations Economic Impact Modeling:
CM acquisition and maintenance costs, port operation costs

- Generation of Scenario: Parameters, Characteristics
- Port or Terminal Model Simulation: Macroscopic or Microscopic
- Microscopic Road Network Simulator using VISSIM
- Impact on Road Network
- Port or Terminal Productivity: effect on flows; idle times of equipment, effect on operations, labor, power etc.
- Terminal Cost Model; Countermeasure Costs
- Economic Assessment
Why PortSec?

• PortSec is focused on the terrorist scenarios that may interfere with the capabilities and missions of ports (as business entities, transport hubs, etc.,) and the ports’ various partners (e.g., carriers, stevedores, truckers) in performing these tasks and accomplishing these goals
  – Ports and similar operations are composed of many different components (e.g., terminals, bridges, inspection points, etc.,), agencies, businesses, and interactions between these "systems"
  – PortSec focuses on the “system of systems”

• PortSec supports both tactical and strategic planning
  – These operations complement each other
  – Allows “what-if” cost-benefit analyses

• PortSec scales from local (e.g., terminal operations) to overall port operations.
  – For example, we calculate a risk assessment for a specific terminal and for the complete port complex.
Next Steps

- Complete development of prototype tactical-only system (May 2009)
  - User interface and middleware modeling infrastructure
  - Incorporate stakeholder feedback
- Refine port risk models (Aug/Sept 2009)
  - Terminal, port, and transportation models
  - Execute selected scenarios
- Complete development of combined tactical and strategic port security prototype system (Winter 2010)
  - Integrate terminal, port, and transportation models into modeling infrastructure
  - Beta test with stakeholders
  - Incorporate stakeholder feedback
- Integrate system into existing port operations (Fall 2010)
Summary

• Completed project requirements and system design
• Developed a generic “infrastructure” security design and refined it for port operations
  – Generic “infrastructure” design allows for system use in other domains
• Produced an initial demonstration tactical prototype and presented to port officials
  – Positive feedback
• Currently extending demonstration prototype to include support for both tactical and strategic operations
  – Includes terminal, port, and transportation model refinements through scenario runs
• Planned Fall/Winter 2010 insertion of system into Ports of LA and Ports of Long Beach operations
  – Working closely with port officials throughout the development and testing effort with this goal in mind