PortSec: Port Security Risk and Resource Management System

Michael D. Orosz  
University of Southern California, mdorosz@isi.edu

Liz Lennon  
Informational Sciences Institute, University of Southern California

Follow this and additional works at: http://research.create.usc.edu/project_summaries  
Part of the Risk Analysis Commons

Recommended Citation  
http://research.create.usc.edu/project_summaries/110

This Article is brought to you for free and open access by CREATE Research Archive. It has been accepted for inclusion in Research Project Summaries by an authorized administrator of CREATE Research Archive. For more information, please contact gribben@usc.edu.
"This research was supported by the United States Department of Homeland Security through the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) under Cooperative Agreement 2007-ST-061-RE0001. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the United States Department of Homeland Security or the University of Southern California."

Cooperative Agreement No. 2010-ST-061-RE0001
Department of Homeland Security

15 October 2012
ABOUT CREATE
The National Center for Risk and Economic Analysis of Terrorism Events (CREATE) was the first university-based Center of Excellence (COE) funded by University Programs of the Science and Technology (S&T) Directorate of the Department of Homeland Security (DHS). CREATE started operations in March of 2004. This annual report covers the eighth year of CREATE funding from October 2011 to September 2012, the first year under Cooperative Agreement 2010-ST-061-RE0001 from DHS. While the text of this report focuses on the eighth year, all data tables, publications, lists of participants, students, and presentations and events are cumulative from the inception of CREATE.

CREATE’s research mission is to develop advanced models and tools for risk assessment, economic assessment, and risk management to counter terrorism. CREATE accomplishes this mission through an integrated program of research, education, and outreach, spanning the disciplines of economics, psychology, political science, industrial and systems engineering and information science. CREATE develops models, analytical tools, methodologies and software, and tests these tools in case analyses, representing critical homeland security investment and policy decisions.

Due to the cross-cutting nature of research in risk, economics, and risk management, CREATE serves the need of many client agencies at the DHS, including the Transportation Security Agency, Customs and Border Protection, Immigration and Customs Enforcement, FEMA and the US Coast Guard. In addition, CREATE has developed relationships with clients in the Offices of National Protection and Programs, Intelligence and Analysis, General Council, Health Affairs, and Domestic Nuclear Detection. Using a mix of fundamental and applied research, CREATE faculty and students take both the long-term view of how to reduce terrorism risk through fundamental research and the medium-term view of how to improve the cost-effectiveness of counter-terrorism policies and investments through applied research.

Please visit www.create.usc.edu for more information.
1 Executive Summary

The primary focus of this research is to develop a risk assessment and security resource allocation system targeting seaport operations. Although initially focused on the Ports of Los Angeles and Long Beach (POLA/LB), this project addresses a major challenge faced by operators of all seaports; determining the proper balance between increasing seaport safety, maintaining or maximizing business throughput and minimizing the impact on the environment. Often these three objectives are at odds with one another (e.g., increasing safety by implementing additional scanning technologies can lead to container/truck traffic slow-down with a corresponding increase in pollutants spewed into the air). The Port Security Risk and Resource Management System (PortSec) is designed to address this challenge. When fully implemented, PortSec will support both tactical day-to-day security allocation decision-making and long-term strategic security planning. The system is intended to support two types of users:

- Port Security Officer – tactical responsibility for daily security arrangements with 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

For tactical usage (Figure 1), PortSec will provide up-to-date risk assessment for both identified areas of interest (AOIs) and for the overall port complex. These assessments reflect current countermeasure resource allocations, planned and unplanned events, and collected intelligence on possible threats. These assessments are frequently updated to reflect changing port conditions and assessed threats. The port security officer attempts to reduce overall risk by re-allocating available counter-measure resources. After each adjustment, the system calculates a new risk assessment score – providing near real-time feedback to the port security officer. In addition, the port security officer can anticipate near-future events based on projected events, counter-measure resource allocation and availability, and intelligence about possible future threats. The advantage of the tactical PortSec is that the decision-maker can quickly and dynamically visualize where high risk areas exists and, just as importantly, quickly discover newly exposed areas (i.e., increased risk) that may result when counter-measure resources are shifted...
from what was a low-risk AOI to a high-risk AOI, now leaving the once low-risk AOI exposed to potential attack.

Figure 1: Tactical PortSec. The shaded regions, which can change in color from red to yellow or green, represent Areas of Interest (AOIs) to the Port Community. The color of each region represents the assessed risk (red – high, yellow – moderate, green – low) of an attack due to the current port operating environment. Risk can be reduced by reallocating the available security resources.

In Year 8, building on the previous year’s effort, Tactical PortSec was successfully extended to support real-time incident response. During this effort the PortSec team realized the goal of linking PortSec to the DHS-funded Unified Incident Command and Decision Support (UICDS) system developed and maintained by SAIC.

Keyword 1: Port Security
Keyword 2: Business Resiliency
Keyword 3: PortSec
2 Research Accomplishments
The PortSec project is composed of following three sub-projects:

- Extension of PortSec middleware and user interface
- Extension of risk assessment and resource allocation module
- Extension and improvement of additional models related to road transportation networks and their relationship to the calculation of possible incident response times.

2.1 Extension of PortSec Middleware and User Interface
This sub-project is a continuation of previous years’ efforts to develop the middleware to link all the system components (Figures 2 and 3) and the user interface to allow decision-makers and analysts to use the system from a single user interface. In Year 8, building upon the previous year’s efforts, work focused on implementation of the interfaces and necessary infrastructure to support interactions with the UICDS system (Figure 4).

![Figure 2: System of Systems Software Solution](image-url)
Figure 3: Alternate view of specific data sets and models connected through middleware of the PortSec platform.

Figure 4: PortSec – UICDS System In Incident PortSec. ConOps: Incident Commander (1) establishes incident alert. Blue Force (2), vessel and traffic locations (3) are extracted by the POLA PortSec client. PortSec calculates risks based on the current operating environment and threat vectors and provides this information to the law enforcement community via UICDS servers (4). Incident information is stored (5) for later use.
ConOps: Each law enforcement agency is allocated a UICDS server. Incident events are generated by the appropriate UICDS server and sent to the appropriate PortSec service (item 1 in Figure 4). Based on the incident event, current blue force positions (item 2 in Figure 4), current surface (ground and water) traffic (item 3 in Figure 4) and the importance of each AOI in the port complex, risk is calculated and the appropriate indicators are provided to the user via the PortSec user interface (Figure 1). Based on this information, the decision-maker reallocates resources to reduce risk of attack and sends this decision to the other stakeholders involved in this event via the UICDEs servers (item 4 in Figure 4). Finally, to support after-action analysis, decisions made along with supporting information are stored (item 5 in Figure 4). As an example, consider the following overview of a usage scenario. After the user is notified of an incident, which is equivalent to item 1 in Figure 4, he or she select the ‘Incident’ tab to create, i.e. report, an incident as indicated in Figure 1. Next the user can populate the fields in the ‘Define Incident’ menu shown (Figure 5).

Figure 5: Image of ‘Define Incident’ menu.

In figure 5, the location field corresponds to the area of interest (AOI) where the incident event is located. In the ‘Define Incident’ menu the priority corresponds to the number and potentially type of resources that will be required to satisfactorily respond to the incident underway. For example, a bomb threat at the cruise terminal may be given a high (5) priority and require multiple police units and bomb detection canines. After the priority is assigned, based on the assessment of current information, the resources can be reallocated to minimize overall risk, which is capture as item 4 in Figure 4. Throughout the incident all the actions and assignments related to the incident, including priority and location, are logged (Figure 6) for after action reporting activities corresponding to item 5 in Figure 4.

For the Year 8 effort, the data sources for information (e.g., Marine Exchange, CalTrans, etc.) that were negotiated in the previous year have been undergoing integration with for the extended PortSec platform. This effort continues and information from various sources continues to be simulated for demonstration and testing purposes.
2.2 Extension of Risk Assessment and Resource Allocation Module

This sub-project is a continuation of previous years’ efforts to refine and improve the risk assessment and resource allocation technology in the PortSec software. In Year 8, the focus not only continued with the extension of the capabilities to support real-time or near real-time incident response, but also on investigating a new approach to the risk assessment based on a Bayesian network analysis in which the risk is related to the likelihood of a successful attack or scenario transpiring given the information regarding the network of available interdiction options. This is a new risk assessment being explored in parallel to the improvement of the risk assessment model currently in place which determines risk based on data sources from the United States Coast Guard MAST study. This approach may provide a more flexible infrastructure that more readily enables PortSec to make calculations, such as incident response, which are only marginally supported in the initial version of the PortSec software.

To help inform the extension of the risk assessment and resource allocation module, members of the PortSec team immersed in POLA Police operations (sea marshals, bike patrol, HAZMAT response, dive team, marine units, etc.). The purpose of these immersions was to help inform the researchers on the day-to-day operations and challenges faced by port security law enforcement personnel.

2.3 Extension and Improvement of Transportation Models for Response Time Determinations

A major challenge when confronting an incident is determining which resources should respond. A major factor behind this decision is the availability and capabilities of the required resources. In Year 8, the focus of the team was in extending the existing VISSUM-based transportation model to support short distance possible calculations. During an incident in the seaport, the closest resource may not necessary be the correct resource to deploy due to traffic impediments. For example, traffic congestion at the end of the work day may impede movement of first responder resources to an incident. Work is continuing on modifying the transportation model to support distance calculations.

3 Applied Relevance

2.1 Extension of PortSec Middleware and User Interface with UICDS Compatibility

PortSec allows decision-makers and analysts to undertake trade-off analyses to determine which security resources to allocate that best address reducing risk of attack while simultaneously minimizing the impact on both business operations and the environment. Due to the complexity of the mission space, there is no one model that does everything. Relying on a set of disparate models, each with different input/output needs and operating conditions increases the analyst’s workload. The solution is a system of systems approach that combines models that address different areas of the mission space into a single system. The PortSec middleware and user interface provide this utility.

2.2 Extension of Risk Assessment and Resource Allocation Module

Extending the tactical capabilities of PortSec to handle real-time incident responses allows stakeholders (e.g., law enforcement, security personnel, etc.) to avoid over-allocating resources to service the incident and leaving portions of the port complex exposed. Although law enforcement and other first responders have established policies and procedures and train to avoid over allocation of resources and to provide a balance response to various incidents, after action reports (based on discussions with subject matter experts) indicate that in many cases, these first responders still over allocate and leave important portions of the physical infrastructure exposed. Incident PortSec addresses these challenges.
4 Collaborative Projects

In addition to real-time information on vessel movements, ground transportation and blue force tracking, another key component of the PortSec decision-making is intelligence on adversarial movements and plans. Knowledge of potential threat vectors and timelines will help in calculating risks from attack and how best to allocate resources to reduce those attacks. The PortSec team is collaborating with the USC CREATE iSARs (Integrated Suspicious Activity Reports) team in establishing 1) defining the types of SARs PortSec requires and 2) defining an interface between PortSec and iSARs. Currently, the focus is on objective one (defining the types of SARs PortSec requires).

In addition, the PortSec team continues to explore teaming with the USC-ISI DETER cyber testbed team to develop a combined Cyber-Physical Infrastructure-Economic system. This system will provide decision-makers with tools to explore the consequence that cyber attacks and the various countermeasures deployed to prevent them have on seaport infrastructures and the economic impact that ripples across the Nation due to a successful attack.

The PortSec team has also begun exploration of a PortSec like system in other domains, such as university campuses, which also have multiple regions of interest and restrained security resources. More specifically, a collaboration for a project with the working title of InfraSec between CREATE and the Ohio State University Department of Public Safety (DPS) is being pursued to investigate the application of a PortSec like risk assessment system for their campus.

5 Research Products

<table>
<thead>
<tr>
<th>Research Products (Please detail below)</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>5a # of peer-reviewed journal reports published</td>
<td>0</td>
</tr>
<tr>
<td>5a # of peer-reviewed journal reports accepted for publication</td>
<td>1</td>
</tr>
<tr>
<td>5a # of non-peer reviewed publications and reports</td>
<td>0</td>
</tr>
<tr>
<td>5a # of scholarly journal citations of published reports</td>
<td>0</td>
</tr>
<tr>
<td>5b # of scholarly presentations (conferences, workshops, seminars)</td>
<td>3</td>
</tr>
<tr>
<td>5b # of outreach presentations (non-technical groups, general public)</td>
<td>x</td>
</tr>
<tr>
<td>5c # of products delivered to DHS, other Federal agencies, or State/Local</td>
<td>0</td>
</tr>
<tr>
<td>5c # of patents filed</td>
<td>0</td>
</tr>
<tr>
<td>5c # of patents issued</td>
<td>0</td>
</tr>
<tr>
<td>5c # of products in commercialization pipeline (products not yet to market)</td>
<td>0</td>
</tr>
<tr>
<td>5c # of products introduced to market</td>
<td>0</td>
</tr>
</tbody>
</table>

2.1 Publications and Reports


2.2 Presentations


2. Orosz, M., Maya, I., USC CREATE Port Security Risk and Resource Management
System (PortSec), presented at the World Conference on Transport Research Society (WCTRS), Special Interest Group 2 - Key Developments in the Port Maritime Sector, 21-22 May 2012, Antwerp, Belgium


6 Outreach

2.1 Models, Databases, and Software Tools and Products

<table>
<thead>
<tr>
<th>Date Delivered</th>
<th>Item</th>
<th>Agency Receiving Product</th>
<th>Agency POC</th>
<th>Commercialization Status (D-delivered, P-Pipeline, M-Market)</th>
</tr>
</thead>
<tbody>
<tr>
<td>30 Sept 2012</td>
<td>PortSec 1.5 (Demonstration Prototype of Incident PortSec)</td>
<td>CREATE</td>
<td>Isaac Maya</td>
<td>P</td>
</tr>
</tbody>
</table>

Currently (as reported in Year 6), PortSec 1.0 – a demonstration prototype – has been demonstrated to both POLA and POLB. The team is currently working on PortSec 1.5.

The PortSec software, when completed (version 2.0) has commercialization potential. Although currently targeted for POLA/LB application, the system is designed and is being developed to be used in any port complex or similar infrastructure environment.

We are currently in the process of filing IP paperwork on the technology

2.2 Education and Outreach Products

<table>
<thead>
<tr>
<th>Education and Outreach Initiatives (Please detail below)</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td># of students supported (funded by CREATE)</td>
<td>1</td>
</tr>
<tr>
<td># of students involved (funded by CREATE + any other programs)</td>
<td>0</td>
</tr>
<tr>
<td># of students graduated</td>
<td>0</td>
</tr>
<tr>
<td># of contacts with DHS, other Federal agencies, or State/Local (committees)</td>
<td>8</td>
</tr>
<tr>
<td># of existing courses modified with new material</td>
<td>0</td>
</tr>
<tr>
<td># of new courses developed</td>
<td>0</td>
</tr>
<tr>
<td># of new certificate programs developed</td>
<td>0</td>
</tr>
<tr>
<td># of new degree programs developed</td>
<td>0</td>
</tr>
</tbody>
</table>

Students supported by CREATE+ any other programs
- Carl Southwell, Ph.D. Graduate Student

DHS, Local/State Contacts:
- Joe DiRenzo III, Ph.D. Deputy, Ops Plans Branch Coast Guard Atlantic Area (Axo), USCG
- CAPT Roger Leferriere, Commander, Los Angeles – Long Beach, USCG
- CAPT John Caplis, Deputy Commander, Los Angeles – Long Beach, USCG
- George Cummings, Director of Security, Port of Los Angeles
- CAPT Curtis Thompson, Port of Los Angeles Police
- CAPT Richard B. McKenna (ret), Marine Exchange
- LT Rudy Zupanc, CCI, Strategic Analysis Intelligence Center, Ohio State Highway Patrol