A Model for Security Evaluation of a Port Storage Area Against Theft in a Container Line Supply Chain

Da-Wei Tang*, Dong-Ling Xu, Jian-Bo Yang and Yu-Wang Chen
Manchester Business School
The University of Manchester, Manchester M15 6PB, UK
***EMAIL: Dawei.tang@postgrad.mbs.ac.uk**

Abstract: Security analysis is very important in Container Line Supply Chain (CLSC) operation as CLSC is a dominant way to transport cargo worldwide and at the same time it is also subject to many threats. In this paper, an evidence based approach for security evaluation of a port storage area against theft in CLSC is proposed. The approach includes evaluation criteria in a hierarchical structure, belief structures to facilitate evidence based evaluation information management, and a belief Rule-base Inference Methodology using the Evidential Reasoning (RIMER) algorithm. The approach is capable of rationally dealing with different types of uncertainty in the security evaluation process. Both the criteria hierarchy and the application of RIMER are validated through a real world case study.

Keywords: Container Line Supply Chain, Security evaluation, Theft

I. Background

Since their introduction in 1950s, containers have become increasingly important in world cargo transportation as it enables smooth and seamless transfer of cargo between various modes of transportation, and thus makes cargo movement much more efficient [15]. It is estimated that around 95% of the world's trade moves by containers [9] and approximately 250 million containers are shipped annually around the world [3]. Therefore, Container Line Supply Chain (CLSC), which transports cargo in containers, is a predominant way to ship cargo around the globe [10].

Meanwhile, CLSC is subject to many threats due to its complexity, vulnerability and inadequate preventative measures. Among the threats, cargo theft is one of the most common threats, which leads to about $40 billion direct cost per year, with indirect costs many times higher worldwide [4]. In addition, besides economic loss, theft can also cause severe consequence regarding human security if the stolen cargo is hazardous (poisonous, explosive, radioactive etc). The worst situation is that a group of terrorists steal a certain amount of hazardous cargo on purpose, and the stolen cargo is used as a weapon of terrorism. On the other hand, with the consideration of criminals' convenience, most thefts occur when cargo is at rest instead of in motion. Regarding the places where cargo is at rest in CLSC, port is a key region. Therefore, cargo theft in port storage area is one of the most important threats in CLSC.

II. Current Research in Security Issues against Theft

Regarding current research on cargo theft, most literature focus on the problem of theft prevention by introducing software systems, hardware facilities or a set of managerial measures, for example: a cargo theft information processing system is introduced by Toth [11]; the development of fast-working, nonintrusive X-ray and detection devices are suggested by Badolato [2] to help to ensure cargo security; and, a set of managerial measures are proposed by Anderson [1] to prevent cargo theft. In addition to academic papers, there are also some regulations aiming at theft prevention, e.g., the Freight Security Requirement [12] and the Trucking Security Requirement [13] issued by Technology Assets Protection Association.

However, most of the current literature are not specifically aimed at theft in ports, and more importantly, little attention has been paid on how to evaluate security level of a certain port against theft. Without the evaluation, preventative measures against theft and the corresponding resources to support the preventative measures may not be allocated systematically and efficiently.

Therefore, it is necessary to develop a model to evaluate security level of a port storage area against theft.

III. Proposed Model to Evaluate Security Level of a Port Storage Area against Theft

Definition of Security

To evaluate security level of a port storage area, it is very important to firstly clarify the concept of security and its difference from other related terms. Among the various definitions in current literature [5] [6] [7] [8], the definitions in [5] will be used here:

- Safety: the degree to which accidental harm is prevented, detected, and reacted to;
- Security: the degree to which malicious harm is prevented, detected, and reacted to;
- Hazard: a situation that increases the likelihood of formation of one or more accidental harm;

- Threat: a situation that increases the likelihood of formation of one or more malicious harm.

Hierarchical Structure of Assessment Criteria

Based on the above definitions, three components are proposed to model security, namely, Likelihood, Vulnerability and Consequence.

Likelihood refers to the possibility that a theft may happen, which can be further described by Intention and Capability Required of the theft. Intention is the motivation of criminals to commit a theft, it is usually determined by the potential benefits the criminals can get if the theft is successful, which is highly dependent on the type of cargo stored in the port storage area. On the other hand, Capability Required indicates the skills or tools the criminals must acquire to commit a theft, it is also relevant to the type of cargo stored: If the cargo need to be carried by trucks or even cranes, the Capability Required will be very high. Based on the above explanation, the Likelihood of theft in a port storage area will be very high if the cargo stored in such area can bring great benefits to the criminals and only basic skills and tools are needed to steal them.

Vulnerability is the feature of the port storage area which can influence the likelihood of the presence of the potential consequence after the theft happens. The feature here refers to both Physical Feature of the port storage area and Intervention Activities conducted by relevant staff. Physical Feature includes Employee Feature, Facility Feature, etc., while Intervention Activities include Preventative Measures and Responsive Measures. Further, Facility Feature, Preventative Measures and Responsive Measures can be decomposed into more detailed levels of criteria until the criteria are measurable. For example, Facility Feature include Hardware Feature and Software Feature, Hardware can be decomposed into Control Facility and Monitor Facility, Monitor Facility can be categorized as CCTV Facility and Lighting Facility, and CCTV Facility can be described by CCTV Coverage, CCTV Media, CCTV Mode, etc.

To model the Consequence component, the following dimensions are proposed in the context of theft in port storage area:

- Human Cost: physical and psychological harm to person involved in the whole supply chain;
- Financial Cost: monetary loss of the port which suffers from theft;
- Corporate Image Cost: reputation loss, loss of customers of the port which suffers from theft;
- Economic Losses: monetary loss of the port's partners along the CLSC;
- Environmental impacts: degradation to the quality of the environment or to endangered species.

Normally, theft can only lead to Financial Cost, Corporate Image Cost and Economic Losses. However, if the cargo stolen is hazardous, it may also lead to Human Loss and Environmental Impacts.

Based on the discussion above, the security level in a port storage area against theft can be modeled using a hierarchical structure of criteria, in which, the criterion at the top of the structure is the overall security level and the criteria at the bottom are measurable criteria.

To assess and generate the security level of a port, information to measure each criterion at the bottom level of the hierarchy need to be collected and aggregated.

Measurement

As a port storage area is operating under a very complex environment, there could be uncertainty in the information collected and judgments made when the security of the port is assessed. In addition, some unknown (or ignorance) may exist in the data collected regarding the security of the port in some areas (or criteria). Further, the nature of an evaluation criterion can be qualitative or quantitative. Some of them have to be evaluated by subjective judgments whiles others by numerical values.

To model various types of uncertainty in a unified format including ignorance and subjectivity in the assessment and measurement data, the concept of belief structure [14] is introduced. . For example, to model "CCTV Coverage" of a port, the following belief structure can be used: {(Wide, 0.8), (Moderate, 0.2), (Limited, 0)}, in which, 'wide', 'moderate' and 'limited' are the grades used to describe "CCTV coverage", and the number 0.8, 0.2 and 0 are the belief degrees to which "CCTV coverage" is assessed to the corresponding grades, which may indicate that 80% of its CCTVs can cover a "Wide" range of area and 20% of them a "Moderate" range. In the example, the sum of the belief degrees is 1, which means the information or judgment on "CCTV coverage" is complete. If not, it indicates that there is ignorance in the assessment.

On the other hand, there are some other criteria which can be described by numerical or categorized values. For example, Fence Height is measured by precise value, while CCTV Media is measured by categorized values, either VCR or DVR.

Inference

Among the existing inference schemes, a belief Rule-base Inference Methodology using the Evidential Reasoning approach (RIMER) will be applied. The approach is based on a Belief Rule Base (BRB), an example of which regarding the relation among Likelihood, Intention and Capability Required is as follows:

IF Intention is High and Capability Required is Low, THEN Likelihood is {(High, 1)}
IF Intention is High and Capability Required is High, THEN Likelihood is {(High, 0.6), (Low, 0.4)}
IF Intention is Low and Capability Required is Low, THEN Likelihood is {(High, 0.3), (Low, 0.7)}
IF Intention is Low and Capability Required is High, THEN Likelihood is {(Low, 1)}

In the consequence part of the above BRB, ‘High’ and ‘Low’ are the grades used to describe or measure Likelihood and the number after each grade is the belief degree to which Likelihood is assessed to the corresponding grade. One of the advantages of BRB over traditional rule base is: BRB can describe the knowledge in a more accurate way with the introduction of belief degrees in the consequence.

Other reasons why RIMER is selected as a tool to conduct the inference regarding security analysis in CLSC include that:

- Using belief structures, RIMER can accommodate various forms of information, including precise values, categorized values, and fuzzy values, and
- RIMER can rationally deal with complete and incomplete information under a unified framework and the inference result of RIMER can reveal the effect of the ignorance in the original data.

IV. Validation

The hierarchical structure of assessment criteria and the inference method proposed above have been validated by a real case study carried out in port storage area in Port of Liverpool, and the evaluation outcome generated is consistent with the actual opinions of the Port Security Officer in the Port.

V. Conclusion and future research

Facing the problem of theft in port storage area within a CLSC, a hierarchical structure of criteria is proposed to evaluate the security level against theft in a port storage area in CLSC. Based on the structure, RIMER is then applied to handle the various kinds of uncertainties involved during the evaluation process and to generate the evaluation result. Such a result can then be used as a basis to improve security level of the port storage area against theft.

In future, further research can be conducted along the following directions:

- The hierarchical structure of assessment criteria proposed here needs to be validated with more real cases and necessary refinement is needed after the validation;
- The method to evaluate security level of a port storage area against theft can be expanded to consider security level of the whole CLSC under various threats with the consideration of features of each threat, features of the members involved in CLSC as well as dependencies among the members in CLSC.

References

[1] Anderson, B., 2007. Securing the Supply Chain-Prevent Cargo Theft. Security, Vol. 44, No. 5, 56-59.

[2] Badolato, E., 2000. Cargo Security: High-Tech Protection, High-Tech Threats. Transportation Research News, Vol. 211, 14-17

[3] DHS, 2007. Strategy to Enhance International Supply Chain Security. DHS Report.

[4] Eyefortransport, 2002. Cargo Security Overview: technologies, government and customs initiatives, Global eye for transport research.

[5] Firesmith, D.G., 2003. Common Concepts Underlying Safety, Security, and Survivability Engineering. Technical Report CMU/SEI-2003-TN-033, Carnegie Mellon Software Engineering Institute

[6] H.H. Willis and D.S. Ortiz, “Evaluating The Security Of The Global Containerized Supply Chain”, RAND Technical Report Series, TR-214-RC, 2004

[7] Jonsson, E., 1998. An integrated framework for security and dependability. In Proceedings of the New Security Paradigms Workshop, Charlottesville, VA, 22–25

[8] Lau, O., 1998. The ten commandments of security. Computers & Security, Vol. 17, Issue. 2, 119–23

[9] OECD, 2003. Security in Maritime Transport: Risk Factors and Economic Impact. OECD Report.

[10] OECD, 2005. Container Transport Security across Modes. OECD Report.

[11] Toth, G. E., 1998. CargoTIPS: an innovative approach to combating cargo theft. In SPIE Conference on Enforcement and Security Technologies, Vol. 3575, Boston, U.S., 315-19

[12] Transported Asset Protection Association, 2009. Freight Security Requirements. Transported Asset Protection Association Report.

[13] Transported Asset Protection Association, 2009. Trucking Security Requirement. Transported Asset Protection Association Report.

[14] Yang, J. B., Liu, J., Wang, J., Sii, H. S., Wang, H. W., 2006. A belief rule-base inference methodology using the evidential reasoning approach – RIMER. IEEE Transactions on Systems, Man, and Cybernetics – Part A, Vol.36, No.2, 266- 285

[15] Wydajewski, K.J., White, B.L., 2002. Processes and techniques for providing critical data to first responders to maritime security incidents. In Oceans 2002 IEEE/MTS Conference Proceedings, Vol.2, Mississippi, U.S., 1180- 90.

Background of Authors

Da-Wei Tang received his B.Eng and M.Eng degree from Huazhong University of Science and Technology, Wuhan, China in 1998 and 2002 respectively. He is now a PhD candidate in Manchester Business School, the University of Manchester. His research interests include: risk analysis, security analysis, Multi Criteria Decision Analysis, supply chain, new product development, etc.

Dong-Ling Xu received the B.Eng degree in electrical engineering from Hunan University, Changsha, China, in 1983 and the M.Eng and PhD degrees in system control engineering from Shanghai Jiao Tong University, Shanghai, China, in 1986 and 1988, respectively. She is currently a senior lecturer in decision and system sciences in the Manchester Business School, University of Manchester, UK. Her current research interests include quality modeling, fault diagnosis, risk management, etc.

Jian-Bo Yang received the B.Eng and M.Eng degrees in control engineering from the North Western Polytechnic University, Xi’an, China, in 1981 and 1984, respectively, and the PhD degree in systems engineering from Shanghai Jiao Tong University, Shanghai, China, in 1987. He is Professor of Decision and Systems Sciences and Director of the Decision Sciences Research Centre at the Manchester Business School, the University of Manchester**.** His current research interests include decision making, risk modeling and analysis, production planning and scheduling, quality modeling and evaluation, supply chain modeling and supplier assessment, and the integrated evaluation of products, systems, projects, policies etc.

Yu-Wang Chen received the B.Eng. degree in electrical engineering from Bengbu Tank Institute, Anhui, China, in 2002 and the M.Eng. and Ph.D. degrees in control engineering from Shanghai Jiao Tong University, Shanghai, China, in 2005 and 2008, respectively. He is currently is a Postdoctoral Research Associate in the Decision and Cognitive Sciences Research Centre in the Manchester Business School, University of Manchester, U.K. He was a Postdoctoral Research Fellow in the Department of Computer Science, Hong Kong Baptist University, H.K. His current research interests include intelligent decision analysis, risk and safety analysis, supply chain management, optimization theory and algorithms, self-organizing systems, etc.