Trust Management and Attribute-Based Access Control Framework for Protecting Maritime Cyber Infrastructure

Yunpeng Zhang[1], Izzat Alsmadi[2], Yi Qi[3] and Zhixia Li[4]
[1]*Information Science Technology Department, University of Houston, Houston, U.S.A.*
[2]*Department of Computing and Cybersecurity Texas A & M University San Antonio, San Antonio, U.S.A.*
[3]*Department of Transportation Studies, Texas Southern University, Houston, U.S.A.*
[4]*Department of Civil and Architectural Engineering and Construction Management, University of Cincinnati, Cincinnati, U.S.A.*

Keywords: Security, Maritime Cyber Infrastructure, Attribute-Based Access Control, Framework.

Abstract: The modern world depends on maritime supply chains to sustain flows of international commercial, industrial, and economic activities. As the maritime supply chain heavily utilizes cyber operations to manage communications and physical processes, maritime cybersecurity emerges as an imperative aspect for maritime safety and security. The maritime cyber infrastructure displays distributed, heterogeneous, networked, and volatile characteristics. This article first studies the effectiveness of the mechanism of traditional access control systems for maritime cyber infrastructure. The research also examines the shortcomings associated with the existing network wide access control and identity theories to develop solutions. In order to develop a suitable method for the maritime context, the paper presents an Attribute-Based Access Control (ABAC) framework which is adaptable and highly scalable for the complex maritime cyber space. The analytical results show that implementing the new framework can enhance the access control of the maritime cyber infrastructure.

1 INTRODUCTION

Nowadays, more critical infrastructure systems are managed through cyber operations. Cybersecurity, as a result, has become a crucial operational domain for these critical infrastructure systems to prepare for potential cyber-attacks, ensure trustable services, repair damages, and improve security and operational performance. Breaches in the cyber space of a critical infrastructure may lead to a variety of consequences. Specifically, cyber-attacks can cause disruptions of the infrastructure systems, leakage of crucial information of people and assets, financial losses, economic damages, and even injuries or losses of lives.

The critical infrastructure studied in this research is the maritime cyber infrastructure. The maritime transportation system is categorized by the experts in public and private sectors as a critical infrastructure system. In any single moment, tremendous values of commodities, merchandises, as well as many people, depend on the maritime infrastructure to travel in global supply chains to support the economic, military, or humanitarian systems. The cyber space of the maritime infrastructure is an extremely complex "system of systems". The maritime cyber infrastructure includes, but is not limited to: networked facilities, software programs, operating systems, database servers, large-scale data storage, and local/remote instruments, wired/wireless sensors, sophisticated workforce, personnel, and wired/wireless and/or satellite networks that connect to other critical infrastructures. This globally distributed, interconnected ecosystem presents unique security challenges to control both physical and cyber maritime operations.

Maritime cyber space has been shown to be highly vulnerable from attacks targeted by various adversarial groups. The attacks may be performed by hackers, criminals, terrorists, international forces, and so forth. The recent maritime attacks caused the global economy around $7 billion USD and multiple losses of lives.(A. Bowden and Lee, 2010) According to multiple reports (Keefe, 2012; Hayes, 2016; Belmont, 2015; Wagstaff, 2014), the emerging organized cyber attacks presents new threats to both cyber and physical maritime operations. A hacking incident in 2001 caused severe Denial of Service problems for the Port of Houston authority (BBC, 2003). In 2011-2013, in-

Zhang, Y., Alsmadi, I., Qi, Y. and Li, Z.
Trust Management and Attribute-Based Access Control Framework for Protecting Maritime Cyber Infrastructure.
DOI: 10.5220/0012126500003538
In *Proceedings of the 18th International Conference on Software Technologies (ICSOFT 2023)*, pages 534-539
ISBN: 978-989-758-665-1; ISSN: 2184-2833

ternational drug traffickers worked with local hackers to intrude the maritime cyber spaces at the Port of Antwerp, Belgium. The criminals IT weaknesses and manipulate sensitive data such as shipment characteristics and pickup schedules to conceal drugs and illegally import them without being detected.

An alarming trend is the emerging cyber-physical attacks against maritime ICT systems. In the Antwerp case, hackers breached physical communication machines to intrude the port's database. These multiplex, organized attacks underscore the importance to secure the maritime cyber operations in the first space to safeguard the physical safety of people and goods.

Finding effective solutions and countermeasures against cyber-attacks now becomes an urgent task for maritime stakeholders. (Vanek et al., 2013) In a vulnerable cyber space, access control is a fundamental mechanism to prevent not only accidental but also malicious violations of security requirements. An access control system regulates user access to resources. It defines the conditions under which to whom access to resources can be granted. Each access request will result in an access decision such as permit or deny.

This research contributes to the maritime supply chain security literature by developing a system of trustable access control. Within the maritime supply chain, data always moves between extensively distributed machines and cannot possibly be controlled by a single, trustable system. To address this challenge, this paper builds an access control framework which can simultaneously achieve efficiency.

The remaining of the paper is organized into three additional sections. In section 2, the related work is discussed to provide the basis for framework and approach development. Section 3 introduces the access control framework for protecting maritime cyber infrastructure. Section 4 presents the concluding remarks and directions of future work.

2 RELATED WORK

In the area of maritime operations and information security literature, papers regarding maritime cybersecurity, especially topics on access control, are few in numbers. In contrast, there is a wealth of publications associated with access control innovations and applications (C. Wang and Gupta, 2023; Singh et al., 2022; Jeong and Li, 2022). Accordingly, we extensively reviewed recent access control publications deemed relevant to maritime cyber operations.

The authors examine and discuss the literature through the lens of the computer security policy (CSP), the supreme principle to govern the goals and elements of the computer systems within an organization. (Li et al., 2015) For a normal maritime supply chain, multiple CSPs may co-exist because of the participation of various supply chain partners. The formulation of any CSP is important because it defines what it means to be secured within the organization boundaries.

In the following discussion, we first discuss the recent trends of maritime cyber-attacks. Secondly, we discuss the state-of-the-art research on access control and gaps and potentials for applications in maritime cyber spaces. Finally, the CSPs of a trust management system to verify maritime cybersecurity is presented (Panos et al., 2020; Gupta et al., 2023; Fasoulis and Kurt, 2019).

2.1 Recent Trends of Cyber Attacks against Maritime Industries

Modern maritime industries are heavily reliant on the information and communication technologies and the use of data. On the one hand, this represents a shift towards safer,more efficient and profitable operations. For example, more and more maritime supply chain partners have increased the use of e-bills of lading, and port authorities have capitalized on computerized systems for the container operations across sharing economies. However, this greater reliance on technologies also brings increased risks in physical and cyber maritime domains. (Brasington and Hadwin, 2016) As clearly stated in (Bull, 2016), "There is also a very real danger that emails being sent to and from ships are monitored or altered. This could have a huge commercial effect on vessels."

More specifically, vessels for both passengers and cargo transportation are equipped with navigation and communication technologies, such as Electronic Charter Display & Information System (ECDIS), Global Positioning System (GPS), Automatic Identification System (AIS), Industrial Control System (ICS), and so on. Currently, all of these systems can be infiltrated by cyber attackers. In fact, cyber-attacks are happening more frequently in the maritime sector according to various maritime reports s (Bull, 2016; MTI, 2017; Vamosi, 2016; Paganini, 2015) and the authors' interviews with practitioners.

The maritime industry evidently is vulnerable to a range of cyber risks. Damages from untrustworthy software or a loss of data integrity through breaches into maritime instruments may result in corrupt, skewed, or incorrect results. Attackers in the Port of Antwerp case had access to control systems, intercepted maritime communication, and altered sensitive shipping information, e.g. characteristics of

goods, container specifics, approved carriers, and so forth. Past maritime cybersecurity incidents have caused the following damages:
• Automated systems malfunctioned or failed entirely;
• Expensive and valuable cargoes were stolen;
• Maritime stakeholders incurred financial, reputational, and/or physical risks;
• Crew on vessels and operators in transit and at critical maritime nodes (e.g., ports, terminals, etc.) were exposed to safety threats to; and
• Cyber operations of other systems connected to the maritime entities were exposed to malicious cyber attacks.
An attack of maritime cyber operations can come about in a variety of ways – access to data can be gained by social engineering attacks, as well as by more sophisticated hacking techniques. An adversarial incident of this nature could affect all of the organizations connected to a port's infrastructure, including those who are not in a position to influence the port's cyber-security or have a role in responding to the incident. (Brasington and Hadwin, 2016)

IBM (International Business Machines) reports that cybersecurity is not only about trying to identify and to prevent systems on board ships from getting hacked. The maritime industry, like many government agencies, as well as the aerospace and defense industry, banking, and health insurance industries, and even the entertainment industry, recently has become a prime target and has suffered substantial losses. The vulnerabilities of maritime cyber operations started to be under the scrutiny by public. This situation indicated that the industry is not immune from cyber threats and must deploy cybersecurity techniques to protect itself. Luck, inaction, and practitioners' tight-lipped community prevent malicious attacks. (Belmont, 2015) In this context, at the most basic level, trustworthy access control techniques need to be implemented to oversee the users and the overall network cyber operations. (MTI, 2016)

2.2 Trust Management Policies for Security Verification

Trust management is a scalable form of access control that relies heavily on delegation. According to Chen, et al. (I. R. Chen and Bao, 2015), trust-related attacks include: (1) self-promoting attacks, which promote own credibility through illegal means; (2) badmouthing attacks: which reduce the trust value of good nodes; (3) ballot-stuffing attacks, which boost the reputation of malicious nodes; (4) opportunistic service attacks, which raise their own reputation through providing quality service in a random manner; and (5) on-off attacks, which provide poor services intermittently. Saied, et al. (Y. B. Saied and Laurent, 2013) presented a method to evaluate the trust value of nodes. The method considers all received reports and past interactions and takes into account parameters of the network's context (service) and resource capabilities. Trust computation models and trust management systems have been implemented successfully in commercial applications. (Y. Zheng and Vasilakos, 2014)

Niu, et al (Niu et al., 2014) applied the trust management concept and developed techniques that support tools to solve problematic security verification instances. When an access control policy fails to satisfy the desired security objectives, it becomes untrustworthy. The tools in that research provide information about how and why the failure occurs. Such information can assist policymakers in designing appropriate policies. The approach to perform the analysis is based on model checking. To ensure the effectiveness of the approach, a collection of reduction techniques was introduced. The paper proved the correctness of these reductions and empirically evaluated their effectiveness. The class of analysis problem instances is generally intractable, which indicates that the reduction techniques are often able to reduce some problem instances into a form that can be automatically verified.

2.3 Summary

The information security literature reviewed above discussed access control systems in general. In order to manage the access control for the modern maritime cyber operations, the method has to reflect the characters and special needs in maritime cyber infrastructure. In Section 3, we present a new access control framework that is adaptable and scalable for the complex maritime cyber space.

3 ACCESS CONTROL FRAMEWORK FOR PROTECTING MARITIME CYBER INFRASTRUCTURE

The setting of the present research includes a central access control system and a sub access control system for a well-defined maritime system, for example, a ship. In a ship, the captain can access any maritime data, e.g., cargo information, ECDIS, GPS coordinates, AIS, etc. The captain also has the au-

thority to communicate with external entities and send any action orders, e.g. turning the ship, stopping the ship, resetting cruise routes, etc. In contrast, a sailor only has a limited access to maritime data and does not have the authority to send any order and communicate with external entities. Other people in the maritime supply chain are not allowed to access or modify any information mentioned above. Without access control, an inside or outside attacker can break in the supply chain system through vulnerable points, as easy as an email, or a USB key. The attacker can access, compromise, steal, or damage sensitive information and control all connected systems. The access control system framework developed below intends to address these threats to protect maritime company's cyber infrastructure.

3.1 Access Control Framework

We incorporate the concept of trust management policy into our access control framework of the maritime cyber spaces. (Hughes and Bultan, 2008) Under the trust-based framework, the method will evaluate the trustworthiness of every node in the maritime communication system. The method will rank all nodes with respect to their reliability levels and select the reliable nodes for the maritime users.

Fig. 1 shows the proposed access control framework. As explained in details below, this framework is adaptable and highly scalable for the maritime industry in light of: 1) the mechanism of traditional access control frameworks and their shortcomings; and 2) the combination with the existing networking access control framework and identification systems. The goal of this framework is to achieve automatic permissions assignment, security protection, and fine-grained, low-energy consumption of the access control in the maritime IT environment. To enable more granular and scalable access control, we use different authentication methods with respect to various trust levels. In doing so, we can capitalize on the flexibilities of the custom trust evaluation mechanisms to authenticate the nodes in the maritime ecosystem.

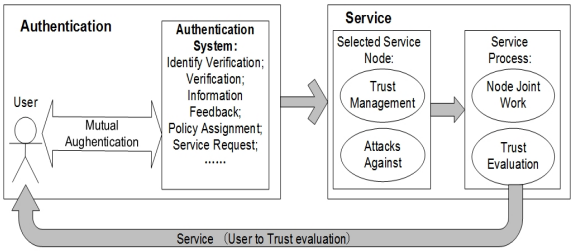

Figure 1: Trust Management and Attribute-based Access Control Framework.

In Fig. 1, the access control framework consists of two modules: Authentication and Service. The Authentication module is mainly responsible for the two-way authentication between the user and the Authentication System. The features of the user authentication system include identity verification, verification information feedback, policy assignment, service request, and so on. In the authentication process, the authentication module firstly verifies the identity information provided by the user. Once the preliminary verification is passed, the feedback information of the user authentication will be sent to the user.

The feedback information includes two sub-modules. The first is the certificate of the authentication system, based on which users verify the legitimacy of the authentication system. The second is a request list of user's information based on which, the authentication system can do a deeper level authentication. After the user has verified the feedback message, the information requested in the feedback information will be sent to the authentication system. The authentication system completes the distribution of user privilege according to the information and sends the user's request to the service module. If any intermediate certification process fails, the verification is terminated, and the validation failure information will be returned.

The service module also includes two sub-modules: The selected service sub-module and the service processing sub-module. The selected service sub-module includes trust management component and attacks-against component. The service processing sub-module includes node joint work and trust evaluation components which do trust evaluation for each node according to the trust computing method and corresponding trust management mechanism. Then it selects the node with the highest reliability for the user. The attack-against component is responsible for maintaining the security of the service module and resists to all kinds of trust-related attacks.

In brief, the framework integrates trust computing into the access control system. The framework includes the network-wide access control, identification technologies, and trusted computing technologies. The trust computing technologies enable the access control framework with the dynamic adaptive capacity and high scalability. The features of this framework result in: 1) significant enhancement in the maritime access control; and 2) Optimized efficiencies and benefits to maritime cyber security.

3.2 Formal Verification for Access Control Framework

The following process provides logical actions to verify the proposed Access Control framework before implementing it in live conditions:
• Define the Access Control Framework formal descriptions;
• Develop a set of reference metrics to analytically evaluate the capabilities of the Framework, and then conduct a comprehensive analysis on the Framework based on the metrics;
• Design a set of oracles to empirically test the runtime functions of the Framework (i.e., whether they can detect the faults embedded in the oracles); and,
• Plan a set of test case scenarios to empirically test the runtime performance of the Framework. These test cases are used not only for evaluating the performance but also for exploring the factors that impact the performance.

3.3 Implementation

There are user authentication and service processing modules in the framework. Service processing module includes service node selection sub-module and service provider sub-module. The authors formalized these modules as follows:
• User AU (Authentication Unit)
• SHU (Service Handle Unit)
• SNSU (Service Node Selection Unit)
• SPU (Service Provider Unit)
Formal verification can be described as follows:
a) The user submits a request. The request accesses by the AU for authentication: User AU: (UserID, Key*, TemporaryCertificate*, Privilege);*
AU: Feedback authentication information, and give the appropriate permissions User*: represents encrypted.
b) AU submits service request to SHU, AU SHU: (AU-ID, TemporaryCertificate*, ServiceRequest)*
c) SHU sends service node selection request to SNSU, SHU-SNSU: (TemporaryCertificate, Request)*
d) SNSU broadcasts the request to all nodes within the maritime infrastructure, gets feedback from nodes, and then selects the service node: SNSU: (SNSU-ID*, TemporaryCertificate*, Request), Node SNSU: (NodeID*, TemporaryCertificate*, TrustValue)*
e) SNSU sends selected node information to SPU:SNSU SPU: (UserID, NodeID*, ServiceRequest) f) SPU uses the target node and user information to provide appropriate services to users and to evaluate the trust value of the node. Then SPU passes the result to SNSU. SPU User, SPU SNSU: (NodeID*, TrustValue)*

The formal verification of the service management (trust management) module is described as follows:
• Th SHU formal Framework includes: (i) initiating a start status, (ii) receiving a service request from AU, and (iii) sending the selected node service request to SNSU;
• The SNSU formal Framework includes: (i) initiating a start status, (ii) receiving a service node selection request from SHU, (iii) broadcasting the request to all nodes within the scope, obtaining feedback from node, and selecting the service node, (iv) sending the selected node information to SPU, and (v) receiving node trust value from SPU after the completion of service;
• The SPU formal Framework includes: (i) initiating a start status, (ii) receiving information of the selected node from SNSU, (iii) using the received node information and user information to provide appropriate services to users, and then assessing the node trust value, and (iv) sending node trust values involved in the process to SNSU.

4 CONCLUDING REMARKS AND FUTURE RESEARCH

The maritime cyber space has become a critical domain to operate global economic, financial, social, and military systems. However, a series of recent reports regarding data breaches in the international maritime industries expose the vulnerabilities in the maritime information and communication systems. To protect maritime cyber infrastructure, the present research developed a novel trust management framework to enhance the access control of maritime cyber operations

Finally, the authors present a number of research directions to account for the limitations of the present research. First, our analysis focused on the cybersecurity of a maritime environment with well-defined boundaries, namely, a boat. Further studies may consider a more complex setting, such as a supplier-customer pair with multiple information systems. Secondly, the access control framework studied here does not detect attacks going through remote nodes beyond the well-defined maritime environment. As such, more research may design and develop intrusion detection systems that span across a more distributed ecosystem, such as a supply chain. Lastly, maritime supply chains may adopt a whole variety of information systems. Distinct computing capacities

of different systems may result in performance variations of the access control method. Therefore, researchers may need to establish systematic metrics to evaluate the effectiveness of access control systems in different maritime information systems.

ACKNOWLEDGEMENTS

This work was supported by the US Department of Transportation (USDOT) Tier-1 University Transportation Center (UTC) Transportation Cybersecurity Center for Advanced Research and Education (CYBER-CARE).

REFERENCES

A. Bowden, K. Hurlburt, E. A. C. M. and Lee, A. (2010). The economic costs of maritime piracy. Oceans Beyond Piracy, One Earth Future Foundation.

BBC (2003). Questions cloud cyber crime cases.

Belmont, K. B. (2015). Maritime cyber attacks: Changing tides.

Brasington, H. and Hadwin, S. (2016). Cyber risks and the maritime industries: risk identification, mitigation and response.

Bull, K. (2016). Maritime companies warned of cyber attacks.

C. Wang, J. Shen, P. V. and Gupta, B. B. (2023). Attribute-based secure data aggregation for isolated iot-enabled maritime transportation systems. volume 24.

Fasoulis, I. and Kurt, R. E. (2019). Determinants to the implementation of corporate social responsibility in the maritime industry: a quantitative study. volume 3, pages 10–20.

Gupta, B. B., Gaurav, A., Hsu, C., and Jiao, B. (2023). Identity-based authentication mechanism for secure information sharing in the maritime transport system. volume 24, pages 2422–2430.

Hayes, C. R. (2016). Maritime cybersecurity: The future of national security. Naval Postgraduate School.

Hughes, G. and Bultan, T. (2008). Automated verification of xacml 3.0 policies using a sat solver. volume 10, pages 503–520.

I. R. Chen, J. G. and Bao, F. (2015). Trust management for soa-based iot and its application to service composition. volume 9, pages 482–495.

Jeong, M. and Li, A. Q. (2022). Motion attribute-based clustering and collision avoidance of multiple in-water obstacles by autonomous surface vehicle. In *IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pages 1–6.

Keefe, M. (2012). Timeline: Critical infrastructure attacks increase steadily in past decade.

Li, A., Li, Q., Hu, V. C., and et al (2015). Evaluating the capability and performance of access control policy verification tools. In *Military Communications Conference, Milcom 2015*, pages 366–371.

MTI (2016). Taking maritime cyber security seriously.

Niu, J., Reith, M., and Winsborough, W. H. (2014). Formal verification of security properties in trust management policy. volume 22, pages 69–153.

Panos, A., Kapnissis, G., and Leligou, H. C. (2020). Blockchain and dlts in the maritime industry: Potential and barriers. volume 4, pages 1–6.

Singh, D., Sinha, S., and Thada, V. (2022). A novel attribute based access control model with application in iaas cloud. volume 7, pages 80–88.

Vanek, O., Jakob, M., Hrstka, O., and Pechoucek, M. (2013). Agent-based model of maritime traffic in piracy-affected waters. volume 36.

Wagstaff, J. (2014). All at sea: global shipping fleet exposed to hacking threat.

Y. B. Saied, A. Olivereau, D. Z. and Laurent, M. (2013). Trust management system design for the internet of things: a context-aware and multi-service approach. volume 39, pages 351–365.

Y. Zheng, P. Z. and Vasilakos, A. V. (2014). A survey on trust management for internet of things. volume 42, pages 120–134.