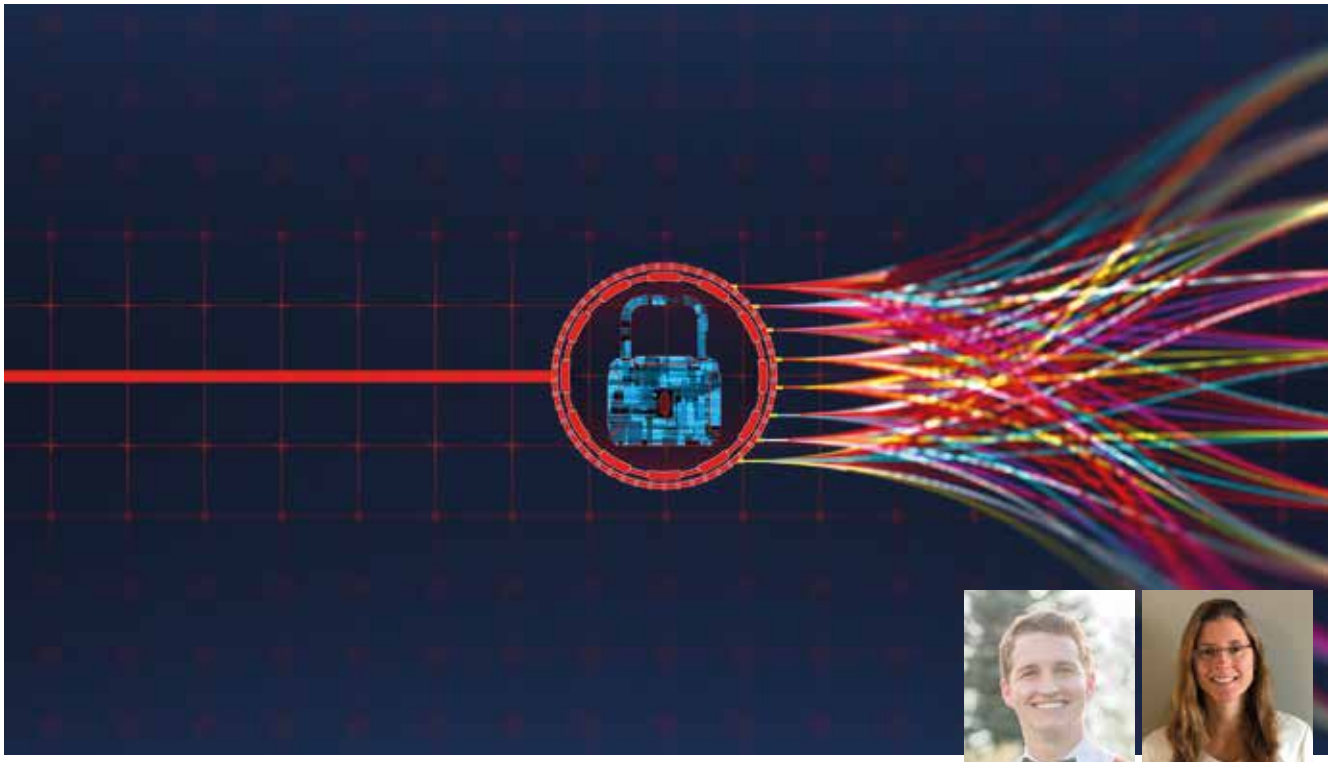

SECURING MARITIME SOFTWARE SYSTEMS

ACADEMIA & INDUSTRY WORKING TOGETHER

Joseph O. Eichenhofer, Elisa Heymann, Barton P. Miller,
Computer Sciences Department, University of Wisconsin-Madison, USA; and
Kyung Won (Arnold) Kang, COO, Total Soft Bank Ltd., Busan, South Korea

The maritime sector is crucial to the world economy, and the computer technology that manages it is critical to its successful operation. Maritime transportation increasingly relies on information and communications technology (ICT) to manage and optimize its operations and services. This technology is involved in many areas, from traffic control communications to container freight tracking to the actual movement of containers. As a consequence, there is an increased dependency on electronic communication and processes with little human interaction. In addition, the maritime logistic ICT systems introduce the risks of being extremely vulnerable to cyber-attack. It is important to note that these ICT systems are based largely on software that has been written specifically to support the operations of maritime logistic systems.

ICT SYSTEMS

Maritime logistic ICT systems are large and complex, having many components used by different players involved in the supply chain. Some of these components are used by general customers, for example the port community system (PCS), to book and track shipments, and exchange documents and information between the public and stakeholders. Other components are intended to be used by port operators, for example the terminal operating system (TOS), to control container movement and storage in the port. Attackers can take advantage of the complexity of this diverse collection of software.

CYBER THREATS

We are faced with sophisticated and determined adversaries that include organized crime and malicious nation-states. For example, in 2013 drug traffickers recruited hackers to breach ICT systems that controlled the movement and location of containers in the Belgian Port of Antwerp [1], managing to reroute (for two years) containers carrying drugs, guns, and cash. Just last year, A.P. Moller-Maersk was almost completely shut down by the NotPetya virus [2].

The software that manages and controls freight transportation systems must be hardened against cyber-attacks. Disruption or unavailability of these ICT systems could have disastrous consequences in cost and availability of goods. Attacks against vulnerabilities in the software can

lead to a wide range of consequences. These consequences include disruption of service, shipment of cargo to unintended destinations, threat to human lives (by remotely controlling the twistlocks of a container spreader to release it over a person, for example) and operation of seaport machinery by unauthorized users. Therefore, there is a critical need to ensure the robustness of the ICT systems and to secure them against cyber-attacks.

While approaching software security is a daunting task, we have made a significant first step. In a collaboration between academia and Total Soft Bank Ltd., a world leader in container terminal software, we performed the first in-depth analysis of a software system that controls maritime shipping. While there have been significant efforts at assessing risk in such transportation environments, the software itself is at risk, there was the need to do a "deep dive" into the code. In our experience, it takes courage and a leap of faith to expose your commercial software to such detailed evaluation. However, the benefits of such an evaluation can be huge, including both a significant improvement in operational security and an increased confidence in the systems by the stakeholders depending on the software.

IN-DEPTH VULNERABILITY ASSESSMENT

Our in-depth software vulnerability assessment was directed at two security-critical TOS and PCS modules provided by Total Soft Bank Ltd. The analysis of the software included a low-level code review that goes well beyond the use of automated assessment tools. The ultimate goal was to find critical vulnerabilities so that the software providers could remediate them before attackers were able to exploit them.

The modules assessed were:

1. A web system that facilitates port status and management access for external stakeholders. It also includes services for processing and storing information including ship schedules and location, container locations, gate access status, dangerous goods locations, and loading/discharge lists. External stakeholders, including shippers and consignees, can check the status of this information through this module. This module is 315,000 lines of code
2. A web application that communicates yard tractor jobs to the operators in those vehicles. Tractor operators log into the web application from a mobile device. The clients of this module can view the yard tractor jobs and update the status of them as they arrive and are completed. This module is 7,000 lines of code

The overall effort took 7 months collectively. The vulnerabilities found were reported to the head of the development team, followed by several interactions with the development team as to how to fix the vulnerabilities. The patched code was then re-assessed by our team.

FINDINGS

To find vulnerabilities, we used a methodology that we developed and have used successfully to assess many real-world software systems, the First Principles Vulnerability Assessment (FPVA) [3]. It is important to emphasize that in addition to common traditional weaknesses, FPVA helps us to identify vulnerabilities that are not commonly known or anticipated. By following FPVA, we identified those parts of the software that would have the highest security impact if they were to be successfully exploited, the high value assets. This identification allows us to focus our analyst resources on the parts of the system that are most security-critical.

Through this approach, we identified both common vulnerabilities and vulnerabilities specific to the system we analyzed.

We now summarize the results of performing an in-depth vulnerability assessment on some modules of a TOS and PCS from Total Soft Bank Ltd. It is worth noting that our results were reported to the software developers in full, including close collaboration on remedying the discovered vulnerabilities, and re-assessing the patched software. In our code assessment, we found several high-impact vulnerabilities. Some of the vulnerabilities we found and reported include:

1. Improper authorization and authentication design allowed illegal access to the system's database. Therefore, the following issues arose:
   - Any user could change any other user's password.
   - Users could access unauthorized services by tampering with client-supplied request metadata.
2. Improper validation in custom file services allowed any user to modify or delete files throughout the server's filesystem. Note that the combination of this weakness along with the password compromise vulnerability in weakness 6 would allow an attacker to steal the username and password for every user of the system.
3. A web server did not check client authorization on all requests. Therefore, many operations were vulnerable to unauthorized access, once the user submitted a correct username and password.
4. An attacker could arbitrarily add log entries to log files.
5. HTTP traffic was not encrypted. As a consequence, the system was vulnerable to:
   - Session hijacking.
   - Password sniffing.
   - Sensitive information exposure.
6. Password compromise: Instead of using a computationally-expensive, salted, one-way hash function, the system stored passwords using an insecure form of two-way encryption. The function uses the decryption key as a password's initialization vector, storing this key in both the database and configuration files. The server also writes the encryption key to the general server log every time a password is checked or updated. In the case of a stolen or compromised database file (which was made possible by weakness 2), an attacker could trivially decrypt the passwords stored in the database. This would lead to full compromise of all accounts and disclosure of users' (potentially reused) passwords.
7. Use of vulnerable versions of third-party software components exposed the system to existing exploits for those components.

CONCLUSIONS

We formed a key collaboration between an experienced academic cybersecurity team and a well-known commercial software provider that manages maritime shipping. We believe that this is the first time that anyone conducted a deep-dive software vulnerability assessment of critical modules of a TOS or PCS.

Our study provided strong evidence that the shipping domain would benefit from more in-depth software vulnerability assessments, whether it is motivated by regulation, stakeholder trust, or other means.

Total Soft Bank Ltd., who allowed their software to be used for this assessment, has taken a significant step forward in providing the maritime shipping industry with a model for more secure ICT infrastructure. This is only a first step, and we hope to see this work extended to other vendors and other aspects of maritime shipping. The goal is to address this problem in a global way.

We believe that this work could provide the foundation for recommendations and guidelines for the maritime freight shipping sector on securing the code of their ICT systems.

REFERENCES

[1] T. Bateman, 2013, "Police warning after drug traffickers' cyber-attack". [Online]. Available from: http://www.bbc.com/news/world-europe-24539417. [Accessed 15 August 2018].

[2] Greenberg, 2018, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", Wired. Available from: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[3] J. A. Kupsch, B. P. Miller, E. Heymann and E. César, 2010, "First Principles Vulnerability Assessment," in Proceedings of the 2010 ACM Workshop on Cloud Computing Security, Chicago.

ABOUT THE AUTHOR

Joseph Eichenhofer earned his bachelor's degree from University of Wisconsin, where he assisted research efforts related to the software vulnerability assessment project. He is now a Princeton University graduate student.

Elisa Heymann is a Senior Scientist on the NSF Cybersecurity Center of Excellence at the University of Wisconsin, and an Associate Professor at the Autonomous University of Barcelona.

Barton P. Miller is the Vilas Distinguished Achievement Professor and the Amar & Belinder Sohi Professor of Computer Sciences at the University of Wisconsin-Madison. He is Chief Scientist for the DHS Software Assurance Marketplace research facility and is Software Assurance Lead on the NSF Cybersecurity Center of Excellence. He founded the fields of Fuzz random software testing and dynamic binary code instrumentation.

Kyung Won (Arnold) Kang is the Chief Operation Officer of Total Soft Bank Ltd. He has 24 years of experience in the maritime, port, and logistic industry. He has led the development of the Terminal Operation System (TOS) and Port Community System (PCS) of Total Soft Bank Ltd.

ABOUT THE ORGANIZATION

The University of Wisconsin-Madison is ranked fifteenth among U.S. public universities. The Department of Computer Sciences is among the oldest computer science departments in the world, boasts the largest student population on campus with 2,100 undergraduate and graduate students, and is a leader in the areas of software security, data sciences, and computer systems.

Total Soft Bank Ltd. is a world leading Maritime Logistics Solution and Services Provider. Since 1988, TSB has been continuously devoted to the innovation of maritime industry with its extensive technology solutions covering from marine terminal, shipping, port community, to simulators.

ENQUIRIES

Elisa Heymann, Barton P. Miller:
e-mail: {elisa, bart}@cs.wisc.edu

Arnold Kang:
e-mail: arnold@tsb.co.kr
Web: www.tsb.co.kr.