Supply Chain Security and Mutual Trust Research Minitrack (Introduction)

Frederick T. Sheldon
University of Idaho
sheldon@uidaho.edu

Robert K. Abercrombie
Prime Time Computing, LLC
abercrombier@ieee.org

Xiaohui Cui
Wuhan University
cuixhui@gmail.com

In January 2012, President Obama released the National Strategy for Global Supply Chain Security. International trade has been and continues to be a powerful engine of the United States and global economic growth. The many cybersecurity challenges facing the U.S. include one of which many Americans are unaware – the serious threat posed by vulnerabilities in the cyber supply chain. Of the many components – including hardware, firmware, and software – that compose a technological product, most contain elements stemming from a broad global market, making it difficult to ascertain the complete security of an end product. With the market for technological goods and components continuing to rapidly grow every year, and with everything from missiles to smartphones relying on these information products, the need for mutual trust cyber supply chain security has never been more critical.

Enhancing the security of any national interests' technological supply chain must not destroy the well-functioning international market for technology. Instead of the two extremes of "intrusive government mandates" or "do nothing," the U.S. government is promoting development of private-sector systems for securing and accrediting technology companies that would allow customers – from the federal government to small businesses – to make more informed and risk-based decisions.

Organizations of all types (business, academia, government, etc.) are facing risks resulting from their ever- increasing reliance on the information infrastructure. Decision and policy makers managing these risks are challenged by a lack of information intelligence concerning the risks and consequences of cyber events (e.g., Sarbanes-Oxley Act, HIPAA, and Gramm-Leach-Bliley ACT). They need to understand the implications of cyber security risks and solutions related to their information infrastructure and business. Risk management investment decisions, within the context of mutual trust among supply chains should involve: (i) a comprehensive approach to cyber security risk management, (ii) credible appropriate data needed to support intelligent decisions, and (iii) assessment of the impacts resulting from the various investment alternatives. Sound, rational IT/business decisions require a comprehensive understanding of the dynamics of information intelligence and the likely effects of cyber security investment choices.

As our dependence on the cyber infrastructure and their associated supply chains grow ever larger, more complex, and more distributed, the systems that compose them become more prone to failures and/or exploitation. Trusted Supply Chains values currency and relevance over detail and accuracy. Information explosion describes the pervasive abundance of (public/private) information and the effects of such. Gathering, analyzing, and making use of information constitutes a business- / sociopolitical- / military-intelligence gathering activity and ultimately poses significant advantages and liabilities to the survivability of "our" society. The combination of increased vulnerability, increased stakes and increased threats make supply chains and their associated processes one of the most important emerging challenges in the evolution of modern cyberspace "mechanization."

In their contribution *DANE Trusted Email for Supply Chain Management*, Joseph Gersch, Dan Massey, and Scott Rose demonstrate the need for trusted email in supply chain management. Spear phishing, forgery, and other attacks can result in data breaches, industrial and government espionage, installation of malware, and financial theft. DANE email extensions are then posited as a solid foundation for global trusted email. The IETF protocol 'Domain Authentication of Named Entities' (DANE) described in this paper has been extended from its initial goal of providing TLS web site validation to also offer a foundation for globally scalable and interoperable email security.

In the second paper *A Structured Analysis of SQL Injection Runtime Mitigation Techniques*, Stu Steiner, Daniel Conte de Leon, and Jim Alves-Foss address SQL injection attacks (SQLIA) which still remain one of the most commonly occurring and exploited vulnerabilities. A considerable amount of research

URI: http://hdl.handle.net/10125/41504
ISBN: 978-0-9981331-0-2

concerning SQLIA mitigation techniques has been conducted with the primary resulting solution requiring developers to code defensively. Although, defensive coding is a valid solution, the current market demand for websites is being filled by inexperienced developers with little knowledge of secure development practices. This paper presents an in-depth analysis and classification, based on Formal Concept Analysis, of the 10 major SQLIA runtime mitigation techniques. Based on this analysis, one technique was identified that shows the greatest potential for transition to enterprise use. This analysis also serves as an enhanced SQLIA mitigation classification system.

In the third paper *Reverse Engineering Integrated Circuits Using Finite State Machine Analysis*," Jessica Smith, Kiri Oler, Carl Miller, and David Manz expand their prior work, in which they proposed a novel method of reverse engineering the finite state machines (FSMs) that integrated circuits are built upon in a non-destructive and highly specific manner. In this paper, the authors present a methodology for reverse engineering integrated circuits, including a mathematical verification of a scalable algorithm used to generate minimal FSM representations of integrated circuits. The method demonstrates that given an isolated state machine with a reset capability, the machine is modeled using a tree framework which allows for machine to machine comparisons and the comparison of states within the machine to find an optimal representation. Through this method it is possible to take a state machine-based IC and, using only the standard input and output pins, re-discover the original FSM. Consequently, they can determine if the in-silicon FSM matches the designed FSM, or rediscover the functionality of an unknown IC. Both capabilities provide a non-destructive means of validation for security purposes.

In the final paper *Towards a Cyber Defense Framework for SCADA Systems Based on Power Consumption Monitoring*, Jarilyn Hernández Jiménez, Qian Chen, Jeffrey Nichols, Chelsea Calhoun, and Summer Sykes present a Supervisory control and data acquisition (SCADA) testbed they developed with the objective to detect cyber-attacks by monitoring and analyzing the power consumption of a Programmable Logic Controller (PLC). The power consumption of the PLC was monitored under three attack scenarios: command injection, Denial of Service (DoS), and replay. Results shown that these cyberattacks leave a detectable signal on the power consumption of a PLC and in route to these results, the authors found and describe vulnerabilities in the DF-1 protocol (an asynchronous byte-oriented protocol used to communicate between the HMI and the PLC via the RS232 link).

The goal of this inaugural minitrack is to challenge, establish and debate a far-reaching agenda that broadly and comprehensively outlines a strategy for mutual trust, cyber security, efficiency, and resilience of our vital global supply chain infrastructure research that is founded on sound principles and technologies.