Cyber Supply Chain

Kathryn Stephens, NSCI
November 18, 2010

National Security Cyberspace Institute, Inc. (NSCI)

Through the combination of research and education, NSCI supports public and private clients aiming to increase cyberspace awareness, interest, knowledge, and/or capabilities. NSCI is committed to helping increase security in cyberspace whenever and wherever possible. NSCI publishes a bi-weekly newsletter (*CyberPro*), has published numerous whitepapers on various cyberspace topics, maintains an online cyber reference library, and has established an email distribution list for sharing cyber-related resumes to interested parties. NSCI is a small, veteran-owned business headquartered in Virginia.

Issues

According to the U.S. Department of Commerce report *Defense Industrial Base Assessment: Counterfeit Electronics* from January 2010, incidents of counterfeit parts rose from 3,868 in 2005 to 9,356 in 2008. The report concluded with the following general findings: all elements of the supply chain have at some point been impacted by counterfeit electronics; there is a lack of communication between organizations that are involved in the U.S. supply chain; organizations in the supply chain assume that others are testing parts; there is a lack of traceability in the supply chain; record keeping on counterfeit parts is limited; most organizations do not have a contact in case of the discovery of counterfeit parts; and most Defense Department organizations do not have any policies in place to prevent counterfeit parts from entering their supply chain.[1]

In the August 2010 edition of *SIGNAL* Magazine, Kent R. Schneider writes that in cybersecurity, "...trust in the network is critical." Schneider says that there must be trust across enterprise boundaries, and that this trust can be achieved by addressing attribution and supply chain vulnerabilities that come from buying software and hardware without knowing the source of the products or what may be included in them.[2] Supply chain risks could allow adversaries to gain access and attack classified national security systems.

CACI International, Inc. and the U.S. Naval Institute recently released a report titled *Cyber Threats to National Security: Countering Challenges to the Global Supply Chain*, which discusses the growing threat to the cyber supply chain -- now global in scale and more difficult to secure. The report states that U.S. supply chains have historically been immune to threats because critical supply chains were always internal to North America. Globalization has spread technologies and capabilities to nations around the world, and our increasing reliance on the cyber domain has made us increasingly vulnerable to cyber threats.[3]

Senators Tom Carper (D-Del.) and Sherrod Brown (D-Ohio) recently wrote to Ashton Carter, undersecretary of Defense for acquisition, technology and logistics, and said that the Department of Defense does not currently have effective policies or processes for detecting, tracking and preventing the use of counterfeit parts. A report from the Government Accountability Office, said that the Defense Department does not even have a department definition of counterfeit, or a way to identify suspected counterfeit parts even though the Defense Department receives products from a global network of suppliers. Defense officials say that they will have a definition and guidance by December. The Senators warn that counterfeit parts could disrupt DoD supply chains, delay missions, and contaminate weapons systems.[4]

---

[1] U.S. Department of Commerce. (2010, January). *Defense Industrial Base Assessment: Counterfeit Electronics.* Retrieved August 16, 2010, from http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf

[2] Schneider, K. R. (2010, August). *The Primacy of Focus on Cybersecurity.* Retrieved August 16, 2010, from SIGNAL Magazine Online: http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2355&zoneid=300

[3] CACI. (2010). *Symposium One: Countering Challenges to the Global Supply Chain.* Retrieved August 11, 2010, from Cyber Threats to National Security: http://asymmetricthreat.net/docs/asymmetric_threat_4_exec_sum.pdf

[4] Weigelt, M. (2010, August 9). *Senators concerned about counterfeit parts.* Retrieved August 19, 2010, from Federal Computer Week: http://fcw.com/articles/2010/08/09/defense-supply-chain-counterfeit-parts.aspx

Security professionals agree that security can no longer be kept behind a firewall, and that developers, vendors, customers and users as well as others along the supply chain of IT systems, hardware and software all have an effect on system security. Jim Lewis, director and senior fellow of the Center for Strategic and International Studies' technology and public policy program says "it's not just how secure you are, but how secure the people you connect with are as well." Foreign suppliers could use the supply chain to attack the United States in several ways. Malware could be inserted into software and hardware that is then used in U.S. systems, and hackers could probe software. Hart Rossman, CTO of cybersecurity solutions with SAIC says that "few supply chain managers or supply chain risk managers have aligned their mission with their computer security center, and they're not commissioned to conduct joint operations." Counterfeiting is another risk, and the Department of Justice says that China produces counterfeit microprocessors that they sell to U.S. government agencies as "military grade" components.[5]

The threat is not only to U.S. government agencies, but also to industry and private organizations. Donald Donahue, CEO of Depository Trust and Clearing Corp., says that his organization faces "organized cyber enemies who are hell-bent on positioning themselves to bring down the entire U.S. financial services system" and that "their intent to penetrate the supply chain exploiting whatever vulnerabilities that may exist is very clear."

Ideas

The CACI Supply Chain report says that in order to combat cyber supply chain threats, Congress must define what roles and responsibilities exist in the cyber supply chain, and diplomatic solutions must be explored in order to minimize the threat.[6]

The Defense Department has already begun taking steps to better secure the cyber-related supply chain. The 2011 Senate Defense Authorization Bill includes a section that would "authorize Defense agency heads to exclude from procurements specific companies to avoid unacceptable supply-chain risk." Some industry organizations say that an agency head should not have the authority to exclude a company without a review in a bid protest before the Government Accountability Office or any federal court. Amit Yoran, chairman and chief executive officer of security software company NetWitness and former director of the Homeland Security Department's National Cybersecurity Division says defense agencies need authority to refuse a technology component that could be dangerous to classified systems, but that there should be a system in place for providing industry with information to mitigate supply chain risks. Yoran says agencies must have "transparent processes for evaluating software products and solutions that allow the agency to perform due diligence, while still providing the [manufacturer] due process in response to any identified vulnerability in its products."[7]

Troy Hodgkins, TechAmerica's vice president for national security and procurement policy, says security standards should be developed in conjunction with industry in order to be the most effective. Hodgkins says the government should provide more information about supply chain threats and vulnerabilities in order to help industry address those threats. The Defense Department says the provision will help to increase supply chain security by maximizing competition among commercial suppliers and also strengthening the security of the department's systems.[8]

---

[5] Hoover, J. N. (2009, November 7). *Securing The Cyber Supply Chain.* Retrieved August 15, 2010, from Information Week: http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=221600499

[6] CACI. (2010). *Symposium One: Countering Challenges to the Global Supply Chain.* Retrieved August 11, 2010, from Cyber Threats to National Security: http://asymmetricthreat.net/docs/asymmetric_threat_4_exec_sum.pdf

[7] Aitoro, J. R. (2010, August 2). *Defense agencies should provide ways for industry to fix security issues.* Retrieved August 16, 2010, from NextGov: http://www.nextgov.com/nextgov/ng_20100802_9255.php

[8] Aitoro, J. R. (2010, August 2). *Defense agencies should provide ways for industry to fix security issues.* Retrieved August 16, 2010, from NextGov: http://www.nextgov.com/nextgov/ng_20100802_9255.php

Cyber Supply Chain

Kathryn Stephens, NSCI
November 18, 2010

The report from the Commerce Department and the Office of Technology Evaluation (OTE) provides several recommendations for improving supply chain security. OTE developed a set of key business practices for organizations including:

- The provision of guidance to personnel on part procurement, testing and inventory management
- Implementation of procedures for identifying and reporting suspected components
- Purchasing parts directly from OCMs and authorized suppliers when possible
- Establishing a list of trusted suppliers to help enable informed procurement and the creation of an untrusted supplier list
- Utilization of third-party escrow services to hold payment for part testing
- Adoption of realistic schedules for procuring electronic components
- Modifications to contract requirements with suppliers
- Ensuring the physical destruction of all defective, damaged and substandard parts
- Expansion of authentication technologies
- Screening and testing of parts to assure authenticity
- Strengthening part testing protocols
- Verification of test integrity
- Site audits of supplier parts inventory and quality processes
- Maintaining an internal database of suspected and confirmed counterfeit parts
- Reporting all suspect and confirmed counterfeit components to federal authorities and industry associations[9]

OTE also proposes the following recommendations based on their study:

- The establishment of a centralized federal reporting mechanism for collecting information on counterfeit parts
- Modifying Federal Acquisition Regulations (FAR), including Defense Federal Acquisition Regulations (DFAR) to allow for best value procurement and requiring U.S. government suppliers and federal agencies to systematically report counterfeit parts to the national federal reporting mechanism
- Issuing clear legal guidance to industry and U.S. federal agencies
- Establishing federal guidance for the destruction and disposal of electronic systems and parts
- Establishing a dialogue with law enforcement to increase prosecution of counterfeiters and those who knowingly distribute counterfeit parts
- Establishing a government repository of electronic parts information
- Developing international agreements covering information sharing, supply chain integrity, border inspection of electronic parts, related law enforcement cooperation and standards for inspecting counterfeits
- Addressing funding and parts acquisition planning issues within the Defense Department[10]

Threats to the U.S. supply chain were also addressed in the Comprehensive National Cybersecurity Initiative, established by the Bush Administration in 2008. Michael Jacobs, former information assurance director at the National Security Agency, says that the recently declassified CNCI contains information about a "multipronged

[9]U.S. Department of Commerce. (2010, January). *Defense Industrial Base Assessment: Counterfeit Electronics.* Retrieved August 16, 2010, from http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf

[10]U.S. Department of Commerce. (2010, January). *Defense Industrial Base Assessment: Counterfeit Electronics.* Retrieved August 16, 2010, from http://www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf

approach for global supply chain risk management" which will include greater awareness of threats and vulnerabilities that come from acquisition. The CNCI also discusses the development of tools that will help to mitigate supply chain risks by retiring products, creating new acquisition policies and partnership with industry to develop supply chain and risk management best practices. Jacobs says it is important to understand where our products come from, including products that, although sold by U.S. companies, may include code written in another country.[11]

Answers

There are several things that can be done to improve the security of the cyber-related supply chain. First, supply chain security must become a part of the U.S. overall cyber intelligence and cybersecurity strategy. The U.S. government should also consider building a limited number of systems that are absolutely certain to be secure, in order to minimize the threat to the most critical systems and information. The public should also be educated on cyber-related threats to minimize vulnerabilities caused by uneducated users. Following the recommendations of the DoC and OTE report, the federal government should create a database of information on counterfeit products and their suppliers, as well as an organization that could handle reports of suspected counterfeit products. Legal requirements and guidelines for dealing with counterfeit suppliers should be clarified, and there should be federal guidelines for destructing counterfeit products. Finally, international agreements that include guidance for procurement and acquisition should be addressed or updated to include policies for counterfeit products.

The Comprehensive National Cybersecurity Initiative includes working on supply chain vulnerabilities and policies with participation from the National Institute of Standards and Technology. NIST's guidelines will include procurement strategies, which require suppliers to carry out specific risk mitigation processes. The NIST guidelines will include security throughout the entire technology life cycle, from design to retirement. The General Services Administration has also announced that it will use market incentives to improve security in hardware and software product designs.[12]

IT risks and vulnerabilities from the cyber-related supply chain are real and growing. By addressing threats from the entire life cycle of technology products, we can improve security of U.S. systems. Cyber supply chain vulnerabilities will improve through a combination of education, international agreements, unified guidelines on procurement and acquisitions, well-defined legal guidelines, and the development of a database for suspected and confirmed counterfeit products and suppliers.

[11] Aitoro, J. R. (2010, March 3). *Monitoring federal networks, global supply chain part of cyber initiative.* Retrieved August 16, 2010, from NextGov: http://www.nextgov.com/nextgov/ng_20100303_9560.php

[12] Hoover, J. N. (2009, November 7). *Securing The Cyber Supply Chain.* Retrieved August 15, 2010, from Information Week: http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=221600499