Technovation 34 (2014) 362–379

Contents lists available at ScienceDirect

Technovation

journal homepage: www.elsevier.com/locate/technovation

Criticality analysis and the supply chain: *Leveraging representational assurance*

Dan Reddy

Engineering and Technology, Quinsigamond Community College, United States

ARTICLE INFO

Available online 9 May 2014

Keywords:
SCRM
Supply Chain
Criticality Analysis
O-TTPS
Treemap
Representational assurance
Counterfeit
Taint

ABSTRACT

System builders who plan to acquire information and communication technology (ICT) products must consider two key risk factors (among many) while planning for the acquisition and design of their systems. They must understand the inter-relationships of all assembled products in any new planned system in terms of its resilience under attack. These system owners will also increasingly assess the risks they may inherit from a global interconnected supply chain. To address these concerns, the recommendation in this paper is for providers of Commercial-Off-the-Shelf (COTS) technology products to perform a criticality analysis on their own products to gauge resilience, rather than later be confronted by an acquirer attempting to solely reverse engineer the system as part of supply chain due-diligence. This paper illustrates the roles that technology providers and system owners each play in following the outlined approach that highlights key risk factors of the tiered suppliers for product elements deemed most critical. ICT COTS providers who do not want to divulge sensitive information about their suppliers can use a "representational assurance" approach to convey meaningful information to potential acquirers without undue disclosure. Analytical graphics such as "Treemaps" can help all parties illustrate where to best focus their attention regarding critical operational risk and supply chain risk. The same data that providers track internally to manage product assurance can be leveraged to support meaningful representational assurance to acquirers. This approach improves the current state where data disclosure by technology providers is seen by acquirers, despite being unrealistic, as the best means to gain confidence in the technology supply chain.

1. Introduction – today's reality

1.1. The landscape of ICT COTS products and their supply chain

Customers in the critical infrastructure, public sector and defense industries are increasingly faced with cost and performance advantages due to dynamic improvements of using Commercial-off-the-Shelf (COTS) Information and Communication Technology (ICT) products. These acquirers are grappling with the challenge of finding the right set of trustworthy products to fit together as part of the ICT planned overall system or solution. Some acquirers expect that COTS ICT products should have to meet the same high assurance expectations of custom ICT products. On the other hand, ICT product vendors (hereafter, ICT providers) typically design their products to meet the high performance needs of a broad and diverse global customer base. In a complex price market, when acquirers plan to leverage COTS ICT in their solution they realize that they could be inheriting some supply chain risk since they do not have direct and deep visibility into the supply chain that led to the creation of the ICT COTS product. Supply chain security has become a burgeoning area of concern in the United States (U.S.) since The Comprehensive National Cybersecurity Initiative (CNCI) #11 evolved under two Presidents to "Develop a multi-pronged approach for global supply chain risk management" (SCRM). This focus heightened awareness of the issue and helped to shape US cyber security policy. CNCI # 11 brought wide attention to the risk that by targeting components or elements of a technology product an attacker could harm the downstream operation of that product as it is deployed in the ultimate customer's environment (U.S. National Security Council, 2008). A U.S. Government Accountability Office report found that thousands of counterfeit parts made their way into systems, adding more data to heighten concern about potential risks in the supply chain (GAO-12-375, 2012). The Software Assurance Forum for Excellence in Code (SAFECode), in its whitepaper, stated that while supply chain attacks may not be as likely as having an attacker exploit a product vulnerability that derives from a coding "bug", supply chain attacks must be addressed (SAFECode, 2009). To address supply chain risk, acquirers might begin to ask

E-mail address: dan.reddy@gmail.com
URL: http://www.linkedin.com/in/danreddySCRMsme

http://dx.doi.org/10.1016/j.technovation.2014.01.009
0166-4972 © 2014 Elsevier Ltd. All rights reserved.

providers to itemize and account for every component of their product as part of a proposal or contract. In addition, acquirers may inquire about the product development and the secure engineering practices of the provider and include the practices of all the suppliers that contributed to the final ICT product. Such an approach is simply not scalable when you consider the volume of the ICT COTS products and their components that are potentially involved. A further constraint in this approach is that for sensitive systems such as those for defense applications, perhaps built with a systems integrator, the acquirer may not want to divulge the purpose or other details about the ultimate system or solution. The question then becomes: "Even if this concept of massive one-way disclosure were viable, how would this information be collected, protected, shared and used effectively?" An impasse exists since the providers will not want to share details about their suppliers and the acquirers may not want to share the nature of their proposed solution. Undue exposure aids both attackers and competitors to the ICT provider.

1.2. What providers do today – state of the art

For decades, ICT providers have invested in quality management programs within their enterprises to improve acquirer satisfaction and to reduce the cost of ongoing operations. ICT providers follow international standards such as ISO 9001 and invest in becoming certified for adopting the key quality requirements in such standards. According to a recent analysis of 42 empirical studies on the benefits of ISO 9001 certification, more than one million companies have gone through the process in 178 countries and have enhanced their financial performance through a combination of increased sales and lower costs (De Vries and Manders, 2010). ICT providers who look for suppliers who also have achieved ISO 9001 certification provide an example of how thoughtful organizational practices can impact the overall provider/supplier ecosystem.

Providers have also invested heavily in quality improvement programs. *Lean-six-sigma* is a related approach that has a long tradition of identifying opportunities for process improvement and reduced costs within enterprises across various industries and sizes. Its methods and tools have been leveraged for driving quality within the manufacturing of products by reducing defects as well as for "Just-in-Time" planning within Supply Chain Management (Singh et al., 2013). Singh et al. suggested the application of rigorous measurement and skill building along with the use of techniques like Value Stream Mapping to identify both the "As-is" and the "To-be" process flows before tackling improvements.

In addition to continuously improving quality, ICT providers:

- Manage internal practices to build secure hardware and software products for broad markets.
- Deal with a complexity challenge in tracking many parts across tiers within the supply chain.
- Deliver high quality and secure systems that are resistant to tampering.
- Avoid exposure of system design elements or the identity of their exact suppliers.
- Limit undue exposure to attackers who may try to exploit any attack surfaces.

Today, one of the many secure development activities that effective ICT providers conduct is threat modeling. This modeling analyzes the security of product designs for architectural weaknesses. Results from threat modeling can be leveraged to inform future design, development, and testing activities along with deployment planning and configurations (Dhillon, 2011).

Threat modeling is being singled out as an example not because it is sufficient as an activity to produce secure, resilient products but because it is analytical, because it uses modeling techniques and because it influences other secure engineering activities. Resilience as an objective here describes the capacity of a product to withstand the impact of an attack from any dimension with as little degradation of operational capability as possible.

In addition to analysis and modeling for security and resilience, product architects naturally design ICT products for the marketplace with high availability and performance in mind, though these factors are considered more as 'standard features' for the commercial marketplace than as security attributes. Taken together these factors illustrate the complexity of what ICT providers must manage. To be effective, they often leverage internal management systems to track their activities and to measure results while striving to deliver secure and resilient products. The product organizations that invest in repeatable secure engineering practices, such as threat modeling, will also position themselves well when preparing for third party product evaluations or organization accreditations that should recognize and value such best practices.

When faced with having to show potential public-sector acquirers that one's provider company is compliant with a range of required regulations and certifications, today companies can post some of their compliance data on public websites for any potential acquirers to see so that the provider does not need to reproduce common information for every acquirer. The U.S. government sponsored System for Award Management (SAM) website (www.sam.gov) has a series of "representations and certifications" for a variety of compliance items. Companies can choose which compliance items they elect to publically display to be considered during potential acquisition. The company thereby represents or certifies that it complies with certain particulars such as the legal restrictions in dealing with certain global entities, complying with child labor laws or being properly designated as a small business as the case may be. This demonstrates that there is some precedent for providers and acquirers to share meaningful information without undue disclosure of details. This notion of sharing representational data could be extended in a new way highlighting assurance information about the suppliers of critical components that would be given to a potential acquirer.

1.3. Common criteria leads as the certification for evaluating the security of ICT products

Currently, assurance information flows to shareholders from compliance with international standards. When it comes to acquirers looking for product evaluations that focus on security capabilities of a specific product within defined boundaries, the international standard *The Common Criteria for Information Technology Security Evaluation* simply known as the Common Criteria (CC) is the leading reference. These certifications have a prescribed method of evaluation and are conducted by independent certified third-party labs. As part of the CC, providers, their lab evaluators, and the country based "authorizing schemes" that support the 26 country mutual recognition system are trained to examine security critical functions within products. The world of product-based evaluations under CC is undergoing a slow transformation from the very specific evaluation of the product's "Security Target" to those that are based on standard "Protection Profiles" for classes of technology (for example firewalls). Although to date CC evaluations have been relatively expensive and time consuming, this is a well-understood and valued certification process for specific product versions where higher assurance is needed.

Acquirers who seek specific product evaluations may also have to comply with location dependent requirements. For example, providers must comply with the relevant import and export location requirements to their operation. This may involve the proper marking and declaration of country of origin for their ICT products and to insist that