Telecommunications Supply Chain Integrity

Mitigating the Supply Chain Security Risks in National Public Telecommunications Infrastructures

John Kimmins
Telcordia Technologies
Piscataway, New Jersey USA
jkimmins@telcordia.com

***Abstract*— Across the globe, many national telecommunications infrastructures are at a crossroads. Incumbent suppliers are increasingly relying on off-shore component sourcing, while new suppliers – some from countries with strong geopolitical tensions – have taken significant actions to position themselves to be major suppliers to various nations' telecommunications operators. Collectively, these factors have brought a sharp focus to the need for a more in-depth review of the integrity of national telecommunications infrastructures and the supporting foreign product supply chains. This paper delineates the above factors and their related risk implications for national and global communications infrastructures. In doing so, the paper reflects an enhanced risk management model and process Telcordia has developed that accommodates both government and private sector issues and builds upon current security practices.**

Keywords-Supply Chain, Network Security, Telecommunications

I. GROWING CHALLENGES TO SUPPLY CHAIN INTEGRITY

A new and growing security challenge is the mitigation of commercial and national security risks associated with the public telecommunications infrastructure. That infrastructure is increasingly composed of components and systems that are designed, developed, and manufactured by foreign firms, or home country companies relying on downstream suppliers integrating foreign components into their products. A prominent example is the substantial amount of network equipment and software for next generation networks (NGNs) being produced by non-traditional suppliers based in foreign countries that are not considered close allies. As service providers seek to reduce their operating costs, the testing, support, maintenance, and repair of NGN equipment may also be provided by these foreign-based suppliers.

The use of equipment from suppliers that are not considered closely trusted as traditional suppliers, and who may be influenced by the political environment in which they reside, present uncharted security threats and risks for many national and global telecommunications infrastructures. A concern expressed by many governments is that a large portion of the national communications infrastructure may become dependent upon equipment and suppliers from a single foreign nation, and this could have very profound national security implications. Also threaded throughout this security issue are political, international trade, and corporate economic dimensions.

Recent industry developments and events have created a new urgency to holistically address this issue. Perhaps most prominently, a small set of telecommunications suppliers have mounted an aggressive approach to profile and address the security trust issue as part of their strategy to penetrate the North American telecommunications market. Additionally, and driven by competitive concerns, Tier 1 & 2 carriers have installed foreign made and supported core network equipment, and the trend is increasing across all infrastructure components.

Facing similar market realities and national security issues, several countries have already been developing and implementing various approaches to address these new security risks. In the United Kingdom, a supplier-funded Cyber Security Evaluation Centre has been established to perform detailed security testing and to interface with the supplier's development and maintenance facilities and provide assessment results to appropriate stakeholders. In India, the government is currently revisiting their requirements that have software escrow, setting up test beds, and conducting third party testing and evaluation provisions. Global IT and telecommunications industries are actively providing inputs for refining these approaches and requirements.

II. KEY THREATS AND THEIR IMPACTS

There are many different types of threats that can be realized with the insertion of products into a carrier network. The placement and functionality of the equipment and applications will also have a strong bearing on which threats will be more prominent than others. The following identifies key threats that a telecommunications service provider potentially faces with deployment of supplier equipment with an unproven trust level, regardless of origin.

978-0-615-51608-0/11 ©2011 EWI

- Disruption of service and network availability due to different levels of denial-of-service attacks at the software, firmware, hardware, management, protocol, architectural, and physical levels
- Loss of network control at the service, network, and element management levels
- Loss of confidentiality and integrity of communications with the ability to target source and destinations across multimedia (i.e., voice, data, video) services, including the manipulation of messaging or injection of false messaging causing misleading information that is acted upon, or creating distrust in the channel
- Unauthorized physical and logical access to equipment, systems, management functions, data bases, and subscriber information by supplier personnel
- Disruption of government emergency and prioritization types of telecommunications services that are being transported by this service provider using network equipment from the foreign supplier in question
- Attacks on other service providers who are interconnected with the service provider having the equipment from the foreign supplier in question
- Fraud and theft of service by subscribers and interconnected network partners.

III. Mitigating The Risks

There is always a risk when introducing new equipment and/or new manufacturers into a critical network infrastructure. For this reason all service providers maintain a risk mitigation plan as a part of their deployment efforts. Because the threats and impacts are multidimensional and are both externally and internally focused, the risk mitigation strategies for carriers have to address many different aspects. The supplier risk mitigation plan is multifaceted and should be comprised of the following four interrelated initiatives:

1) *Procedural measures* include supplier site inspections, physical presence and enforcement of security-related contract obligations; product software analysis and testing prior to deployment; and the strategy of purchasing similar types of equipment from at least two independent suppliers to reduce any dependency on a single supplier
2) *Contractual measures* that stipulate terms, conditions, and obligations between the service provider and the equipment supplier
3) *Physical measures* include additional means to restrict supplier access to equipment and systems beyond existing practices for securing its facilities and equipment
4) *Technical measures* such as an enhanced security architecture, ongoing security management, and multistage security testing of the supplier products and its associated lifecycle.

The first three initiatives are addressed by the provider and supplier during the procurement, installation, and operation of the equipment. This white paper focuses on the ***technical measures*** that need to be addressed, not just by the carrier and supplier but by the industry and government, to be truly effective and cover the entire public telecommunications infrastructure. The main goal is to detect vulnerabilities, malicious code, weak security features, undocumented commands, default commands, unprotected interfaces, third party product vulnerabilities, etc. that may be embedded in the supplier's product through rigorous and structured security testing and analysis throughout the product's lifecycle.

IV. An Enhanced Product Security Assessment Approach

In the United States, as with many other nations, the federal government is faced with the responsibility of ensuring the security and reliability of the national communications infrastructure – as it is used for both commercial and government purposes. The U.S. Government has long maintained that the integrity of the U.S. network is at a perceived greater risk when the infrastructure itself, or the critical equipment that is used in the communications infrastructure, is manufactured in a non-U.S. location. For this reason the U.S. Government instituted a range of processes and partnerships to enhance national security and homeland security considerations, such as:

- Committee for Foreign Investment in the U.S. (CFIUS) – a process to assess national security risks and approve or deny foreign acquisitions of U.S. corporations, technology, or infrastructure. The Department of the Treasury is the lead agency.
- National Security Telecommunications Advisory Committee (NSTAC) – established by Executive Order 12382, NSTAC advises the U.S. President on a wide range of policy and technical issues related to communications, information systems, information assurance, infrastructure protection, and other national security/emergency preparedness concerns.

While many nations have instituted similar processes to the above, these approaches typically do not provide an adequate process to assess the risk and potential vulnerabilities to national security and critical infrastructures from increasingly complex and foreign-sourced product supply chains. Due to the nature of global competition, the use of

foreign-manufactured and supported equipment will continue to mushroom, resulting in even greater numbers of potentially un-trusted products being incorporated into the national communications infrastructures.

In light of the above, there is growing global recognition that an enhanced risk mitigation model and supporting technical approaches must be developed in cooperation with the telecoms industry to reduce the risk of disruption to the communications infrastructure through intentional or unintentional exploited vulnerabilities and capabilities. It is clear that such a comprehensive product security assessment program must not only be systematic, but also transparent and independent. And, that it needs to be conducted in a way that directly addresses the needs of the various stakeholders: service providers, government entities, and the suppliers themselves. These needs center on ensuring detailed disclosure without compromising competitive advantage. Such an approach is commonly employed by other commercial markets; e.g., in the entertainment industry content providers require multimedia device suppliers to be independently evaluated by third parties.

There are numerous aspects that need to be incorporated into a new supply chain integrity policy and telecommunications product security risk assessment program to be effective, comprehensive, and timely. Critical aspects include:

- Defining a policy that addresses the competitive global supplier landscape and recognizes market dynamics for timely assessments and the need to demonstrate compliance to the new requirements
- Ensuring a product security assessment approach that is comprehensive and sufficiently detailed to address current and future product features, as well as the entire product lifecycle activities including development, maintenance, testing, and support operations and processes
- Anticipating the constantly changing threat environment and reflecting those dynamics in the evaluation criteria and testing regimes
- Ensuring consistent program oversight in order to manage and minimize longer term national security risks
- Enhance existing internationally recognized security risk management methodologies and test criteria to address the new supply chains risks and facilitate global acceptance.

Over the years, the telecommunications industry has responded to different types of attacks by increased emphasis on security testing and architectures. Security requirements, such as Telcordia's network elements security requirements (GR-815-CORE) and other specifications, were published and widely adopted by carriers and suppliers. Telecommunications suppliers also contract with various industry firms or organizations for software and hardware assessments to validate compliance with various software development and other standards. While all these assessments are important, they provide inadequate assurance regarding security risks and vulnerabilities related to foreign supply chain exposures throughout a product's lifecycle. Under these standards and testing approaches, even the most highly evaluated software and hardware products may possess serious security risks. The assessment criteria and testing is not focused on identifying and calibrating the wider variety of security weaknesses that could be exploited by a malicious adversary.

The required product security assessment approach needs to be specifically focused on identifying and evaluating security threats and vulnerabilities, such as malicious code or subversive network control and monitoring, contained in a supplier's software, firmware, and hardware implementation, across their involved foreign supply chains. In doing so, it is critical that any such approach be both comprehensive and relevant in order to address the market's technical and other related complexities, as well as its rapid pace of development. Existing security evaluation approaches such as the Common Criteria and the NIST risk management methodology (SP-800 series) would be used as input, but would be expanded to address the detailed and comprehensive security testing and analysis required by the market realities described above.

V. Product Assessment Elements

The scope of this proposed security assessment approach would include, but not be limited to, the following technical areas:

A. Vulnerability analyses and controls assessment of product design, architecture & system components; specifically:
   1) Interfaces across management, control & user planes
   2) Product security features
   3) Selected Source code analysis
   4) Product releases, patches & field maintenance processes and handoffs
   5) Product development environment
   6) Supply chain & third party product and component integration

B. Testing software, hardware, & firmware of Element Management Systems and Network Elements

There also needs to be a governance framework to define the process and test criteria for product and supply chain security assessments. To address national needs as well as the competitive product and services' environment, the government and industry stakeholders need to find an appropriate partnership structure. This creates a participative process for receiving inputs from industry, facilitating exchanges of opinions, keeping the test criteria current with

evolving threats and achieving a higher probability of industry buy-in into the assessment program.

Another critical element to provide greater integrity and recognition for the process is the identification of the evaluator characteristics. Self-assessment is a model that has been used with limited success. A more realistic model used in financial auditing and other markets is the role of the independent third party evaluator. Any such third party independent evaluator would need to possess the following attributes:

- A clear absence of any conflict of interest pertaining to any suppliers or telecommunications service providers.
- Deep experience in the conduct of complex independent telecommunications security assessments, and an established record of producing unbiased security evaluations.
- Credibility with government agencies and the different roles and missions.
- A deep knowledge of Government and private sector critical infrastructure issues regarding relevant information technology and telecommunications threats and vulnerabilities.
- Extensive experience in supporting the development, acceptance and application of domestic and international telecommunications security standards and best practices.

VI. Conclusion – Addressing Security Holistically

Critical components of many nations' telecommunications networks are increasingly being procured from off-shore, untrusted sources. While industry assessments exist for telecommunications standards compliance, there is no process for holistically assessing security threats and vulnerabilities. This gap is particularly apparent for the assessment of telecommunications product functionality and architectures and the associated lifecycle phases and support activities. A risk management framework, such as the one discussed here, needs to be urgently created and shared across nations. Each nation needs to balance their view of national security issues with telecommunications market dynamics and international trade. An international approach that has common elements will have greater acceptance by the industry and start addressing this critical risk.