ISSN 2409-2665
Journal of Logistics, Informatics and Service Science
Vol. 2 (2015) No.1, pp. 28-41

A Systematic Study for ICT Supply Chain Security

Tianbo Lu[1,2], Puxin Yao[1], Xiaobo Guo[1], Xiaoyan Zhang[1] , Lingling Zhao[1] and Hongyu Yang[2]

[1]School of Software Engineering, Beijing University of Posts and Telecommunications, Beijing, China.

[2] Information Technology Research Base of Civil Aviation Administration of China , Civil Aviation University of China.

lutb@bupt.edu.cn; yaopuxin@163.com

(*Received Dec 2014, accepted Mar 2015*)

Abstract. Global supply chain security has become a rising concern by most countries all over the world since the 2001 “911” terrorist attacks. Many countries and organizations did their research on supply chain security and many initiatives have been developed and taken into practice. But most of them are focusing on physical supply chain which is addressed in transporting cargos. The study for ICT supply chain security is in preliminary stage, especially lacking of a systematic study. This paper systematically analyzes the security threats to the ICT supply chain, and presents a framework of the security models on ICT supply chain and international regulations or standards ICT supply chain, and meanwhile propose a series of recommendations conducive to developing one’s own strategy for most countries on ICT supply chain security in national level.

Keywords: ICT supply chain • Information Security • Models • Standards

1. Introduction

Supply chain is a key element in global commerce. Any disruptions in supply chain can cause huge loss. However, before Sept.11, 2001, many companies were not aware of the importance of supply security and they only relied on luck to resist disastrous supply chain disruption [1].

Supply chain is a system of organizations, people, processes, technology, information and resources. According to its nature, the risks in the supply chain are divided into emergencies and operational risks. Emergency usually means a material adverse effect on system events caused by natural disasters or man-made factors. [14] The objectives of supply chain risk management fall into two aspects: the one is to enhance profit, the other is to lower the disruptions existing supply chain. [15]

ICT is short for information and communication technology. ICT supply chain refers to the full set of key actors included in the network infrastructure, including end-users, policy makers, procurement specialists, systems integrators, network provider and software/hardware vendors. Through the interaction of organizational layer and process layer, these users/suppliers plan, build, manage, maintain, and protect the network infrastructure [20].

The ICT supply chain, compared with the traditional/physical supply chain, has its own characteristics, such as: The equipment used in the supply chain usually includes hardware, software, and many other components; Functionality and quality of the equipment is difficult to test, measure and display intuitively. In short, ICT supply chain is a critical part of supply chain nowadays. If it is destroyed, the traditional supply chain depending on it will also be destroyed.

This paper first introduces the concept of ICT supply chain. Then in section 2, it systematically analyzes the security threats to the ICT supply chain, and section 3 presents a framework of the security models on ICT supply chain and section 4 shows a framework for international regulations or standards ICT supply chain. At last authors propose a series of recommendations.

2. Threats to ICT Supply Chain

It is necessary to understand that ICT Supply Chain is facing many security threats. In this paper, those threats are classified into three kinds. As we can see from Fig. 1, it is a model that provides three aspects to study ICT Supply Chain Security.

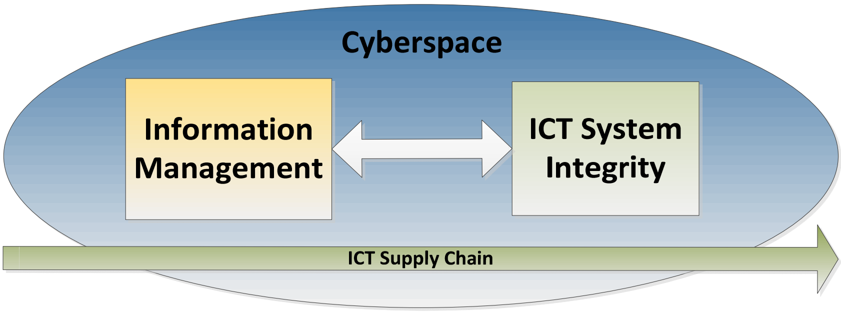

Fig.1: Three aspects to assure ICT supply chain security

2.1 Information Threats in ICT Supply Chain

"In the modern world, the supply chain is information. When something has been ordered ... where it's going to be manufactured and by whom and how much and what specifications ... all are either on the Internet or in private data systems that are subject to being hacked and invaded."[16] The supply chain is actually an extremely complex information management system, and products and services provided by ICT supply chain are used to transfer and carry large amounts of data. Companies in the supply chain often need to share inventory information, the demand for information, sales information, forecasts, customer data and technical documentation and so on. It provides the hostile a very easy way to access or tamper with the internal information and resources to make disruptions.

One of the most important information threats is supply chain information leakage, which is the process of leaking information intentionally or unintentionally to the enterprises not involved in the enterprise information sharing. Here the enterprises include the ones in the supply chain but not involved in the information sharing and the ones outside the supply chain. [4] Supply chain information is always leaked through the following four ways:

- Leaking from third party outside the supply chain
- Leaking from the upstream enterprises
- Leaking from the downstream enterprises
- Leaking from supply chain management system

2.2 Systematic Threats in ICT Supply Chain

ICT supply chain activities began with acquirement, but rarely acquirement system can track the final product completely in the supply chain. Acquirers often only know about the participants in contact with him directly but know nothing about sub-suppliers in the supply chain. Any secondary supplier can insert loopholes in software or hardware he provides.

The composition and structure of system itself jointly determine the system security threats which ICT supply chain is facing. Once there is a conflict or system bottlenecks in the system itself, it's likely that the system cannot effectively come into play. The overall strength of any system is only as strong as its weakest point, that is, system bottleneck. If there is a great disparity in capacity and strength between the system bottleneck capacity and other members, we can identify supply chain structure is irrational, existing the systemic risk of structural imbalance. [17]

Systematic threats include embedded malicious logic, counterfeit components, and critical products interruption, replacement of old components, penetration of unintentional vulnerabilities and so on. The details of these vulnerabilities are shown in Table 1.

Table 1. Systematic threats in ICT supply chain

Vulnerabilities	*Detail*
Embedded malicious logic	Deliberately include or implant hardware, firmware or software in the system with malicious intent (such as, viruses and Trojans).
Counterfeit components	Contain hardware or software with counterfeit components or code
Critical products interruption	Sudden accidents bring that shipments and customer demand, cost or quality deviate significantly from the supply chain management's objectives.
Replacement of old components	Suppliers stop producing hardware and software, but the Operating time of the system is longer than its components', so that the system owner must find alternative sources corresponding to replace the component.
Penetration of unintentional vulnerabilities	Inadvertently insert hardware, software or firmware which may cause damage in the system, they are produced from unintentional behaviour.

2.3 Cyber Threats in ICT Supply Chain

All aspects of the supply chain are likely to suffer from network attacks or manipulation. Much of ICT supply chain facing threats are caused by the network, while many network threats are caused by network attacks.

The asymmetries of converged computer and communications technologies available to cyber actors are especially striking. Beyond an Internet-connected computer, the cyber attackers' marginal technical and operational resource requirements are low. The barriers of entry to cyber actors at all levels of organization are low. The cost of exploits is low. The cost of launching attacks is low. The cost of failure or getting caught is also low. [8]

2.4 Examples in Hardware Supply Chain Security

Here, we provide an example to explain the three aspects of threats. The security risks which hardware supply chain are facing not only include traditional risk factors, such as natural disasters, terrorist incidents, emergencies, but also include its own unique threats in ICT supply chain, such as Hardware Trojans, malicious firmware, and counterfeit components, and so on.

A. Hardware Trojan

Hardware Trojan is a small malicious circuit, which is artificially implanted electronic systems during the supply chain process of integrated circuit design, manufacturing or secondary development. At some time point or someone launches an cyber-attack by it, it can make IC disabled or destroyed IC, and may also disclose confidential information to the opponent, and even change the system functions to reach the purposes of monitoring and damaging the opponents or potential opponents. This threat covers both information and cyber threats.

B. Malicious firmware

Firmware is a software program in a specific hardware device. For certain types of hardware, firmware can be set by the device manufacturer, and will not change. Malicious firmware refers to firmware with malicious code. Malicious firmware can always lurk in the electronic equipment. Once its execution conditions formed, it may lead to information system failures, and even control electronic devices under the control of the attacker.

C. Counterfeit

Office of Technology Evaluation, which is belong to Bureau of Industry and Security under U.S. Department of Commerce, developed a broad definition of the term “counterfeit” to encompass the views of different segments of the supply chain. For this assessment, a counterfeit is an electronic part that is not genuine because it: is an unauthorized copy; does not conform to original component manufacturer (OCM) design, model, and/or performance standards; is not produced by the OCM or is produced by unauthorized contractors; is an off-specification, defective, or used OCM product sold as “new” or working; or has incorrect or false markings and/or documentation. [5]

3. Models on ICT Supply Chain Security

It is because of the presence of the security problems in all aspects of the ICT supply chain, we need to implement security measures. So far, models covering the entire ICT supply chain operations have not been developed, but several famous supply chain models have been promulgated.

3.1 Supply Chain Operations Reference Model

The supply chain operations reference model (SCOR) is a supply chain management approach developed and authorized by the international Supply-Chain Council (SCC).Its basic idea is to integrate business process reengineering, benchmarking and best practices into a multifunctional model [3]. SCOR is the first standard supply chain process reference model and it is a supply chain diagnostic tool that covers all industries. It is conducive to promoting the internal and external supply chain cooperation and the level process integration, by means of giving relationships between processes (such as planning and acquisition, planning and manufacturing). It enables accurately communication between enterprises, objective performance assessment, and the determination of performance improvement.

3.2 Cyber Supply Chain Assurance Reference Model

In support of the CNCI and its urgent mission to protect the nation's cyber-assets, SAIC and the Supply Chain Management Center (SCMS) of the Robert H. Smith School of Business, University of Maryland (UMD) at College Park, collaboratively undertook a research initiative to develop a Cyber Supply Chain Assurance Reference Model [19].

It stresses there is a need to implement security measures in cyber supply chain life cycle and to make an effective integration between the field of network security and supply chain risk management. It research sought to fuse together the fields of cyber security and supply chain risk management by applying proven supply chain practices to this evolving cyber domain.

This research first give a description of network supply chain ecosystem and gives each key actor's role: policy makers, ecosystem acquisition specialists, system integrators, software developers, hardware/component developers, network providers, operators/end users. Then it defines the cyber supply chain assurance model which includes strategic relations, organizational structure, operating parameters and scope of application.

The most important goal of the ICT supply chain security assurance model is:

definite a series of related principles/measures and its organizational framework. If these principles/measures are effectively implemented, the construction and operation of the cooperating agencies, the integrity and quality of ICT supply chain system, and the highly integrated control implementation will become reality. Based on the actors' common interests, this model not only makes enterprise itself be in charge of the upstream enterprises, but also for the whole supply chain.

3.3 Supply Chain Security Dimension Model

Supply chain security dimension model is proposed in "Transportation & Logistics 2030 Volume 4: Securing the supply chain" published by PricewaterhouseCoopers, which responses to the problem of supply chain security in the context of globalization. This model takes a comprehensive look across five dimensions of supply chain security: personnel security, ICT security, process security, physical security, supply chain security partnerships and offer suggested activities for each area, supported by a key performance indicator (KPI) and the time horizon for when the activity could be put into practice [18].

This model sketches out a range of possible options. But the list is not exhaustive, and not every activity will be a good fit for every organization, particularly as existing legislation varies around the world. It should, however, serve as a pragmatic starting point for thinking creatively about how you can optimize your security profile. It can also help promote discussion with supply chain partners about how to work together to improve the security of shipments throughout the entire supply chain.

3.4 NIST-System Development Life Cycle Model

NIST-System Development Life Cycle Model is proposed by the U.S National Institute of Standards and Technology (NIST) in its special publication NIST SP 800-64. It first describes key security roles and responsibilities in most information system development. Then it fits security measures into all the phases of system development life cycle model (SDLC) [7].

3.5 Software Supply Chain Security Models

For assuring software supply chain security, we summarize and describe five kinds of software supply chain security assurance models, including S3R, the Microsoft SDL, OWASP CLASP, Touchpoints and OWASP SAMM. [6]

- S3R, which is means security, safety, survivability and reliability, is software assurance model. It was proposed to describe the discipline of software assurance.
- The Microsoft Security Development Lifecycle (SDL) is a software development process used and proposed by Microsoft to reduce software maintenance costs and increase reliability of software concerning software security related bugs.
- CLASP is the outgrowth of years of extensive field work in which system resources of many development lifecycles were methodically decomposed in order to create a comprehensive set of security requirements. These resulting requirements form the basis of CLASP's best practices which allow organizations to systematically address vulnerabilities that, if exploited, can result in the failure of basic security services — e.g., confidentiality, authentication, and access control.
- Software Security Touchpoints Model is based on good software engineering and involves explicitly pondering security throughout the software lifecycle. It specifies one set of touchpoints and shows how software practitioners can apply them to the various software artifacts produced during software development, including requirements, architecture, design, coding, testing, validation, measurement and maintenance.
- The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization.

4. Standards for ICT Supply Chain

So far, International standards covering the entire ICT supply chain operations have not been developed, but the ones involving one or several aspects have been promulgated. This paper provides an overview of standards in the aspects of the information management and system assurance.

4.1 An Overview of the ICT Supply Chain Standards

As shown in Fig. 2, the ISO 27000 family of standards can be basically divided into the following four parts. It reserves 60 standard numbers from ISO/IEC27000 to ISO/IEC 27059. So far, the organizations have released 14 standards of the information security management system.

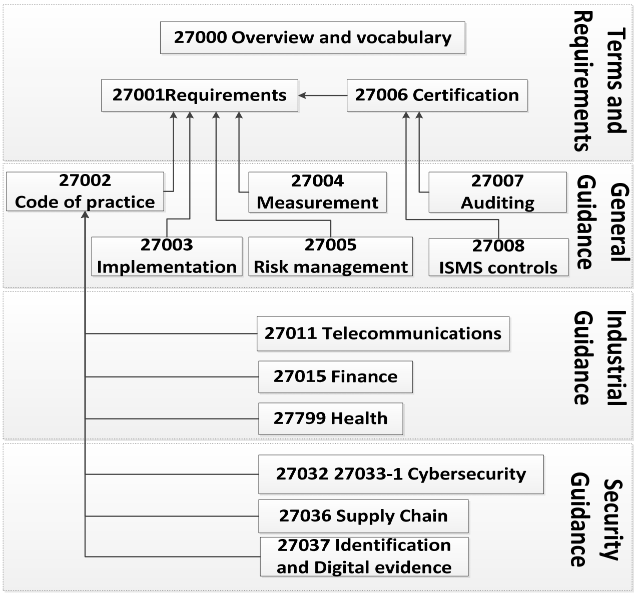

Fig.2: Classification of ISO 27000

As shown in Fig. 3, [10] ISO/IEC 15288 and ISO/IEC 12207 are working together to contribute to the diversification of the system. They are supported by four criteria, which provide additional requirements and guidelines on common problems: ISO/IEC 15289 is the executive documentation of the lifecycle process; ISO/IEC 15939 is the measurement process; ISO/IEC 16085 is the risk management process; ISO/IEC 16326 is the project management process. In addition, ISO/IEC 24748 describes how the lifecycle processes manage the entire lifecycle of the development of a system or software. ISO/IEC 15026 is compatible with other standards. [11]

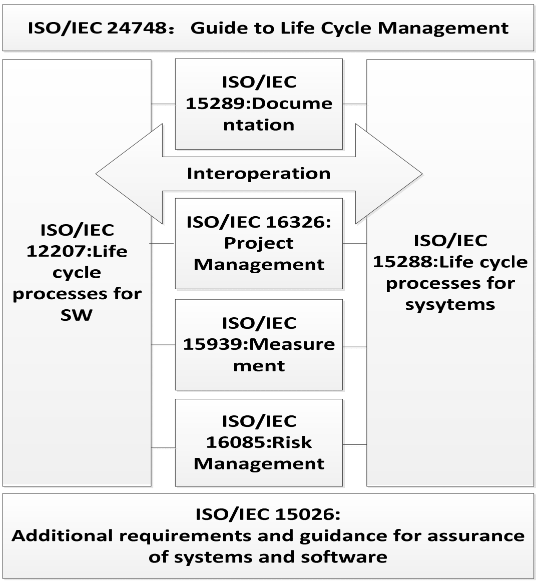
ISO/IEC 24748： Guide to Life Cycle Management
ISO/IEC 12207:Life cycle processes for SW
ISO/IEC 15289:Documentation
Interoperation
ISO/IEC 16326: Project Management
ISO/IEC 15939:Measurement
ISO/IEC 16085:Risk Management
ISO/IEC 15288:Life cycle processes for sysytems
ISO/IEC 15026: Additional requirements and guidance for assurance of systems and software

Fig.3: Standards on System Assurance [6]

4.2 ISO/IEC 27036

ISO and IEC develop the international standard 27036 for the ICT information security management from the view of supply chain. ISO/IEC 27036 provides needs and guidance for suppliers and buyers in how to protect the information in the supplier relationship. It can increase the visibility and traceability of the supply chain and help buyers know more about the product origin and development or integrated product operation situation. [12] The third part of the ISO/IEC 27036 is dedicated ICT supply Chain Security Guide. ISO/IEC 27036-3 explains how to get and manage the security risks caused by the geographical dispersion of the ICT supply chain, how to integrate the processes and practices of information security into life cycle process of systems and software, and how to establish response for the risks caused by the global supply chain of ICT products and services, including all the risks that have the ability to affect the security of agency which use the products and services. [13]

4.3 ISO/IEC 15026

Large-scale system represents complex supply chain integration. In order to cope with the risk of system integration, ISO developed the system and software assurance international standards ISO 15026, which provides an overall framework to connect different disciplines and links with existing standard of life cycle process. It provides a unified set of underlying concepts for ICT supply chain systems integration, and makes the understanding of views across different fields and the clear use of terminology become a reality. It provides lifecycle requirements, including systems and software product development, operations, and maintenance. In this way, various measures can be injected into the ICT supply chain from the requirement phase and the system assurance throughout the life cycle can be a reality. [9]

4.4 NISTIR 7622

As securing the ICT supply chain, it is urgent and worthwhile for countries and regions to propose a new standard of managing security risks for Information Systems. NISTIR 7622 is guidance for cyber supply chain risk management drafted by the U.S. National Institute of Standards and Technology (NIST), designed to eliminate the supply chain risk of the high-impact joint information system life cycle in the process of purchase, development and operation. This document is the first concrete step in addressing the portions of the Comprehensive National Cyber Security Initiative (CNCI) concerned with Supply Chain management. Overall, this document demonstrates the US Government's attention about supply chain, components and design tools sourcing for critical infrastructure systems [2].

5. Conclusion

Many countries are purchasing foreign IT products and services, which is equivalent to open the door of the national security. So it is necessary to conduct this study. Countries should proceed from their own national conditions, developing both in line with its own national conditions and consistent with international standards of ICT supply chain security. It can be considered as follows: Rank systems and services acquirement as an important security control class; Develop risk management measures of information systems supply chain; Refer to the rules of the WTO effectively; Establish an authoritative third-party certification standards actively.

ICT supply chain security involves multiple disciplines and fields. This study cannot contain all of them. And much further study would be taken in the future.

Acknowledgement

This work is supported by the following programs: the National Natural Science

Foundation of China under Grant No.61170273; Open Project Foundation of Information Technology Research Base of Civil Aviation Administration of China (NO.CAAC-ITRB-201201); 2010 Information Security Program of China National Development and Reform Commission with the title "Testing Usability and Security of Network Service Software".

References

Boske, L. B. (2006). Port and supply-chain security initiatives in the United States and abroad. *NIST*, Gaithersburg.

Boyens J., Paulsen C., Bartol N., Moorthy R., & Shankles S.. (2012) NISTIR 7622: Notional Supply Chain Risk Management Practices for Federal Information Systems. *NIST*, Gaithersburg.

Deliver, M. (2003). Supply-Chain Operations Reference-model. *Supply-Chain Council.*

Dong, S.H., Xi, B., T, L.N. (2009). Ways of Information Leakage of Supply Chain and Their Prevention Countermeasures, *Commercial Research,* 12, 33-39.

DoC. (2010). Defense Industrial Base Assessment: *Counterfeit Electronics*. U.S. Department of Commerce, Washington, D.C

Ellison, R. J., Goodenough, J. B., Weinstock, C. B., & Woody, C. (2010). Evaluating and mitigating software supply chain security risks (No. CMU/SEI-2010-TN-016). *Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst.*

Grance, T., Hash, J., & Stevens, M. (2003). NIST SP800-64: Security Considerations in the Information System Development Life Cycle. *NIST*, Gaithersburg.

Hageman, H., Harper I., & Sagan P.M., Weyman A. (2010). Cyber Threats to National Security: Countering Challenges to the Global Supply Chain. *CNCI and USNI*, Virginia.

ISO. (2008). Systems and software engineering –Systems and software assurance-part 1: Concepts and vocabulary. *ISO*, Geneva.

ISO. (2009). ISO27000: Information technology-Security-techniques-Information security management systems-Overview and vocabulary. *ISO,* Geneva.

ISO. (2010). Cyber Security and ICT SCRM Standards. *ISO*, Geneva.

ISO. (2012). Information technology -Security techniques -Information security for supplier relationships-Part 1: Overview and concepts. *ISO*, Geneva.

ISO. (2012). Information technology -Security techniques -Information security for supplier relationships-Part 3: Guidelines for ICT supply chain security. *ISO*, Geneva.

Liu H.L, Cao, Y. (2012). Evaluation system of the supply chain stability. *Journal of System and Management Sciences*, 2(1), 70-78.

Li, Y, Chen, X.F, & Jia, L. (2013). Supply chain disruption assessment based on the newsvendor model, *JIEM,* 6(1), 188-199.

Swanson, M., Bartol, N. and Moorthy R. (2010). NISTIR 7622: Piloting Supply Chain Risk Management Practices for Federal Information Systems. *NIST*, Gaithersburg

Nicholas, Paul. (2009). Global Supply Chain Security: Towards a Common Risk-based Framework, *Microsoft*, Redmond.

PwC. (2011). Transportation & Logistics 2030 Volume 4: Securing the supply chain. *PricewaterhouseCoopers*, London

Rossman, H., Smith, R. H. (2009). Developing A Cyber Supply Chain Assurance Reference Model. University Of Maryland and Supply Chain Management Center, *Maryland.*

Zlatko NEDELKO. (2008). The Role of Information and Communication Technology in Supply Chain. *Logistics & Sustainable Transport*. 1(3). 13-20.