Architectural Solution Integration to Contain ICT Supply Chain Threats

Xiaofeng QIU
Beijing University of Posts and Telecommunications
Beijing,P.R.China
qiuxiaofeng@gmail.com

Liang ZHAO
NSFOCUS
Beijing, P.R.China
richard.zhao@nsfocus.com

***Abstract*—Information Communication Technology, which has been more and more critical in the modern economy and society , means more than information technology and traditional telecommunications. The integrity of ICT supply chain has slightly different meaning than the traditional security and assurance. Partly for the sake of difficulties to technically testify the increasingly complicated modern ICT products, it's by no means to figure out an end to end integrity assurance program and methodology, letting alone test cost and timing factors.**

This paper investigates the threats of ICT supply chain integrity, particularly covert channel. An architectural approach, named as Architectural Solution Integration, is given out to assure the integrity of ICT system and contain the potential threats through supply chains. The quantitative assessment of ICT supply chain integrity is discussed as well, followed by the future work analysis.

Keywords —ICT Supply Chain Integrity； assurance； security； covert channel

I. INTRODUCTION

Nowadays, Information Communication Technology systems have been core components of the critical infrastructure of many industries, while most of these systems count on multiple vendors to design, build, provision, etc. As shown by the Fig.1, typically each of the suppliers has to produce its ICT software and/or hardware based on its own suppliers (they are named tier 2 suppliers hereafter). Offshore outsourcing, which has been becoming more and more popular in order to lower the cost of ICT design and manufacturing, elongates the ICT supply chain and worsens the integrity concerns [1].

From technical perspective, these ICT supply chains have becoming so overwhelmingly complicated in the modern industry that it's non-practical or mission impossible to approve the integrity of an ICT system or even a single component thoroughly, through testing to cover 100% of system functionalities.

Meanwhile, increasing number of bugs, vulnerabilities, Trojan horses, and security incidents due to nefarious insiders and industrial espionage activities have been reported [2].

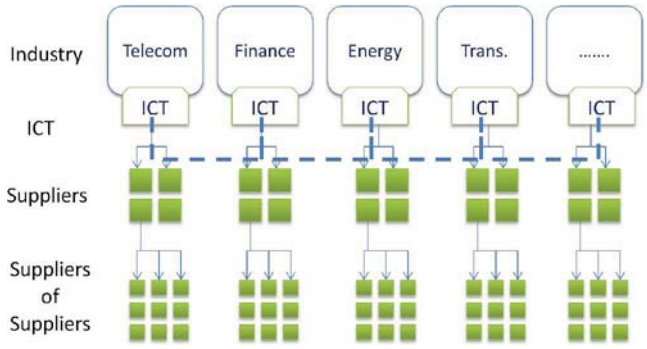

Fig.1 ICT Supply Chain

There is a concern raised about warfare attacks through ICT supply chain, even though ICT supply chain attacks was regarded not as efficient as other common vulnerability based remote attacks [3].

In the past years, a few standardization development organizations (SDO) and 3rd party industrial organizations have been working on the survey and frameworks to improve the integrity of ICT supply chain.

At the first *Worldwide Cybersecurity Summit*, a breakthrough group championed by East West Institute was kicked off to address the issues haunting around *ICT Development Supply Chain Integrity* [4].

It's very critical to notice that, for the sake of overwhelming complexity of modern ICT systems, it's not feasible to redo the large existing base of ICT systems. That means, from a practical perspective, even a high security ICT system might have to be built upon or work with some components designed or manufactured by not-so-trustworthy suppliers. How to build trustworthy system with untrustworthy components should be an emerging challenge for the enterprise architects and technical decision makers.

A brief analysis of threats to ICT supply chain integrity is given at section 2. An innovative architectural design methodology to address the untrustworthiness is introduced at section 3. Future works are discussed at section 4.

II. THREATS TO ICT SUPPLY CHAIN INTEGRITY

A technology supply chain attack subverts the hardware, software, or configuration of a product, prior to customer delivery, for the purpose of introducing an exploitable vulnerability [5].

978-0-615-51608-0/11 ©2011 EWI

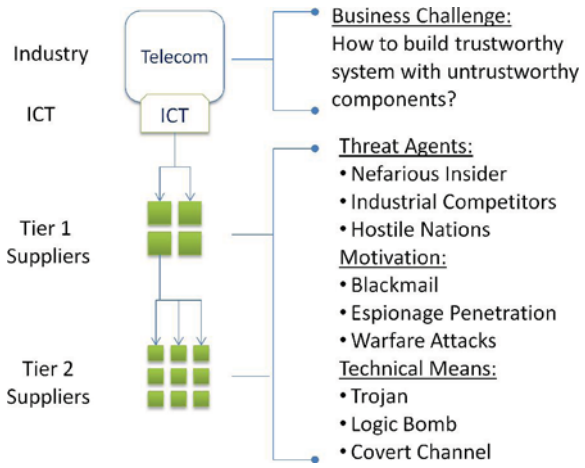

Fig.2 Threats to Supply Chain Integrity

There are multiple agents who have the potential to conduct supply chain attacks, including nefarious insiders, industrial competitors, and even hostile nations. The motivations of supply chain attacks may range from individual blackmail, to espionage penetration and even cyber warfare attacks, as shown by Fig.2.

The threat agents may conduct attacks through Trojan horses, logic bomb, covert channel, and etc.

Generally, there are two most popular ways to plant Trojan horse, logic bomb and covert channel inside an ICT component - modification of an existing file and insertion of a new file. Some best practices have been suggested by industrial organizations, including use of reconciliation or brand protection technology within the fabrication/assembly processes, e.g. the use of tamper-resistant packaging, remote tracking and monitoring, tilt meters, code signing, etc.[5]

They are good practices to mitigate attacks by nefarious insiders and intruders. However, considering the integrity concerns related to warfare or untrustworthy suppliers, those best practices are not adequate to eliminate or contain the supply chain attacks. A malicious supplier or malicious insider working for a tier 1 or tier 2 supplier still has various means to perform unpredictable operations through a sophisticated covert channel.

In computer security, a covert channel is a type of computer security attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy [6].

More commonly, we think of covert channels within the context of transferring information from within a protected network to a remote host on the outside of that network and connected to it by the Internet.

According to "The Orange Book", two types of covert channels exist: storage and timing channels. A storage channel "involves the direct or indirect writing of a storage location by one process and the direct or indirect reading of the storage location by another process". A timing channel involves a sender process that "signals information to another by modulating its own use of system resources (e.g.,CPU time) in such a way that this manipulation affects the real response time observed by the second process"

Reportedly, covert channel is widely used to conduct various malicious operations ranging from personal data theft to industrial espionage [7].

Covert channel analysis is listed as part of the standard assurance testing for a software system with B2 security level requirement or EAL5 in Common Criteria equivalently [8]. That means there is not covert channel analysis at all for the ICT systems with security assurance requirement below EAL5. Cost and inadequacy of technological means might be part of the reasons behind this situation.

Covert channel attack is a typical asymmetric attack where an attacker can evade the expensive security and integrity testing and monitoring with relatively minor effort.

Unfortunately, once again it's very challenging or mission impossible to detect and remove covert channel from both practical and theoretical perspectives.

In summary, covert channel is one of the major threats to ICT supply chain integrity. No matter through modification or insertion of files, it's very expensive and time consuming or even impractical to guarantee the integrity through technical testing.

An innovative approach is needed to address the issues around the untrustworthiness of suppliers.

III. Architectural Solution Integration

Generally, there has been relatively mature software security and quality standards or best practice frameworks in place, including ISO 9000 and ISO27001, Capability Maturity Model, SAS 70, and Security Guidance released by Cloud Security Alliance, etc. They provide a commonly agreed benchmark to help qualify suppliers.

For organizations with higher security concerns, 3rd party product validation and certification systems have been operating for decades, including TCSEC and Common Criteria. They are used to test out the conformance of an ICT product or a component.

EAL 5 and above have not been widely implemented at the industry so far, while EAL 4 and below cannot provide adequate assurance to many organizations with very high security requirements.

After investigating the previous threat analysis and existing practices, a layered approach is explored to analyze, describe and address ICT supply chain integrity objectives. This idea was firstly touched at the first *Worldwide Cybersecurity Summit* at Dallas[4].

As shown by Fig.3, four layers are designed to reflect different assurance level of ICT supply chain integrity. From bottom up, layer 1 is the process and best practice based quality systems as we have described; layer 2 is the 3rd party functionality testing and certification; layer 3 is the architectural solution integration which is our focus at this paper. The top layer is to reflect the most strict integrity requirements which are titled as "Hostile solution

validation". Conceptually, we put two test scenarios under the top layer, including:

- Extreme testing including Distributed Denial of Service and Electromagnetic Pulse (EMP), etc.
- Extreme service/application level starving test, etc.

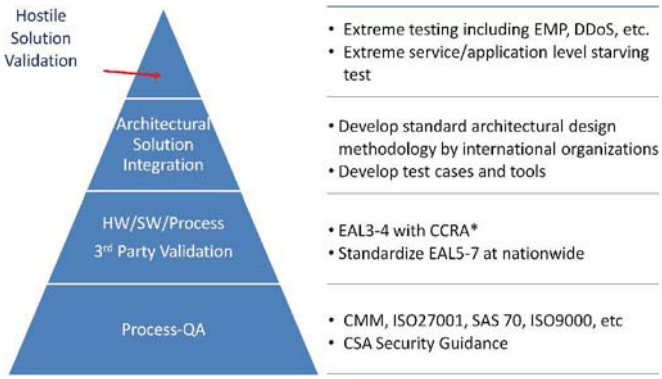

Fig.3 Architectural Solution Integration

Architectural Solution Integration (ASI) is designed to contain the potential supply chain attacks through interrupting and exposing the covert channels. Supplier diversifying is one of the major design criteria to meet this objective.

It consists of the following critical activities:

- Design, populate and maintain the Supplier Database (SDB) which includes various attributes and relationships to other suppliers
- Identify major threats and critical information assets that need to be protected
- Analyze data flow and critical path
- Assess the trustworthiness of each critical path
- Tune the network topology and suppliers and perform assessment recursively till security policy is met.

SDB is a fundamental component of ASI, providing the core intelligence. Supplier attributes and relationships are two main categories of data in the database. The major attributes of each supplier might include trustworthiness, locations, suppliers, technologies, etc., where trustworthiness is somewhat a credit and reputation system from the implementation perspective. It should be updated regularly based on solid information sharing among public and private sectors. The attribute of "Suppliers" is a recursive enumeration reflecting the supply chain, which depends on the security policy that how many tiers of suppliers should be taken into account. The attribute of "technologies" is a enumeration of hardware and software products. Relationships are designed to reflect the dependencies among suppliers, e.g. "manufactured by", "outsourced to", "subsidiary of", etc.

ASI can bring immediate business values including but not limited to the below:

- Better vendor management and cost efficiency than one-size-fits-all integrity requirements and supplier screening
- Smooth evolvement and living with existing ecosystem
- Built-in ICT Supply Chain Integrity at design phase
- Potential quantitative assessment of ICT systems from Supply Chain Integrity perspective

Let's raise an example to illustrate how ASI works for a small network topology as shown by Fig.4.

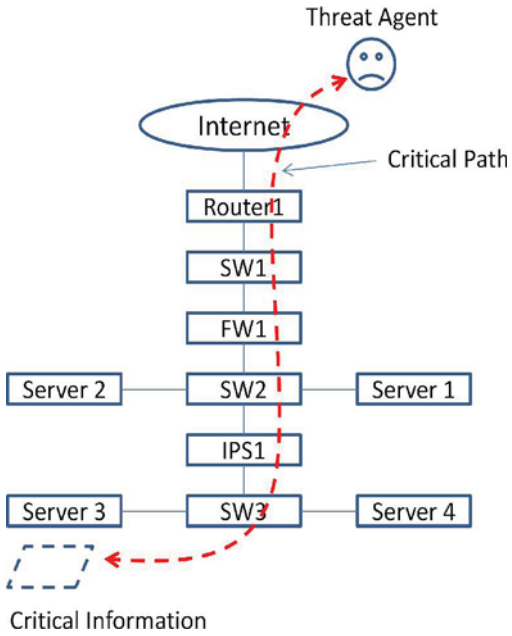

Fig.4 An example of ASI

To simplify the operations, let's consider tier 1 suppliers only. Assuming we have already built a SDB with complete data of suppliers, all the suppliers of ICT components of Fig.4 can be identified, with a corresponding pre-assigned trustworthiness value.

Suppose the data at Server3 is identified as the target critical information. The major threat agent is identified to be from Internet. The dot line might be determined to be the critical path.

We have:

$$\mathbf{S} = \{\boldsymbol{S_1}, \boldsymbol{S_2}, \boldsymbol{S_i}\} \text{ and } \mathbf{T} = \{\boldsymbol{T_1}, \boldsymbol{T_2}, \boldsymbol{T_i}\} \quad (1)$$

where S represents supplier set, S_i is ith supplier along the path, T represents trustworthiness set, T_i is the trustworthiness value of S_i .

The trustworthiness of this critical path can be calculated to be:

$$\boldsymbol{T}|_{\boldsymbol{CP}} = \boldsymbol{f}(\boldsymbol{T}) \quad (2)$$

Where $T|_{CP}$ represents the trustworthiness value of the critical path. Relationships may influence the function $\boldsymbol{f}$ as well.

If $\mathbf{T}|_{CP} < \mathbf{T}|_{Policy}$, either some of the suppliers or the network topology should be adjusted. The critical path trustworthiness will be recalculated and compared with the

policy value. This loop will be conducted recursively until the trustworthiness criterion is met.

The calculation in a real scenario must be much more complicated than the above one, particularly when the security policy requires that more tiers of suppliers must be investigated. In addition, the critical path analysis could lead to multiple paths for a single pair of threat agent and critical data.

It must be noticed that vendor diversifying will bring additional cost and complexity to IT operations, while it brings benefits from supply chain integrity perspective.

Although this example demonstrates how to apply ASI to analyze ICT infrastructure supply chain integrity, in fact, ASI can be applied to application and service cases. Nowadays, more and more ICT services will be migrated into cloud that might be running at a remote public cloud data center. Under this scenario, very possibly, only the services and interfaces can be available for user test. The security testing methodology and tools for cloud services by far lag behind those of traditional static (with source code) and dynamic (with binary code only) testing. This will bring additional challenges to assess and guarantee the supply chain integrity of cloud services. ASI is expected to work as long as the cloud service provider shares adequate information about the related structure and data flow inside the cloud.

IV. Future Works of Architectural Solution Integration

Architectural solution integration can help contain the threats of ICT supply chain integrity, without rebuilding the critical ICT systems with totally trustworthy elements which means formidable cost increase compared with current sourcing structure. A series of collaborative research and development efforts by both public and private sectors are needed to further this innovative approach, which include the below critical areas:

- Architectural solution integration and corresponding assessment methodology. Standard components and relationships must be defined as the common language. International agreements, standards, policy and regulations (ASPR) are critical to the success of ASI.
- Visualization of data flow. A thorough and complete data flow analysis for a certain ICT system topology and structure is the key to guarantee the final effectiveness.
- Supplier distribution and dependency analysis. Various supplier combinations of a certain ICT system are evaluated with dependency analysis.
- Tolerance analysis with graph theory. Graph theory has potential to be exploited to evaluate the assurance to tolerate the failure of supply chain integrity or contain the potential supply chain attacks.
- Simulation of the architectural solution integration. Simulation software can help implement ASI and quantitatively evaluate an ICT architecture from ICT supply chain perspective.

Acknowledgement

Authors would like to appreciate Mr. Karl Rauscher，Mr. Mark Adams for the discussions on the initial idea of this paper.

Reference

[1] ENISA, Priorities for Research on Current and Emerging Network Technologies,

[2]Richards J. Heuer, Jr , Katherine Herbig, Espionage by the Numbers: Statistical Overview , http://www.dm.usda.gov/ocpm/Security%20Guide/Treason/Numbers.htm

[3] SAFECode, The Software Supply Chain Integrity Framework, July 2009

[4] EWI – Initiatives/Break Through groups - http://www.ewi.info/system/files/EWI%20Cybersecurity%20Priority%20Breakthrough%20Subjects%20ExecSummary.pdf

[5] Open Group, O-TTPF, *www.opengroup.org/*

[6] http://en.wikipedia.org/wiki/Covert_channel

[7] http://www.securityfocus.com/news/11406

[8] US Department of Defense, “Trusted Computer System Evaluation Criteria,” "The Orange Book". ,Tech. Rep. DOD 5200.28-ST, December,1985, csrc.nist.gov/publications/history/dod85.pdf