# Secure Information Sharing in Digital Supply Chains

Bharat Bhargava, Rohit Ranchal
PLM, CERIAS and Computer Sciences
Purdue University
West Lafayette, IN, USA
{bbshail, rranchal}@purdue.edu

Lotfi Ben Othmane
Department of Mathematics and Computer Science
Eindhoven University of Technology
Eindhoven, Netherlands
l.ben.othmane@tue.nl

*Abstract*—**Modern organizations interact with their partners through digital supply chain business processes for producing and delivering products and services to consumers. A partner in this supply chain can be a sub-contractor to whom work is outsourced. Each partner in a supply chain uses data, generates data and shares data with other partners, and all this collaboration contributes to producing and delivering the product(s) or service(s). The main security challenge in supply chains is the unauthorized disclosure and data leakage of information shared among the partners. Current approaches for protecting data in supply chain rely on the use of standards, service level agreements, and legal contracts. We propose an auditing based approach for protecting shared data in digital supply chains.**

***Keywords—supply chain; security; privacy; auditing; data sharing***

## I. Introduction

Most organizations are not self-sufficient, i.e., each performs independently its operations for making and delivering products and services to their customers. They primarily focus on their core competences and outsource other activities to specialized partners, such as suppliers, contractors, distributors, advertisers, which is more cost effective. For instance, they outsource delivery of goods to shipping companies such as FedEx or UPS.

Organizations use supply chain to collaborate with their partners in transforming raw materials into products delivered to the customers. Supply chain streamlines materials flowing from the raw material source through various stages in the chain to the final product delivered to the consumer. The movement of physical product and related entities, such as raw materials, resources, unfinished product at different stages, money, is managed through the associated information flow. Effective product management depends upon the effective flow of related information.

The main threats (circumstances or events with the potential to adversely affect a system through unauthorized access, destruction, disclosure, or modification of data, or denial of service [1]) in digital supply chains are **unauthorized disclosure and data leakage of information** shared between the partners—e.g., commercial information shared with advisors and lawyers, personally identifiable information about customers and employees and intellectual property shared with suppliers. The information could be disseminated to other organizations, making it impossible to track its access and usage.

There have been numerous cases of supply chain compromises resulting in substantial damages to organizations. For instance, in November 2012, a $1.5 million stash of iPad minis, coming from Apple's assembly partners in China, was stolen from JFK airport in New York, USA. There have been theories of information leakage within the supply chain that led to this event [2].

A second case: Hackers penetrated Foxconn network—which assembles about 40 percent of the consumer electronics products in the world—and stole sensitive data including contact details of Foxconn's global sales managers, usernames, IP addresses, client e-mails and purchases. They made this stolen data public on the Internet. This data could be used to place fraudulent orders from the Foxconn's clients. Foxconn had to take its services offline to prevent damages [3].

Even the most reputable companies, such as Apple, HP and, Sony have shipped pre-owned laptops, hard drives, and other devices with viruses, worms, and trojans on them which were inserted through their supply chain. There have been numerous cases of counterfeit hardware chips with "built-in back doors" that could allow system access for espionage or data theft. Such chips set up with malicious components through supply chain loopholes have found their way in highly secure organizations like DOD in US [4]. Compromised components coming through the global supply chain weaken the integrity of the products that might jeopardize businesses confidentiality or the overall availability of essential services.

A 2011 report published by Verizon, which analyzed 855 reported data breaches in 2011, indicates that there has been an increase in the number of data breaches across the globe [5]. The report reflects the digital supply chain challenges for the organizations conducting global business. The report advises that high tech companies must implement a comprehensive set of policies and procedures that ensure supply chain data is protected not only at their company, but also among their partners, component suppliers and others handling sensitive supply chain information.

The World Economic Forum, in 2011, also highlighted the problem of supply chain data sharing and the associated threats [6]. The report mentions the increasing importance of information and IT in the supply chain and the problem of securely sharing information.

This paper investigates the security of supply chain. It (1) examines the challenges for securing digital supply chains and (2) proposes an approach for end-to-end security auditing of business processes that compose supply chains. The approach enables tracking the information flows of shared data and detecting compromised business processes of partners. It addresses information leakage and unauthorized data disclosure in supply chains.

The rest of this paper is organized as follows. Section II provides an overview of digital supply chains; Section III outlines the challenges for securing digital supply chains; Section IV reviews existing approaches; Section V describes our approach; and section VI concludes the paper.

## II. Overview of Digital Supply Chains

Organizations collaborate in producing and delivering products to their customers; they share information about the products and about their activities through a digital supply chain system. *A digital supply chain system* is composed of systems (hardware, software, communication networks) that support interaction between globally distributed organizations, orchestrating the activities of the partners in supply chains. The activities include buying, making, storing, moving and selling a product.

Supply chain activities generate new information, share information with other partners who perform supporting activities for the product, and use existing information. This information could be for developing and delivering the products and for improving the efficiency, driving business decisions, and maintaining competitiveness in the market. This information may be a highly sensitive product description, customers' information, trade secrets, blue prints, intellectual property, and private organizational or personal information.

Information used in supply chains changes as the products or services are being made and delivered to customers. For instance, purchase orders are approved or declined; containers are loaded or unloaded; shipments are flagged or cleared; transportation arrives on time or is delayed. Thus, there is a constant *flow of information* in the supply chain.

Organizations track the flow of their information in a supply chain, so they know the access to, use of, and sharing of their information, and the transformation applied to it. They lose this knowledge the moment this information leaves the organization's domain; it is difficult, for an organization to track the information, its interactions and the actions being applied to if it is outside its domain.

The information in a digital supply chain is distributed among and controlled (their usage, sharing, and tracking) by a multitude of parties. A digital supply chain is composed of the supply chain processes of the globally distributed partners. Therefore, the control of information in a digital supply chain cannot be confined to a single domain controlled by a single organization—it doesn't reside inside the boundaries of a single organization.

Figure 1 shows an example of the information exchange between generic services that compose a digital supply chain. For an organization, a partner in the supply chain, there is an internal domain and an external domain. The internal domain includes business processes owned or controlled by the organization, such as product design, manufacturing etc. This domain is trusted because the organization has complete control over the usage, sharing and tracking of information. The external domain[1] includes partner business processes, such as suppliers, distributors, retailers etc. It is not possible to track the information flow in external domain because the organization has no control over the processes in this domain.

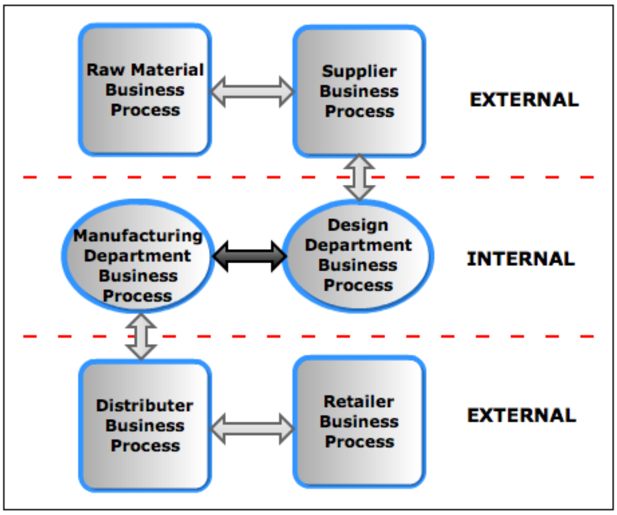
Raw Material Business Process
Supplier Business Process
EXTERNAL
Manufacturing Department Business Process
Design Department Business Process
INTERNAL
Distributer Business Process
Retailer Business Process
EXTERNAL

Figure 1: Information flow in a supply chain.

A key risk [1] in distributed supply chains is of the **unauthorized disclosure and data leakage of information** shared between the partners, across multiple domains. The information could be disseminated to other organizations, making it impossible to track the access to and use of the information.

The impact of the threats [1] includes financial losses and damage to the reputation of one or many of the partners. Leaked information could reach competitors, malicious entities, government institutions, or criminal organizations [1]. For instance, organizations may suffer high financial losses if the list of customers or product secrets reaches competitors. Also, leakage of sensitive governmental information may be used by criminal organizations and affects national security.

Organizations fear information leakage and unauthorized disclosures of information. They are sometimes reluctant to share information with other organizations in the distributed supply chain. This results in inefficiencies in distributed supply chains, e.g. resource mismanagement, inventory misallocation, shortages, costly transportation, increased product prices and reduced customer service. Thus, it is imperative that supply chain information be protected according to its owner's policies, regulatory and legal requirements.

[1] Actually, the external domain is composed of a set of domains, each is of a partner. An organization views the set of domains of its partners in a supply chain as one external domain.

## III. Challenges for Securing Digital Supply Chains

There are three main challenges in distributed supply chains. Their description follows.

The first challenge is the lack of mechanisms to communicate owner's policies associated with information to the protection frameworks of the partners of a supply chain. The policies are rules for sharing, accessing, and using the information. The information owner policies may include the required capability of a partner to protect the information, the authorization to a partner to share the information with its sub-contractors, the regulatory and legal policies that the partners must comply with. Violation of the policies could cause big financial and business harms to the owner of the information.

The second challenge is the lack of common, applied, information sharing standards for protecting data in distributed supply chain. Each organization, a member of supply chain, has its own business processes for managing its activities and applies custom security requirements. These differences reduce the ability to ensure enforcement of required policies on the shared information among all partners of a supply chain which may also leave security gaps [8]. Tracking the information flows and ensuring protection of shared data throughout the supply chain is a significant issue.

The third challenge is that the information security standards evolve to satisfy changing business models, regulatory and other requirements. This requires, for organizations, not only updating their protection mechanisms, so they comply with the new standards; but also, coordinating with their supply chain partners to have protection mechanisms that could integrate to enforce the security and privacy policies they require.

## IV. Existing Approaches

This section[2] describes four existing approaches that aim to protect data shared in supply chains. They are GS1 standards, NIST guidelines, secure supply chain protocols, and Active bundles for securely sharing information.

### A. GS1 Standards

*GS1* [9] are the most used supply chain standards. They define the EPCglobal computer network to securely share product data and track objects in transit between supply chain partners—e.g., suppliers, manufacturers, logistic providers, retailers, or third parties. Supply chain partners use the network to interact, get information and share information.

Products have Radio Frequency Identification Devices (RFID), which enable capturing and reporting their movements to the EPCglobal network; RFIDs are used to track the products, e.g., track products moving through a manufacturing or distribution facility.

GS1 standards enable to efficiently share information about products across multiple partners in a supply chain [9]. However, they have severe limitations in protecting the product's information including: (1) do not consider how sensitive information are used, shared or protected by partners, (2) do not consider owner policies related to the information usage (3) do not provide any mechanism to ensure correct policy (rules for accessing and using the data that are generally set by the creator of the data) enforcement by the partners.

The impact of these limitations includes: unauthorized track and use of information by entities not part of a supply chain, violate the privacy [1] of the partners, and identify assets of an individual or an organization. A Virtual Private Network (VPN) can be used to address the limitations and reduce the risks of confidentiality and integrity compromise. However, the technique does not scale, has administrative overhead for a dynamic, distributed, and global supply chain, and doesn't consider owner policies and their correct enforcement [9].

### *B. NIST Guidelines*

The guidelines of the National Institute of Standards and Technology (NIST) for supply chain [10] encourage the use of trusted suppliers, service-level agreements related to quality, and security during various stages of supply chain—e.g., supply, manufacturing, distribution.

In the past, the supply chain solutions have adopted the use of a centralized trusted party. They assume that all the information in the supply chain (e.g., supplier information, manufacturing data, prices, inventory status, transportation, etc.) is available to a central planner. In contrsat, current supply chains are distributed and managed by several organizations participating in the supply chain; each has its own policies, proprietary information, and specific information that it can access or use.

### *C. Secure supply chain protocols*

Atallah et al. [11] address the problem of reluctance of organizations to share their information in distributed supply chain; they give protocols for secure supply chain interactions. The proposed approach is theoritical; the authors do not discuss the implementation of their protocols in a supply chain system and do not evaluate the impact of their protocols.

### *D. Using Active bundles for securely sharing information*

We proposed in [12] an approach for securely sharing information in Product Lifecycle Management (PLM) systems using the concept of self-protecting data based on the active bundle construct [15, 16]. PLM solutions support the development and management over the entire lifecycle of products from concept to retirement and have supply chain management as one of their components.

## V. Proposed Secure Data Sharing Approach

This section provides an overview of the proposed approach, describes the components of the architecture, and describes the information flow of an example supply chain scenario.

### *A. Overview of the proposed approach*

The aim of a secure distributed supply chain system is to provide information to partners but ensure only authorized

[2] The aim of this section is to report about some of the existing approaches and not to survey the existing literature.

entities can access and use the information and the information is only used in the context of the supply chain. The approach will ensure the following:

- Controlled information sharing in trusted domains.
- Information flow tracking in trusted domains.
- Monitoring information usage and detecting illegal sharing in trusted domains.
- Noninterference between the security mechanisms and the supply chain operations.
- Being scalable and reliable, so it could be used for large supply chains.
- Reporting unauthorized information usage and disclosure by entities while in transit between the partners.

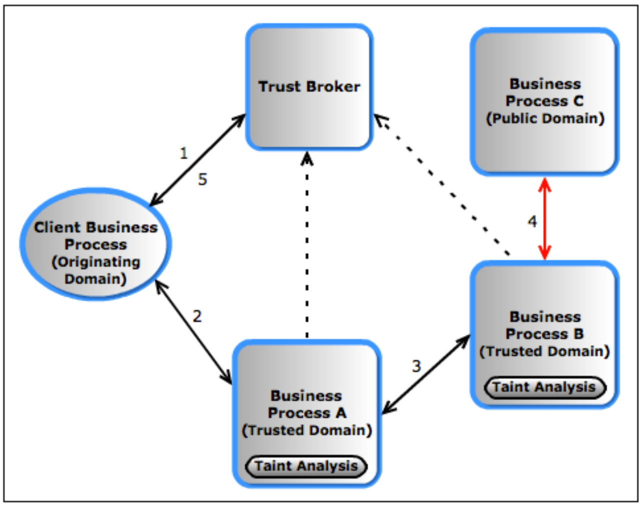
Trust Broker
Business Process C (Public Domain)
1
5
4
Client Business Process (Originating Domain)
2
3
Business Process B (Trusted Domain)
Taint Analysis
Business Process A (Trusted Domain)
Taint Analysis

Figure 2: An example of supply chain composed of three partners. (The Trust Broker is typically not a partner and an organization that manages Business Process in Public Domain C—is not a member of the supply chain, but it provides services to a partner that controls Business Process B in a Trusted Domain.)

We developed a solution for assuring end-to-end security in Web services that use external web services in [13]. We propose to adapt the approach we used, to secure interactions between business processes of organizations that compose a digital supply chain—assuming a secure communication channel between the organizations. We substitute web services with business processes. In both cases the solution tracks the data flow and actions upon them and enables auditing, detecting and reporting policy violations. (Policy violations occur when an entity accesses or uses data while it is not allowed by the policy or uses it for a purpose other than the ones specified by the policy.)

In the following we simulate the proposed approach in a reference scenario.

### B. *Components of the proposed architecture*

Figure 2 depicts the scenario, which is composed of a Client Business Process, a Trusted Business Process A, a Trusted Business Process B, a Public Business Process C, and a Trusted Broker (TB).

A *client business process* is a business process managed by the originating domain i.e. the organization owning the product in the supply chain. A *trusted business process* is either (1) a business process managed by the originating domain or (2) a business process managed by a domain that uses our Taint Analysis (TA) module. An *untrusted business process* is a business process that does not fit above two criteria for a trusted business process (Public Business Process C in this case).

*TA module* (detailed description in [13]) monitors the interactions of business processes (at runtime) and inspects the data exchanges (information flow) between them to detect policy violations. TA uses program instrumentation, which hooks to the execution; so that the TA component can gain control when certain events occur while business processes process data. We instrument business processes using aspect oriented programming (AOP) [14], which enables auditing business processes and keeping a reasonable overhead [13].

A *Trust Broker (TB)* (detailed description in [13]) is a trusted third party responsible for maintaining end-to-end auditing in a chain of information flow upon the request of a client business process. TB has the following two functions:

1. It maintains a list of certified business processes that use the TA Module and their compliance with the required security requirements. A business process is certified by the TB upon certification by an external trusted authority. The certification assures that the business process allows tracking of information flow and ensures secure messaging.
2. It maintains an end-to-end session of business processes' interactions. A client process initiates an interaction in the supply chain by requesting TB to create a session for the interactions of the partners in the context of the supply chain. TB collects and logs the activities of the business processes of the collaborating partners. If a trusted business process interacts with public services (possibly sharing client process's information) or interacts with trusted business processes that are not supposed to collaborate in the supply chain, TB logs a warning and informs the client process about the detected violation.

### C. *Information flow using the proposed solution*

The information flow of the scenario, as shown in Figure 2, is:

1. The Client Business Process decides sharing information with a Trusted Business Process A and requests a session in the Trust Broker (TB) to keep track of this interaction's activities for end-to-end information flow.
2. The Client Business Process shares information with Trusted Business Process A.
3. The Trusted Business Process A uses this information and shares it with Trusted Business Process B. During this

exchange, the Taint Analysis (TA) module intercepts the communications and reports any illegal external interaction to the TB.

4. Trusted Business Process B shares data with (possibly untrusted) Public Business Process C. TA detects the interaction and reports the activity to TB.

5. TB informs the Client Business Process about the activity of Trusted Business process B.

## VI. Conclusion

This paper investigates the challenges and existing approaches for secure collaboration among partners in digital supply chains and proposes an innovative approach that relies on the use of trust broker and taint analysis. Future work will involve developing an application specific prototype and evaluating it in a real scenario.

## Acknowledgment

This research was supported by a grant from PLM Center of Excellence and CERIAS at Purdue University.

## References

[1] R. Shirey, “Internet Security Glossary, Version 2,” The Internet Engineering Task Force (IETF), RFC4949, August 2007. Online at http://tools.ietf.org/html/rfc4949

[2] “iPad Mini Heist: $1.5 Million Stash Of Apple Devices Reportedly Stolen From JFK Airport,” Nov. 2012, online at: http://www.huffingtonpost.com/2012/11/15/ipad-mini-heist-million-stolen-jfk-airport_n_2137799.html

[3] “Hackers attack Foxconn for the laughs,” Feb. 2012, online at: http://www.macworld.com/article/1165298/foxconn_reportedly_hacked_by_group_critical_of_working_conditions.html

[4] H. Livingston, T. Telesco, L. Gardner, R. Loeslein, E. Zelinski, and W. Pumford, “Counterfeit Parts Safeguards and Reporting – U.S. Government and Industry Collaboration to Combat the Threat,” Defense Standardization Journal, pp.9-16, Jan/Mar 2010.

[5] “Verizon 2012 Data Breach Investigations Report,” http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf?CMP=DMC-SMB_Z_ZZ_ZZ_Z_TV_N_Z037

[6] World Economic Forum, “New Models for Addressing Supply Chain and Transport Risk,” 2011.

[7] Insider Threat Center at Cert, “Examining Insider Threat Risk at the US Citizenship and Immigration Services,” Dec. 2010, online at: http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_11-33_Jan11.pdf

[8] N. Browne, M. de Crespigny, J. Reavis, K. Roemer, and R. Samani, “Business Assurance for the 21st Century: Navigating the Information Assurance landscape,” white paper, Information Security Forum, 2011.

[9] B. Fabian, and O. Günther, “Security Challenges of the EPCglobal Network,” Communications of the ACM, v.52 n.7, July 2009.

[10] M. Swanson, N. Bartol, and R. Moorthy, “Piloting Supply Chain Risk Management Practices for Federal Information Systems,” Draft NISTIR 7622. NIST, 2010.

[11] M. Atallah, H. Elmongui, V. Deshpande, and L. Schwarz, "Secure supply-chain protocols," in IEEE International Conference on E-Commerce, pp. 293-302, 2003.

[12] R. Ranchal, and B. Bhargava, “Protecting PLM data throughout their lifecycle,” in 9th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (Qshine), 2013.

[13] M. Azarmi, B. Bhargava, P. Angin, R. Ranchal, N. Ahmed, A. Sinclair, M. Linderman, and L. ben Othmane, “An End-to-End Security Auditing Approach for Service Oriented Architecture,” In 31st IEEE Symposium on Reliable Distributed Systems (SRDS), 2012.

[14] G. Kiczales, J. Lamping, A. Mendhekar, C. Maeda, C. Lopes, J. Loingtier, and J. Irwin, “Aspect-oriented programming,” European Conference on Object-Oriented Programming (ECOOP’97), pp. 220–242, 1997.

[15] L. Othmane, and L. Lilien, “Protecting Privacy in Sensitive Data Dissemination with Active Bundles,” In The 7th Annual Conference on Privacy, Security and Trust, Saint John, NB, Canada, 2009.

[16] L. ben Othmane, “Active bundles for protecting confidentiality of sensitive data throughout their lifecycle,” Theses, Western Michigan University Kalamazoo, MI, USA, December 2010.