Winter 11-4-2009

A Proposed Cross Platform Privacy and Security Framework for Supply Chain Information Sharing

Jerrel Leung

Frank C.H. Tong

Zongwei Luo

A PROPOSED CROSS PLATFORM PRIVACY AND SECURITY FRAMEWORK FOR SUPPLY CHAIN INFORMATION SHARING

Jerrel Leung, Frank C.H. Tong, Zongwei Luo
The Chinese University of Hong Kong,
The University of Hong Kong,
The University of Hong Kong,
jerrelleung@baf.msmail.cuhk.edu.hk，ftong@eti.hku.hkzwluo@eti.hku.hk

Abstract

Information sharing has become eminent to supply chain management, as it allows supply chain partners to collaborate more closely. However, currently supply chain partners are often on disjoint information platforms, which prevent them from effectively sharing critical supply chain information. One of the main barriers of information sharing is revealing confidential information to unintended parties and thus the disclosure of privacy. Therefore the information sharing needs and characteristics of a supply chain has been analyzed and subsequently a cross platform privacy and security framework to allow safe information sharing has been proposed.

Introduction

Supply chain management (SCM) has become a much discussed topic and as believed by many, business does not compete on a product level any more, but business competes and differentiates on a supply chain level [1]. It is inevitable that information sharing is needed for businesses to cooperate and many argue that information sharing is a key ingredient for a successful SCM [2]. The advent of RFID technology takes the information sharing detail level to an even higher level, as it can provide information about the physical product movement on an item level. Basically, RFID allows supply chain partners to integrate the physical flow with the information flow.

There are currently many service platforms to facilitate information sharing between supply chain partners. However, sharing information between these service platforms is not a common practice. There is therefore an urgent need to share information across these disjoined service platforms, as the number of service platforms expand. Privacy and security in its broadest sense is a barrier for companies to share information [3] [4]. In general, the privacy and security are in place for individual service platforms, but there lacks a privacy and security framework for sharing information across platforms. Thus in order to facilitate cross platform information sharing, a privacy and security framework needs to be developed first to lower the barrier of information sharing between supply chain partners.

The objective of this study is to develop a privacy and security framework for cross platform information sharing for supply chain partners. In order to satisfy the supply chain needs, we analyze the information sharing requirements based on the following areas:

- Supply chain information sharing issues and concerns on security and current measures typically in use, and,
- Typical scenarios of supply chain management practices in the context of privacy and security.

The paper is organized as follows: In the next section we provide an overview of information sharing across supply chains, subsequently we present the findings of our case study. Based on the case study, we propose a cross platform privacy and security framework to safeguard confidential information sharing. Moreover, the proposed platform is illustrated by a typical information sharing scenario. Finally, we conclude and give some remarks on our future work.

Literature review

There are currently many platforms available to share supply chain information. Many of the existing platforms focus on parts of information sharing, e.g. EPCglobal, focuses on RFID data and Dell's VMI system focuses on suppliers. However, in order to gain visibility, supply chains partners may need information that reach beyond RFID data and beyond only the suppliers segment. [5][6] for instance described that inventory information sharing across the entire supply chain can lessen the order placing distortion, also known as the Forrester effect and the Bullwhip effect respectively. Therefore supply chains are in need for a platform and cross platform to share information among its supply chain partners.

Information sharing across enterprise boundaries in supply chains involves many issues. In a generic supply chain, there are raw material/parts/semi-finished goods, suppliers, logistics services provider, manufacturers, wholesalers, retailers [7]. Wholesalers or retailers

process purchase orders to suppliers, and logistics services providers will deliver the requested materials to manufacturers and they will deliver the finished goods to wholesalers and then retailers. Back and forth information flow across these parties could sometimes happen on more than one supply chains. For example, a dye manufacturer order raw materials from a vendor, the information flow here impact both a garment brand store's supply chain as well as a painting oil brand store's supply chain. Such multi-parties and multi-supply chain scenario makes the information sharing more complicated, and the privacy issues arises here [8].

Other privacy concerns include specific products' volume, relationship, and contracts, price, manufacturer's customer contacts; the nature of relationship can be viewed as vendor-manufacturer [6], upstream-downstream partners, distribution center-retailer (warehouse charges), and retailer-consumer (CRM) [9][10]. Most privacy-protecting schemes for RFID have focused on the consumer privacy problems. Industrial privacy, i.e. data secrecy and business confidentiality, is important too, but less frequently considered [11].

As aforementioned, supply chains can exist of many different supply chain partners. Usually supply chain partnership is characterized as a buyer-supplier relationship [12]. The supply chain partnership can vary from being fixed e.g. by contracts [13] to being dynamic e.g. ad hoc collaboration [14]. Fixed supply chain partnership has the characteristic of being lasting in which the relationship is clearly defined. Dynamic supply chain partnership on the other hand is ad hoc and can change from transaction to transaction. Therefore, dynamic partnership brings a new element to privacy and security in a supply chain context where it has to adapt to both the established and changing supply chain partnerships.

Methodology

The main objective of this study is to create a privacy and security cross platform information sharing framework for supply chains. However, the current literature lacks examples of how information is shared among supply chain partners and platform. Therefore a case study is used as an illustration of a typical supply chain. This research methodology is well suited for this problem, as it can bring out the problems that arise during information sharing. Moreover, case studies can provide information about a given context and eventually deduce theories from it [15].

Case study

For this study we studied a supply chain for power tools, e.g. power drills. The supply chain consists of a supplier, a manufacturer, a trader, and a retailer. The supplier and the manufacturer are both located in China, where the supplier provides the parts and accessories and where the manufacturer assembles the power tools. A trader, located in Hong Kong, functions as a middle man between the manufacturer and retailer to source, to WPK (warehousing packing kitting), and to ship the products to the retailer. Obviously, the trader does not actually perform the all the activities, e.g. WPK and the shipping. The trader outsources these activities to a 3PL and a carrier respectively. Finally, the retailer, located in the USA, owns several stores and DCs in order to sell the power tools to the consumers.

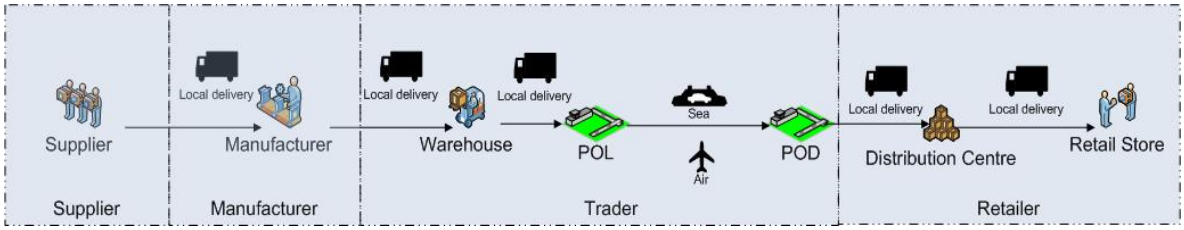

Figure 1. Case - supply chain setting

The power tools supply chain partners are distributed among three platforms, with the manufacturer, trader, DC, and retailer as the main information sharing partners (see Figure 2).

The manufacturer is on a platform called the "manufacturer platform" and on this platform the supplier can share information with the manufacturer, e.g. part delivery tracking information. Therefore the manufacturer can be considered as the data owner and where the supplier only provides information to the manufacturer.

Furthermore, the trader is on a platform called the "trader platform" and where the 3PL and carrier can share information with the trader, e.g. shipping tracking. Trucker A and warehouse X in their turn can share information with the 3PL, e.g. warehouse receipt confirmation, who subsequently can pass

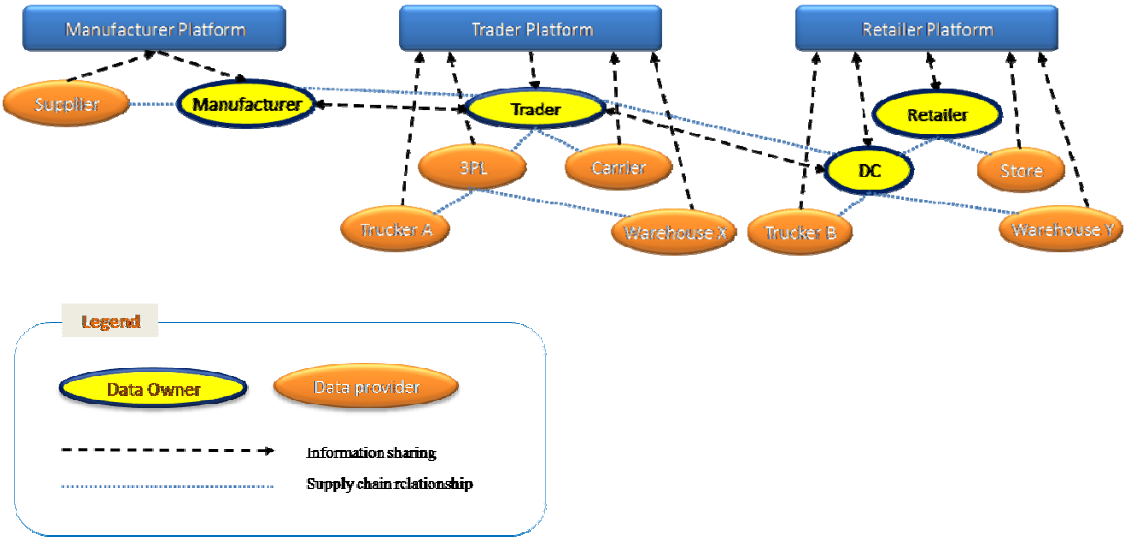

Figure 2. Case - Supply chain information sharing infrastructure

through the data to the trader. Therefore the trader can be considered as the data owner and where the 3PL, carrier, trucker A, and warehouse X only provides information to the trader.

Finally, the DC and the retailer are on the "retailer platform". Store, trucker B and warehouse Y can provide information to the DC and retailer, e.g. inventory status. Therefore the Retailer and DC can be considered as the data owner and where the store, trucker B, and warehouse Y only provides information to the retailer.

Currently, the information sharing between platforms are performed manually, e.g. by email, phone, and fax. The data that needs to be shared is in general already detailed by means of contracts. The depicted supply chain (Figure 2) shows that the supply chain partners already share information within their supply chain segment (platform), but cross platform information sharing is less well established. The information sharing between data owners, and in this case the major supply chain partners, are generally predetermined by contracts, and in some cases by ad hoc project, and can usually be obtained manually. However, there are cases, where for instance warehouse X needs information of the DC. In such case, this information sharing might not be covered by contracts, as they might not even be aware that they are within the same supply chain, and the trial to obtain the particular information can become a dreadful process. First warehouse X needs to contact the 3PL, who needs to contact the trader and who in its turn, contacts the DC for the particular information. Subsequently, the information has to travel the same path backwards to deliver the information to warehouse X.

Cross platform privacy and security framework

We propose the following cross platform privacy and security framework (CPPF), in order to allow supply chain partners seamlessly share information across platforms. The proposed CPPF must have the following in place:

Cross platform environment – There exists a technology that allows us to single uniquely identify (SUI) each item, e.g. similar to EPC code for RFID information and MAC address for computer network cards. Moreover, there exist some form of 3rd party e-service [16] that can discover per SUI request of all platforms that contain information about the SUI. For now we call this service the SUI discovery service (SUI-DS). Some Internet-aware addressing form will be provided as a pointer to the platform containing the SUI data. Let us take the Object Name Service (ONS) of EPCglobal as an example of how this is performed for RFID data [17].

Information portal – Each portal knows three roles 1) Sole Operator (SO), which is the platform itself, e.g. manufacturer platform as described by the aforementioned case study 2) Data Owner (DO), the supply chain partner who owns the data, e.g. manufacturer as described in the aforementioned case study, and 3) 3rd Party

Contributor (3PC), the supply chain partners who act as data providers, e.g. the supplier in the manufacturer platform as described in the aforementioned case study

Data dimension – For the CPPF we categorize the data by their data dimensions, which include location, sensitivity, and ownership. Data can be stored in different locations, e.g. local database, intranet, and Internet, and we assume that information stored on the platform are considered as information that can be shared with selected supply chain partners. Data sensitivity implies that data can be classified according to different sensitivity levels, e.g. high, medium, and low. Where high sensitivity contains item specific data that can reveal "trade secrets" and these data should only be shared with close supply chain partners. While low sensitive data contains generic data and can be shared with less close supply chain partners. Finally, data ownership in this framework includes the roles as described above, namely data owner and third party. The reader is referred to [18][19][20] for further readings about the data dimensions.

Privacy preference – This is the preference of the requested information provider in terms of privacy protection when sharing information [21], meaning what information to share with what type of relationship, e.g. sharing of high sensitive data with "close" supply chain partners and sharing of low sensitive data with indirect supply chain partners. The privacy preference concept is initially developed to collect personal information of any user [22] and in this project we extent the concept

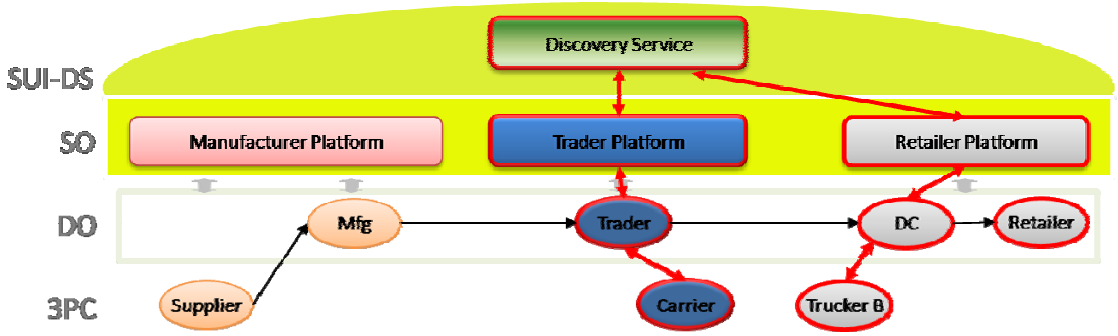

Figure 3. Cross platform privacy and security framework

to a B2B context. Thus each supply chain partner can specify sharing information preference, for different types of supply chain partners. The data sharing is determined based on the privacy preference at the time of data request and therefore can support both fixed and dynamic relationships [21].

Security Scheme – One party is the receiver (of information) and the other party is the sender. The 'send' and 'receive' can actually be implemented by 'grant' and 'access' (the sender granting the access to the receiver, and the receiver accessing the information intended to be shared by the sender). The general practices, such as simple rights as read-only, write-only or read-and-write, are to be adopted along with other more fine grained access control at such the best visibility can be obtained with the maximum protection of privacy.

The general information sharing follows these similar steps:

1. *Data request of a DO* – A request from a DO, the receiver for information is posted to an information portal.
2. *SUI-DS determines data location* – The information portal queries the SUI-DS, and the data location pointers are returned.
3. *SOs matches privacy preference* – The information requesting DO submits its privacy preference, and the information sender DO does the same. Based on an authorization scheme, the characteristics of information sharing are determined.
4. *Exchange of information* – The receiver obtains the information as intended by both parties with privacy and security ensured.

Information sharing across platforms scenario

We will discuss one typical scenario to better explain and illustrate CPPF. In this scenario we portray that the supply chain partners are in a cross platform environment as described by CPPF, trucker B of the retailer platform wants to obtain information of the carrier of the trader platform, e.g. delivery note (DN), as shown in Figure 3 with the thicker lines depicting the information sharing path. Previously, trucker B had to call or fax the trading company to obtain the DN, who in its turn had to obtain it from the carrier operator. However, with CPPF trucker B can access the DN via existing

	Transparent	Translucent	Opaque
Vendor	Manufacturer XYZ 123 street name China	Manufacturer in China	-
ETA	01 January 2010	01 January 2010	-
Quantity	Product A – 50 pieces in 5 cartons Product B – 80 pieces in 4 cartons	9 cartons	-
Gross weight	Product A – 100kg Product B – 80kg	100 – 200 kg	-
Price	Product A - $25/piece Product B - $10/piece	$10 - $ 30 per piece	-

Table 1: Data sensitivity

retailer platform. In order to obtain the DN trucker B must go through the following steps:

1. *Data request of a DO* – Trucker B is a 3PC and in CPPF the SOs only are aware the DOs, as described by the information portal of CPPF. Therefore trucker B sends out a data request to the DC, as the DC is the data owner. The DC in its turn sends out a data request of the specific DN to the retailer platform.
2. *SUI-DS determines data location* – Thus the DC queries the retailer platform for the specific DN on behalf of trucker B. The retailer platform subsequently queries the SUI-DS, and the SUI-DS web service returns a pointer with the platform (trader platform) containing the specific DN.
3. *SOs matches privacy preference* – The DO requester (DC) submits its privacy preference and the DO provider (trader) submits its privacy preference. In our scenario the privacy preference is a fixed relationship, by means of a contract, and the relationship predetermined a security scheme that only a translucent view, see below for an explanation of the translucent view, of DN should be shared to the DC.
4. *Exchange of information* – Since the privacy preference allows a translucent view of the DN to be shared with the DC, the DC receives the translucent view DN information from the trader platform via its own retailer platform and passes the DN to trucker B.

In our scenario we consider that the DN data is stored on the platform and therefore can be shared with supply chain partners. Moreover, we propose three views of the DN (based on the data sensitivity) in our security scheme, namely transparent, translucent, and opaque [23]. In the current practice we usually either completely share the data (transparent) or not share the data at all (opaque). However, this might not be adequate to facilitate the needs of the supply chain and we therefore propose a third view, namely translucent. In the translucent view supply chain partners can share only selected/aggregated data. An illustrative simple version of the DN is shown in Table 1.

The translucent view provides trucker B with adequate information to anticipate and to prepare the transportation of the products, without disclosing sensitive information of the trading company (e.g. manufacturer name and price). With this view we can create a mutual benefit, where trucker B can plan their operations in advance and where the trading company does not have to worry about disclosing sensitive information.

Concluding remarks

In order to facilitate information sharing across entire supply chains, a solution is needed to connect the disjoined platforms. This study addressed the privacy and security issues of this solution. We have proposed a novel information sharing platform to safeguard confidential information shared across platforms. Literature has been reviewed and a case study has been utilized to portray a typical supply chain set up. The framework is designed in such a way that both fixed and dynamic partnership can be facilitated. Moreover, a scenario is developed to illustrate the framework. We believe that this framework can contribute to the development of solutions that can connect disjoined platforms for supply chain integration with proper protection for business confidentiality.

This study is an initial step that allows us to anticipate how cross platform privacy and security can be implemented and what issues it brings. Although CPPF has been demonstrated by the aforementioned scenario, it still lacks an actual implementation. Moreover, CPPF is based on a supply chain configuration and it therefore might not be applicable to all supply chains. However, CPPF is designed to handle both fixed and dynamic partnership and can therefore support many different supply chain partnerships. Moreover, there are still areas in the study that require further investigation to establish a holistic foundation for the privacy and security issues and concerns in CPPF. The following potential further investigation

can be the suggested: Relation based access control method, the data characteristic models, and the privacy preference scheme.

CPPF is actually a part of our study to develop web services methodologies that allow information sharing across platforms. The study will continue to advance and in continuation a prototype will be developed. Technologies such as P3P (Platform for Enterprise Privacy Practices), EPAL (Enterprise Privacy Authorization Language), ISTPA (Internet Security & Trust Privacy Alliance), SAML (Security Assertion Markup Language), and XACML (eXtensible Access Control Markup Language) are currently being evaluated for implementation of the prototype in our study.

Acknowledgement. This research is supported by the R&D funding (ITP/024/07LP) granted from the Hong Kong R&D Centre for Logistics and Supply Chain Management Enabling Technologies.

The authors extend their appreciation to Sung-Chi Chu and Waiman Cheung of the Center of Cyber Logistics, the Chinese University of Hong Kong, for their valuable advice on this research work.

References

[1] Christopher, M. Logistics & Supply Chain Management: Strategies for Reducing Costs and Improving Services, 1st edition, Pitman Publisher, London, 1992.

[2] Moberg, C.R., Cutler, B.D., Gross, A., and Speh, T.W. Identifying Antecedents of Information Within Supply Chains, *International Journal of Physical Distribution and Logistics Management*, 32 (9), 2002, pp 755-770.

[3] Ohkubo, M., Suzuki, K., and Kinoshita, S. RFID Privacy Issues and Technical Challenges, *Communications of ACM*, 48(9), 2005, pp. 66-71.

[4] Garfinkel, S.L., Juels, A., and Pappu, R. RFID Privacy: An Overview of Problems and Proposed Solutions, *IEEE Security and Privacy*, 3(3), 2005, pp. 43-43.

[5] Forrester, J. Industrial Dynamics, MIT Press, Cambridge, MA, 1961.

[6] Lee, H.L., Padmanabhan V., Whang S. Information Distortion in a Supply Chain: The Bullwhip Effect, *Management Science*, 43 (4), 1997, pp. 546-558.

[7] Mentzer, J.T., DeWitt, W., Keebler, J.S., Min, S., Nix, N.W., Smith, C.D., and Zacharia, Z.G. Defining Supply Chain Management, *Journal of Business Logistics*, 22 (2), 2001, pp. 1-25.

[8] Li, Y. and Ding, X. Protecting RFID communications in supply chains, In Proceedings of the 2nd ACM Symposium on information, *Computer and Communications Security*, Singapore, 2007.

[9] Malhotra, N.K., Kim, S.S., and Agarwal, J. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model, *Information Systems Research*, 15 (4), 2004, pp. 336-355.

[10] Maloni, M. and DeWolf, F. Understanding radio frequency identification (RFID) and its impact on the supply chain, Penn State Behrend – RFID Center of Excellence, 2007.

[11] Juels, A. RFID Security and Privacy: A Research Survey, *IEEE Journal on Selected Areas in Communications* 24 (2), 2006, pp. 381-394.

[12] Lamming, R.C., Beyond Partnership: Strategies for Innovation and Lean Supply, Prentence-Hall, Hemel Hempstead, 1993.

[13] Cachon, G.P. and Lariviere, M.A. Contracting to Assure Supply: How to Share Demand Forecast in a Supply Chain, *Management Science*, 47(5), 2001, pp. 629-646.

[14] Wong, C.W.H. Dynamic Partnership in Online Logistics Community: Concepts and Knowledge Framework, Dissertation, Department of DSE, Faculty of Business Administration, The Chinese University of Hong Kong, 2008.

[15] Benbasat, I., David, K., Mead, G., and Mead, M. The Case Research Strategy in Studies of Information Systems, *MIS Quarterly*, 11(3), 1987, pp. 369-386.

[16] Chen, G., Chu, S., and Cheung, W. Third Party e-Service: Conceptualization and Service Architecture, *the International Conference on e-Business and Information System Security*, 2009.

[17] Armenio, F., Barthel H., Burstein, L., Dietrich, P., Duker, J., Garrett, J., Hogan, B., Ryaboy, O., Sarma, S., Schmidt, J., Suen, K.K., Traub, K., and Williams, J., The EPCglobal Architecture Framework, EPCglobal Final Version 1.2, 10 September 2007.

[18] Henderson J.C., Plugging into Strategic Parnerships: the Critical IS Connection, *Sloan Management Review*, 30(3), 1999, pp. 7-18.

[19] Konsysnki, B.R. and McFarlan, F.W. Information Partnerships – Shared Data, Shared Scale, *Harvard Business Review*, 68 (5), 1990, pp. 114-120.

[20] Du, C.T., Wong, M., Cheung, W.M., and Chu, S.C. A Privacy and Security

Framework for the EPC Network Infrastructure, BA Working Paper Series, WP-06-02, The Chinese University of Hong Kong, 2006.

[21] Chu, S.C., Cheung, W., abd Du, T. A Relationship-Based Access Control Model for On-demand Privacy and Security Entitlement in RFID-enabled Supply Chains, *Proceedings of the Eighth Conference on Electronic Business*, 2008, pp. 117-124.

[22] Reagle, J. and Cranor, L., The Platform for Privacy Preferences, Communications of ACM, 42(2), pp. 48-55.

[23] Lamming., R., Caldwell., N., and Harrison, D., Developing the Concept of Transparency for Use in Supply Relationships, *British Journal of Management*, 15(4), 2004, pp. 291-302.