

# **Modeling in Confidentiality and Integrity for a Supply Chain Network**

**Kuo Lane Chen**

School of Accountancy and Information Systems  
University of Southern Mississippi

**Marn-Ling Shing**

Early Child Education Department and Institute of Child Development  
Taipei Municipal University of Education, Taiwan

**Huei Lee**

Department of Computer Information Systems  
Eastern Michigan University

**Chen-Chi Shing**

Information Technology Department  
Radford University

## **ABSTRACT**

Bell-LaPadula Model and Markov Chain Model are used for supply chain networks in the previous literature. However, Bell-LaPadula Model only considers the confidentiality aspect of security. Markov Chain Model is used to simulate the dynamics of the security states. In a typical supply chain network, the integrity of business transactions should be as important as confidentiality of those transactions. The purpose of this paper is to apply Clark-Wilson model to the supply chain network integrity. The major concepts of the Clark-Wilson model such as separation of duty, constrained data items, well-formed transactions, and transform procedures are applied to different situations of a supply chain network.

## **INTRODUCTION**

A supply chain is a sequence of processes that take place between customers, manufacturers/distributors and suppliers (Chopra & Meindl, 2006). Narrow definition of supply chain network, or suppliers relationship management (SRM) is limited to the management of relationship between suppliers and manufacturers (or retail-chain distributors). The broader definition of a supply chain network includes all the parties from customers to suppliers. Therefore, it further includes customer relationship management (CRM), warehousing, production, and product design. Most textbooks use the broader definition for supply chain management. Today most large manufacturers such as General Motor or retail-chain distributors such as Wal-Mart are in the form of supply chain networks.

One of the major goals of supply chain management is to minimize the total system costs from customers to suppliers so it can attract and retain customers in a competitive environment. Another major goal of supply chain management is to achieve the efficiency of supply chain network so it can meet the philosophy of just-in-time manufacturing/delivery. The efficiency of a supply chain network is relied on the success of the supply information network software system and IT infrastructure. A broader supply chain network system includes Enterprise Resources Planning (ERP) and Customer Relationship Management (CRM) systems. The Intranet or extranet are examples for IT infrastructure for the supply chain network. Another important issue of a supply chain network is the security of the information system. In a supply chain network, most suppliers may have conflict of interests so the integrity and confidentiality of the information is important in a supply chain network.

Chen et. al. (2006) proposed the application of Bell-LaPadula model in the design of a supply chain network. In the Bell-LaPadula model a subject has a security clearance and an object has a security classification. The goal of the Bell-LaPadula security model is to prevent “read” access to objects at a security classification higher than the subject’s clearance (Bishop, 2003). However, the Bell-LaPadula Model only considers the confidentiality aspect of security. In a typical supply chain network, the integrity of business transactions should be as important as confidentiality of those transactions.

The Clark-Wilson model is one of the security models for information integrity for a business environment. This paper attempts to model the security on a supply chain network using the Clark-Wilson Model by applying the major concepts such as separation of duty and transformation procedures (TP) in different supply chain situations.

## **LITERATURE REVIEW**

### **Information Security**

The word “information” is defined as “Knowledge obtained from investigation, study, or instruction; Intelligence, News; Facts, Data” (Merriam-Webster Online, 2006). And the word “security” is defined as “measures taken to guard against espionage or sabotage, crime, attack, or escape”. Therefore, after combine these two definitions, information security can be defined as “measures, for which knowledge obtained from investigation, study, or instruction; intelligence, news taken to guard against espionage or sabotage, crime, attack, or escape”. More specifically, information security is defined in an NIST document as “protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability” (NIST, 2002). In the same document “integrity” is defined as guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. The word “confidentiality” means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. In addition, the word “availability” means ensuring timely and reliable access to and use of information. In other words, information security are “measures adopted to prevent the unauthorized use, misuse, modification, or denial of use of knowledge, facts, data, or capabilities” (Maiwaid, 2004).

In the design of a secured supply network, there are many different models in providing policies for different aspects of the information security. For example, Bell-LaPadula Model has been used in military and is originally designed for modeling confidentiality in information security (Bishop, 2003). Bibba model uses subject and objectives theories from the Bell-LaPadula Model to provide security policy on data integrity. Bell-LaPadula model represents sensitivity levels of information in terms of a set of security clearances. The more sensitive the information is, the higher the security clearance is. The security clearance of a subject can be in one of the levels: top security, security, confidential, and unclassified. In the mean time, an object also has a security classification. A subject is only allowed to read the objects at a security levels not higher than the subject’s security clearance. Every subject must belong to a unique security clearance level. And every object must also belong to a unique classification level. For example, a CEO, who is in a “Top Security” security clearance, can read the personnel files. Whereas, a custodian, who is in a “unclassified” security clearance, can read the telephone lists. The CEO can also read the telephone lists; however, the custodian cannot read the personnel files. In the following section, we review the applications of Bell-LaPadula Model in supply chain networks discussed in Chen et. al. (2006).

### **The Bell-LaPadula Model for Supply Chain Networks**

Several papers discussed the information security in a supply chain network (Dynes, et. al., 2006). Chen et. al. (2006) proposed to use the Bell-LaPadula model for a supply chain network. Also mentioned by Shing et. al. (2006), the price offered by suppliers in a supply network should be confidential due to competition. In fact, the confidentiality of most suppliers’ information is essential in today’s competitive business world. In order to design the security infrastructure in a supply chain network, Chen et. al. (2006) suggested the use of the Bell-LaPadula model.

According to the Bell-LaPadula model, Chen et. al. (2006) classified the employees (subjects) in the buyer’s company into several security clearances and different documents (or objects) into some security classification

levels. For simplicity, assuming there are two security clearances for all employees in a buyer’s company. They are managers and employees. The managers can access (read) two documents: supplier evaluation and buying decision. On the other hand, employees can only access (read) two documents: public bidding notice and public retail price list. The managers can also access the documents which employees can access. However, employees cannot access the following documents: supplier evaluation and buying decision.

Figure 1 shows the relationship between a purchasing company and their suppliers. Parties involved include: 1) managers in the purchasing company, 2) employees in the purchasing company, and 3) different suppliers. Since a supplier and other suppliers may be in competition position, certain documents from this supplier to the purchasing company cannot be read by other suppliers. Also, certain documents cannot be read by other employees in the purchasing company but these documents can be read by managers in the purchasing company. Table 2 shows security classifications and clearance levels for a purchasing company and its suppliers (Chen et. al., 2006).

Figure 1: A purchasing company and its suppliers. (Chen, et. al., 2006)

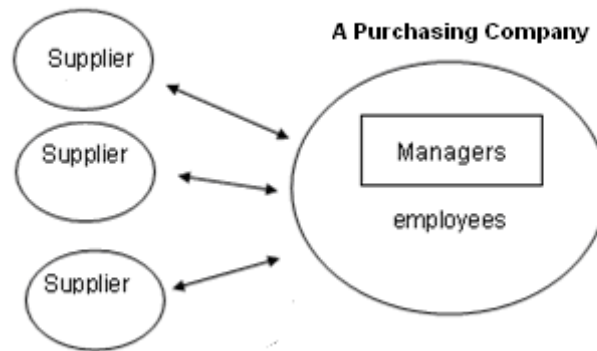


Table 2: Security classification in a supply chain network. (Chen, et. al., 2006)

Security Classification	Purchasing Company Personnel and Their Suppliers
Top Secret (TS)	Managers in the purchasing company
Secret (S)	Other employees in the purchasing company
Confidential (C)	An individual supplier
Unclassified (UC)	All the suppliers

**The Markov Chain Model for Supply Chain Networks**

Shing et.al. (2006) proposed the use of the Markov Chain Model for a supply chain network. Given a set of random variables  $\{X(t), t \geq 0\}$  indexed by the time parameter  $t$  (all possible values of  $t$  form the parameter space  $T$ ). The process  $X(t)$  is a stochastic process. The values  $X(t)$  are called states. Consider time points  $t_0 < t_1 < t_2 < \dots < t_n < t$ . A Markov process is a stochastic process  $\{X(t), t \in T\}$  if

$$P[X(t) \leq x \mid X(t_n)=x_n, X(t_{n-1})=x_{n-1}, \dots, X(t_0)=x_0] = P[X(t) \leq x \mid X(t_n)=x_n]$$

That is, a Markov process is a stochastic process that the probability of the process at a state depends only on the previous state, not on the previous history of getting to the previous state. If the states are discrete and the stochastic process has a discrete parameter space, then it is called a Markov chain  $\{X_n, n=0, 1, 2, \dots\}$ . In other words, a

stochastic process  $\{X_n\}$  is a Markov chain if at any  $k$  time points  $n_1 > n_2 > \dots > n_k$ , there are  $k$  corresponding states  $i_1, i_2, \dots, i_k$ , the probability that the process is at state  $j$  at time  $n$ , given that the process was at state  $i_1$  at time  $n_1$  and  $\dots$ , the process was at state  $n_k$  at time  $i_k$  is equal to the probability that the process is at state  $j$  at time  $n$ , given that the process was at state  $i_1$  at time  $n_1$ . That is,

$P(X_n=j | X_{n_1}=i_1, \dots, X_{n_k}=i_k) = P(X_n=j | X_{n_1}=i_1)$ , where  $i_j$  is the state of the processes at time  $n_j$  ( $n_k \leq i_j \leq n_1$ ) [1]. This says that the probability that the Markov chain is in state  $j$  at  $n$ , depends only that the Markov chain was in state  $n_1$  at  $i_1$ . This is the transition probability  $P_{i_1,j}^{n_1,n}$  from state  $i_1$  to the state  $j$ . If  $P_{i_1,j}^{n_1,n}$  depends only on the time difference  $n - n_1$ , then the Markov chain is time-homogeneous. For a time-homogeneous Markov chain,  $P_{i,j}^{n+1,n} = P_{i,j}^{m+1,m}$ , this is called one-step transition probability. It is denoted by  $P_{ij} = P(X_{m+1}=j | X_m=i)$ .

For a time-homogeneous Markov chain, at time 0 the probability that the system is in one of states  $\{1, 2, \dots, m\}$  is represented by  $q(0)$ , the state vector at time 0,

$$q(0) = \begin{bmatrix} p_1(0) \\ p_2(0) \\ \dots \\ p_m(0) \end{bmatrix}, \quad \sum_{i=1}^m p_i(0) = 1 \quad (1)$$

where  $p_i(0)$  represents the probability of the system is in state  $i$  at time 0. Then the probability that the system is in one of those  $m$  states at time 1 is represented by  $q(1)$ , the state vector at time 1,

$$q(1) = \begin{bmatrix} p_1(1) \\ p_2(1) \\ \dots \\ p_m(1) \end{bmatrix}, \quad \sum_{i=1}^m p_i(1) = 1 \quad (2)$$

where  $p_i(1)$  represents the probability of the system is in state  $i$  at time 1. And

$$q(1) = Q q(0), \quad (3)$$

where  $P$  is the one-step transition probability matrix,

$$Q = \begin{bmatrix} p_{11} & p_{21} & \dots & p_{m1} \\ p_{12} & p_{22} & \dots & p_{m2} \\ \dots & \dots & \dots & \dots \\ p_{1m} & p_{2m} & \dots & p_{mm} \end{bmatrix}, \quad \sum_{j=1}^m p_{ij} = 1, \quad (4)$$

for  $i=1,2,\dots,m$ , and  $p_{ij}$  is the probability of the system in the state  $j$ , given it was in the state  $i$ . The probability that the system is in one of those  $m$  states at time  $s$  is represented by  $q(s)$ , the state vector at time  $s$ ,

$$q(s) = \begin{bmatrix} p_1(s) \\ p_2(s) \\ \dots \\ p_m(s) \end{bmatrix}$$

where  $p_i(s)$  represents the probability of the system is in state  $i$  at time  $s$ . And

$$q(s) = Q(Q(\dots(Q q(0))))=Q^s q(0), \tag{5}$$

where  $Q$  is the transition probability matrix, By combining the subjects and objects possible security levels, we can list all possible states as states in the Markov chain model. After identify the starting state vector at time 0,  $q(0)$  in (1), and the one-step probability transition matrix  $Q$  in (4), the state vector at the next time 1,  $q(1)$  in (2) can be obtained straightforward by (3). The state vector at time  $s$ ,  $q(s)$ , can be directly calculated by (5). (Shing et.al., 2006).

**CLARK-WILSON MODEL IN THE SUPPLY CHAIN NETWORK**

Purchasing is a key activity of the supply chain management. In order to keep the cost down, a purchasing company tends to send out the request for quotation for a group of potential suppliers. The purchasing company will choose a supplier with the best combination of price and quality. Sometimes a potential supplier will try to collect the information about other suppliers so it can provide the best bid to the purchasing company. Since most transactions involved will go through a computer-based network system such as Extranet or Internet, the data integrity and confidentiality becomes very important between suppliers and the purchasing company.

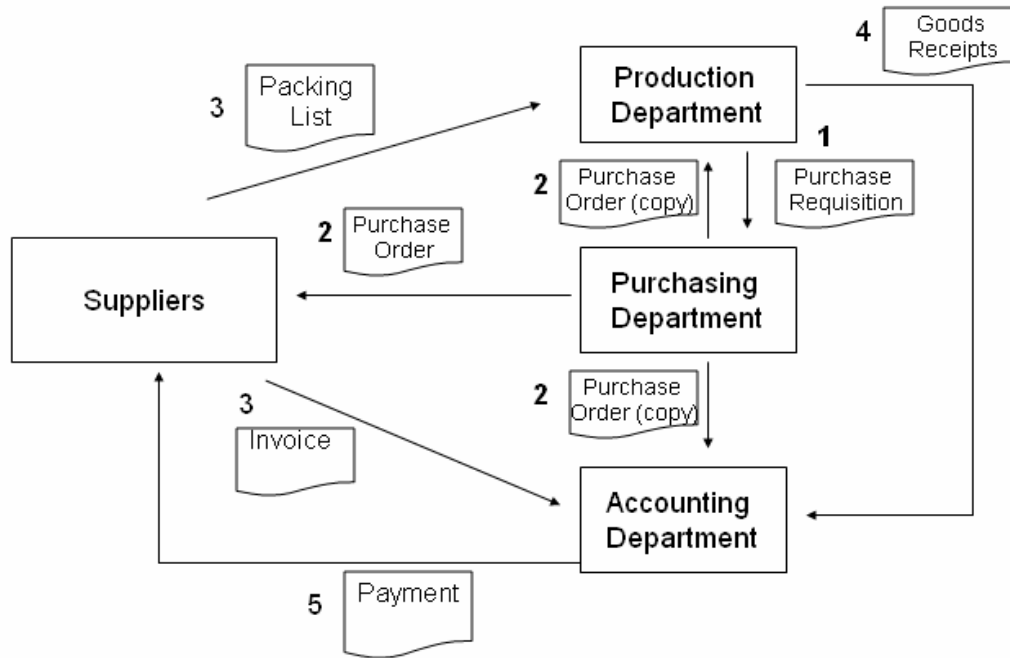
Clark-Wilson Model is designed for a commercial environment (Bishop, 2003). The Clark-Wilson model uses three important concepts: separation of duty, constrained data items, and well-formed transactions (Javvin Technologies, Inc.). Separation of duty means that no single person should perform a task alone. A task should be done by two or more people or monitored by another person to prevent the fraud. The Clark-Wilson models divided all the data into two categories: Constrained Data Items (CDI) and Unconstrained Data Items (UDI). Unconstrained data items do not need to be protected while constrained data items are protected by Integrity Verification Procedure (IVP). Well-formed transaction means that a user has to use the data under certain constrains and cannot change data as they want. Blake (2000) used an example to explain how the Clark-Wilson model is applied to a typical purchasing process. We make a slight revision to his example as follows:

1. The production department needs a component and submits an acquisition request to the purchasing department and the accounting department.
2. Purchasing department creates a purchase order for the component and sends copies to several suppliers, the receiving department, and the accounting department.
3. Upon receiving the components, the production department checks the delivery and make sure that the quality and quantity meet the specifications, signs a goods receipt (the term used by SAP R/3 software). Goods receipt goes to the accounting dept.

4. The supplier sends an *invoice* to the accounting department. Accounting department compares the invoice with the purchase order and the goods receipt. If there is no problem, the accounting department issues an electronic payment or check to the supplier.

The process is shown on Figure 2.

Figure 2: Purchasing process in a supply chain networks.



As mentioned by Blake, "... Data items are changed only by transformation procedures, thereby maintaining their integrity." Because the separation of duty, a simple purchasing task is divided to: production department, purchasing department, suppliers, and accounting department. The constrained data items are the purchase order, packing list, goods receipts, invoice and electronic payment (or check). "Each department may only invoke some transformation procedures, and a pre-specified set of data objects or CDIs" (Ge, et. al., 2004). The transformation procedures (TP) are sending purchasing requisition, creating purchase order, sending purchase order, sending goods and goods receipt, signing goods receipt form, creating invoice, sending invoice, comparing invoice to order, and so on (Ge, et. al., 2004).

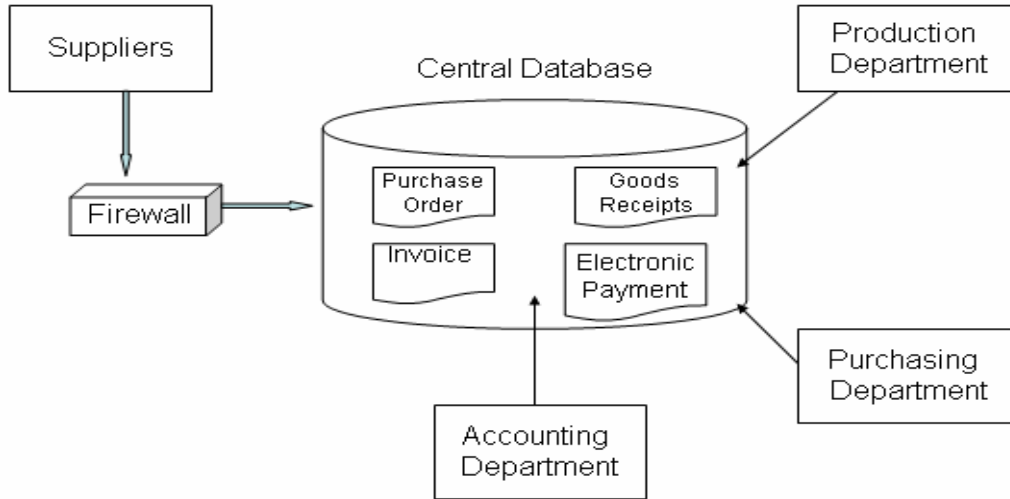
Today most SCM systems such as SAP R/3 and SAP APO use a central database. It means all the data and forms are actually stored in a physical database as Figure 3 (See next page).

In such a case, possible security leaking loophole can happen. For example,

1. The clerk in the accounting department can access all the three documents: the purchasing order, the invoice, and the goods receipt. In principal, he can read these documents but he cannot modify these documents except the electronic payment. However, he is in the internal position and may be very familiar with other department's conditions. Normally, the production department only concerns about whether they receive the components. A bad clerk can hack into the systems and revise all document in a small amount, (i.e. change from \$1000.00 to \$1050.00)

and send a payment \$1000.00 to the supplier and sends \$50.00 into a dummy account which eventually will go to his pocket. In the above situation, the separate of duty and TP will make this kind of situations hard to happen.

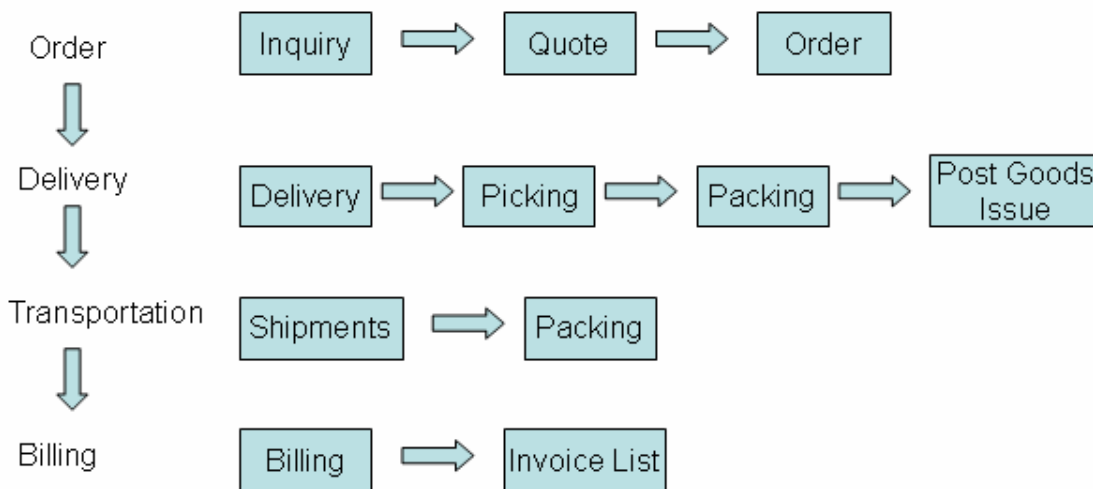
Figure 3: A computerized supply chain network system.



2. Another supplier can hack into the computer systems and increases the amount in purchase order in the step 2 and the transaction may not happen in the step 3 because of misunderstanding.

One of the most popular SCM software is SAP R/3. Figure 4 shows the transformation procedure used by SAP. SAP uses “document principle” which means a transform process is associated with a physical document or electronic document.

Figure 4: Transformation procedures for purchasing in the SAP software. (Source: SAP handouts, 2003)



## CONCLUSIONS

In conclusion, the integrity for the supply chain networks can be modeled by Clark-Wilson model. It is important for an SCM software package to incorporate the security features to the design the supply chain network. One of the problems is the trade-off between the security features and user-friendliness of the software. Transform procedure (TP) is good method to prevent possible fraud but it makes the computer systems more complex or bureaucrat. Future research may focus on the number of minimum TPs is needed for maintaining the integrity level.

## REFERENCES

- Bhat, N. (1972). *Elements of Applied Stochastic Processes*, John Wiley & Sons, New York, NY.
- Bishop, M., (2003). *Computer Security: Art and Science*. Addison-Wesley, Boston, MA.
- Blake, S. Q. (2000). The Clark-Wilson Security Model. Retrieved May 2007, from <http://www.lib.iup.edu/comscisec/SANSpapers/blake.htm>
- Chen, K.L., Lee, H. and Yang, J.(2006). Security Considerations on the Design of Supply Chain Networks. *Proceedings of the Southwest Decision Sciences Institute (SWDSI)*, 14(1/2/3).
- Chopra, S. and Meindl, P. (2006). *Supply Chain Management*. 3<sup>rd</sup> ed.. Prentice Hall: Upper Saddle River, New Jersey.
- Dynes, S., Brechbühl H., Johnson, M.E. Information Security in the Extended Enterprise: Some Initial Results From a Field Study of an Industrial Firm. Retrieved May 2007, from <http://infoecon.net/workshop/pdf/51.pdf#search='information%20security%20in%20supply%20chain>
- Ge, X., Polack, F., & Laleau, R.(2004). Secure Databases: An Analysis of Clark-Wilson Model in a Database Environment, *Advanced Information Systems Engineering - 16th International Conference, CAiSE 2004*, Riga, Latvia, June 2004, Persson A., Stirna J. (Eds.), LNCS, 3084 , 234-247.
- Javvin Technologies, Inc. Information, Computer and Network Security Terms Glossary and Dictionary, Retrieved May 2007, from <http://www.javvin.com/networksecurity/ClarkWilsonModel.html>
- Maiwald, E. (2004). *Fundamentals of Network Security*. McGraw Hill: Burr Ridge, IL.
- Merriam-Webster Online (2006). Retrieved May 2007, from <http://www.m-w.com/dictionary/information>
- NIST (2002). Retrieved May 2007, from <http://csrc.nist.gov/policies/FISMA-final.pdf>.
- SAP (2003), SAP Training Handouts.
- Shing, M., Shing, C., Chen, K., and Lee, H. (2006). Security Modeling on the Supply Chain Networks. *Proceedings of EIST 2006*, Orlando, FL.