Supply Chain Security Using RSA Algorithm

A Theoretical Frame Work

Efosa Aiguokhian
Master’s Thesis

___.___.______ ________________________________

Valitse kohde.

SAVONIA UNIVERSITY OF APPLIED SCIENCES **THESIS**

Abstract

Field of Study Technology, Communication and Transportation			
Degree Programme Master’s Degree Programme in Industrial Management			
Author(s) Aiguokhian Efosa			
Title of Thesis Supply Chain Security Using RSA Algorithm			
Date	24.1.2013	Pages/Appendices	53
Supervisor(s) Jukka Kinnunen			
Client Organisation/Partners Savonia University of Applied Sciences			

Abstract

The success of supply chain depends greatly on how its information technology is used. Over the years the rate at which supply chain sensitive information is sent over the internet and network has increased drastically. It is for this reason that every company wants to ensure that its supply chain information is secured because large volume of sensitive information is sent over the internet on daily basis. This has created room for this information to be properly secure so that unauthorized user cannot gain access to such sensitive information. There is need for supply chain information to be transmitted via the internet and computer networks to be protected. The integrity of supply chain information can be secured by using appropriate data security technology.

The aims of this thesis were to focus on supply chain security and how supply chain information sent through the computer network and internet can be secured using RSA technique. The thesis elucidates on the limitations of RSA algorithm and how these limitations can be overcome.

The methods used in this thesis are information derived from secondary source materials made up of journal articles, conference proceedings, textbooks and good websites source. In this thesis, it was showed that supply chain security powered with RSA techniques was very important in supply chain management. In conclusion, 2048 bits or more bits RSA are recommended for better supply chain security.

Keywords: RSA, RSA Algorithm, Supply Chain, Supply Chain Security

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala
Tekniikan ja liikenteen ala

Koulutusohjelma
Maisterin koulutusohjelma Industrial Management

Työn tekijä(t)
Aiguokhian Efosa

Työn nimi
Supply Chain Security RSA algoritmi

Päiväys	24.1.2013	Sivumäärä/Liitteet	53

Ohjaaja(t)

Jukka Kinnunen

Toimeksiantaja/Yhteistyökumppani(t)
Savonia-ammattikorkeakoulu

Tiivistelmä

Toimitusketjun menestys riippuu suurelta osin siitä, että miten sen tietotekniikkaa käytetään. Vuosien varrella toimitusketjun nopeus, millä arkaluontoiset tiedot lähetetään Internetin ja verkon välityksellä, ovat kasvaneet rajusti. Tämän vuoksi jokainen yritys haluaa varmistaa, että toimitusketjun tiedot ovat suojattuja, koska suuri määrä arkaluontoisia tietoja lähetetään Internetin välityksellä päivittäin. Tämä on luonut tilaa tiedon asianmukaiselle suojaukselle, niin että luvattomat käyttäjät eivät pääse käsiksi arkaluontoisiin tietoihin. Toimitusketjulle on tarvetta, jotta tietoja voidaan lähettää turvatun Internetin ja tietoverkon välityksellä. Tietoketjun eheyden vuoksi, tietoja voidaan turvata käyttämällä asianmukaista tietoturvateknologiaa.

Tämän työn tavoitteena oli keskittyä toimitusketjun turvallisuuteen ja mitenkä tietoverkon ja Internetin välityksellä lähetetyt toimitusketjun tiedot voidaan turvata käyttämällä RSA:a tekniikkaa. Työssä selvennetään RSA-algoritmin rajoituksia ja miten nämä rajoitukset voidaan voittaa.

Työssä käytettävät menetelmät on saatu toissijaisista lähtöaineistoista, jotka koostuvat lehtiartikkeleista, konferenssijulkaisuista, oppikirjoista ja hyvistä sivulähteistä. Tässä työssä osoitettiin, että toimitusketjun turvallisuutta tehostettiin RSA tekniikoilla ja se oli hyvin tärkeä toimitusketjun hallinnan kannalta. Lopuksi, 2048 bittiä tai suurempi määrä bittejä RSA:ssa suositellaan käytettäväksi, jos halutaan parantaa turvallisuutta toimitusketjussa.

Avainsanat: RSA, RSA-algoritmin, Supply Chain, Toimitusketjun Turvallisuuden

Glossary and Abbreviations

AEO EU Authorized Economic Operator; it is a program that was formed to make sure a safer and more protected end-to-end supply chain entering or leaving the European Union (EU).

ASIS American Society for Industrial Security; it is devoted to rising the efficiency and productivity of security professionals.

CBP Customs and Border Protection; it is formed to secures the homeland by preventing the illegal entrance of people and goods. It promotes legitimate travel and trade.

CCC Customs Cooperation Council; it is set up to enhance the efficiency and effectiveness of customs administrations worldwide.

CIOs Chief Information Officers; it is a job title normally given to the most senior executive in an enterprise in charge of information technology.

CRT Chinese Remainder Theorem; it give a remainders by dividing a given number *n* by some given divisors.

CSCMP Council of Supply Chain Management Professionals; it is the leading global association of professionals in supply chain management.

CSI Container Security Initiative; it is international initiative that defends global trade.

C-TPAT Customs Trade Partnership against Terrorism; it is supply chain security initiative.

E-Supply Chain Electronic Supply Chain; it is supply chain that is technology enable and is based on electronic linkages and structurally.

GAO Government Accountability Office; it is an investigative section of congress responsible taking care issues relating to the receipt and payment of public funds.

GPS Global Positioning System; it is a navigation and accurate positioning tool.

GSCF Global Supply Chain Forum; it discuss and debate issues relating to supply chain issues

ICT Information and Communication Technology

ISPS International Ship and Port Facility Security; it is a complete set of measures to promote the protection of ships and port facilities

ISO/PAS 28000 International Organization for Standardization; it is formed to enhance the growth of standardization and related activities in the world.

IT Information Technology

NSCCA	Nested Supply Chain Cryptographic System; it is cryptographic system for supply chains.
PET	Privacy Enhancing Technologies; it is intended to raise awareness of the concept of privacy enhancing technologies.
PGP	Pretty Good Privacy i.e. Email Security
PWC	Pricewaterhouse-Coopers; It is a worldwide professional services firm with headquartered located in London, United Kingdom.
RFID	Radio-Frequency Identification Technology; it is a tracking system that uses clever bar codes to track goods.
RSA	Ron Rivest, Adi Shamir and Len Adleman; they are the inventor of RSA cryptosystem.
SILC	Secure Internet Live Conferencing; it is a network protocol intended to offer uninterrupted security for conferencing services.
SCM	Supply Chain Management
SSH	Secure Shell; it is a cryptographic network protocol for secure data communication.
SSL	Secure Sockets Layer; it is frequently used protocol for organizing the security of a message transmission on the Internet.
TLS	Transport Layer Security; it is a protocol that ensures privacy between communicating applications and their users on the Internet.
TWIRL	The Weizmann Institute Relation Locator; it is an electronic device for large integer’s factorization.
TQM	Total Quality Management; it is an integrated effort by organizational designed to enhance quality.
VPN	Virtual Private Networks; it uses public network to creates a secure network connection.
WCO	World Customs Organization; It ensures better international trade and security.
WMD	Weapons of Mass Destruction; it is a weapon that can take life and bring major harm to a great number of people.

CONTENTS

1 Introduction

The aim of every company is to ensure that its supply chain information is secured because large volume of sensitive information is sent over the internet on daily basis. The success of supply chain depends greatly on how its information technology was been used. The rate at which supply chain sensitive information is sent over the internet and network have increased drastically over the years. This has created room for sensitive information to be properly secured so that unauthorized user cannot gain access to such information. Supply chain is a combination of organizations, people, technology, information, activities and resources involved in providing goods and services from supplier to consumer. The activities in supply chain involve how raw materials can be transformed into finished products to satisfy the end customer's requirements. There is need for the supply chain sensitive information to be transmitted via the internet and computer networks during the provision of goods and services to consumers. Importantly, supply chain information needs to be secured against online criminals, terrorist and hackers that can cause significant negative economic effects that will jeopardize the effectiveness of supply chain. In this study, the integrity of supply chain information can be secured by using the appropriate data security technology.

The aim of this thesis is to focus on supply chain security and how organization can secure its supply chain information sent through the computer network and internet using RSA technique. The thesis also talks about the limitations of RSA algorithm and how these limitations can be overcome.

The method used in this thesis is in the form of literature review. The source of information in this thesis is secondary source materials and it is made up of journal articles, conference proceedings, textbooks and good website sources.

2.1 Supply Chain Management

The origin of the term supply chain management (SCM) was introduced by a consultant Keith Oliver in 1982. In the late 1990s, the term was used by many operations managers with increasing regularity (Jacoby 2009, Blanchard 2010). The meaning of SCM has been re-conceptualized from integrating logistics across the supply chain and to the current understanding of integrating and managing main business processes across the supply chain (Cooper *et al.* 1997). In 1998, the difference between the definitions of SCM and logistics was modified by the Council of Logistic Management (CLM). The modified definition clearly demonstrated that logistics management is only a component of SCM (Lambert and Cooper 2000). In spite of the popularity of the term SCM, there has been considerable misunderstanding as to its meaning both in academia and practice (Mentzer *et al*. 2001). Some authors define SCM in operational terms involving the flow of materials and products, some view it as a management philosophy, and some view it in terms of a management process (Tyndall *et al.* 1998). The definitions of SCM differ across authors and they can be classified into three categories; a management philosophy, implementation of a management philosophy, and a set of management processes (Mentzer *et al.* 2001).

The definitions of SCM by different authors are described below. The Global Supply Chain Forum (GSCF) defined SCM as the integration of key business processes from end user through original suppliers. The original suppliers provide products, services, and information that add value for customers and other stakeholders (Lambert et al, 1998). According to the forum website, SCM is not a business function rather new business model necessary for an organization's success and everyone in the organization needs to be involved (www.scm-institute.org). The Council of Supply Chain Management Professionals (CSCMP) also defines SCM as encompasses the planning and management of all activities involved in sourcing and procurement, conversion, and all logistics management activities. Importantly, it also includes coordination and collaboration with channel partners, which can be suppliers, intermediaries, third party service providers, and customers.

Also, SCM integrates supply and demand management within and across companies (www.cscmp.org). The processes that are involved in fulfilling the needs of the end customers are known as supply chain and typical supply chain includes the following chain; distributors, producers, vendors, and final consumers (Luong and Phien, 2007). SCM is a network of organizations that are involved, through upstream and downstream linkages, in different processes and activities that produce value in the form of products and services in the hands of the ultimate consumer (Christopher 1992). SCM is defined as the life cycle processes comprising physical, information, financial and knowledge flows whose purpose is to satisfy end-user requirements with products and services from multiple linked suppliers (Ayers 2001). SCM deals with the total flow of materials from suppliers through end users (Jones and Riley 1985). SCM is an integrative philosophy to manage the total flow of a distribution channel from supplier to the ultimate user (Cooper et al 1997). Supply chain model with all kinds of flows is depicted in figure 1.

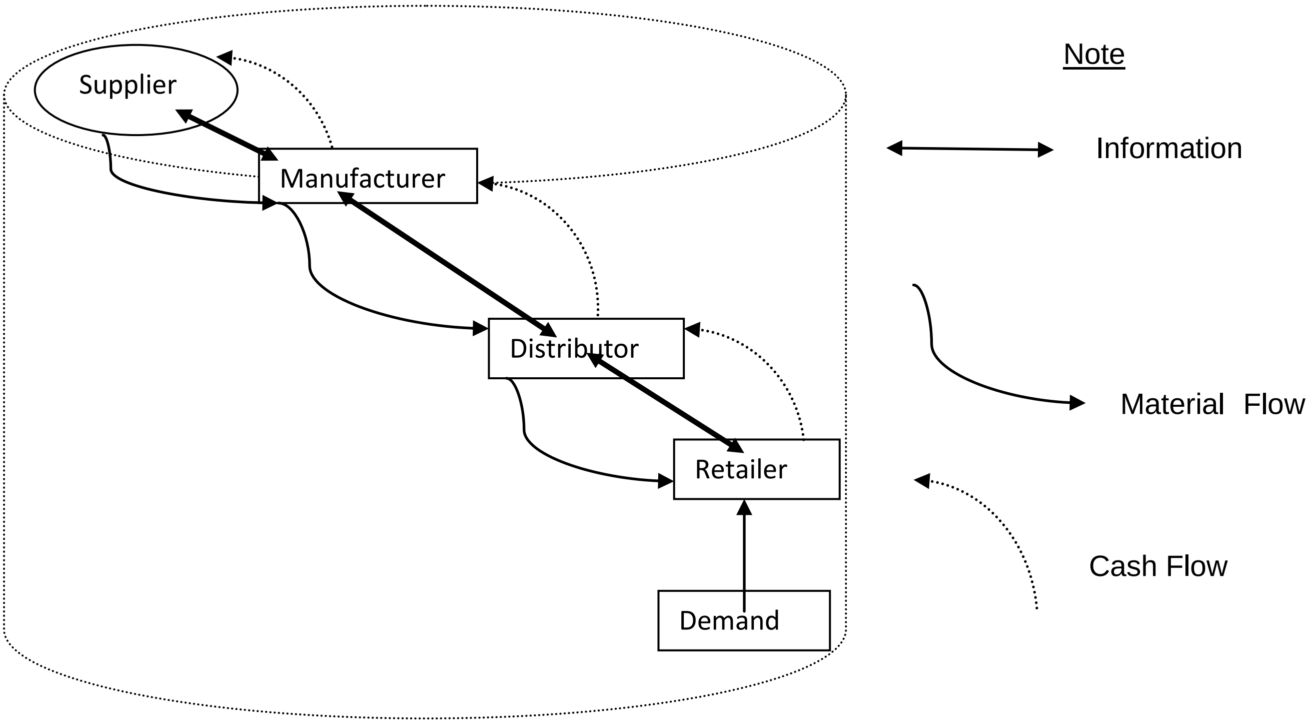


Figure 1 Supply Chain Model containing all flow types (Wadhwa et al 2009.)

2.2 Importance of Supply Chain Management

Supply Chain Management is the vital backbone of modern organization through effective marketing, availability of goods and services that meet the needs of the consumers. The success of many business organizations depends on revenue realized from effectiveness supply chain strategies. The importances of supply chain management to the society and business environment are shown in figure 2.

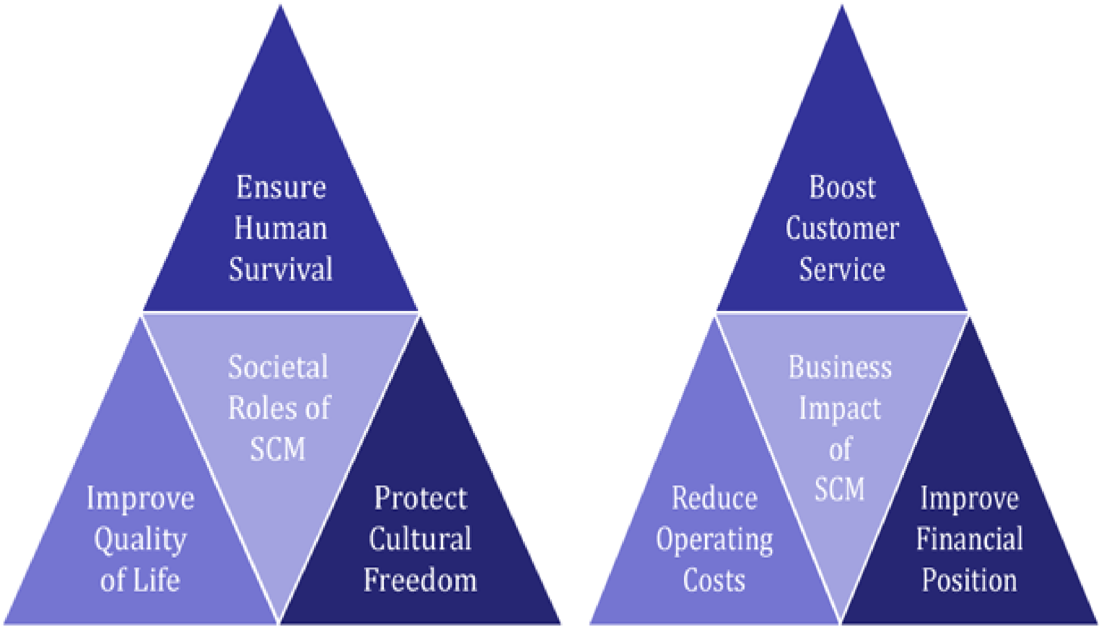


Figure 2 The importance of supply chain management to the society and business environment (Council of Supply Chain Management professional 2011 (www.cscmp.org))

SCM plays a significant role in both societal and business survival to ensure effective well-being of the consumer as well as manufacturers.

2.2.1 SCM and the Society

The SCM ensures human survival which includes protection of human health from extreme climatic conditions such as environmental pollution. It also serves as foundation for economic growth and providing energy. Finally, it protects cultural freedom and development this includes protects of delivery necessities and defends human freedom.

2.2.2 SCM and Business Environment

SCM and business environment boost customer service. It includes right stock location, right delivery time and right products assortments and quantity. Also, improve financial position in an organization. These increased profit leverage of the business organization, increased cash flow and decreased fixed assets of the firm. It reduces operation costs by decreasing purchasing cost and production cost of the firm and decreasing the total supply chain cost.

2.3 Problems of Supply Chain Management

The concept of SCM is associated with some problems such as lack of empirical evidence supporting the benefits attributed to SCM (Lambert *et al*. 2005; Stock *et al*, 2010); unavailability of a universally accepted definition of SCM which leads to difficulty in research and practice (Mentzer *et al.* 2001). Also, it has been found out that SCM field lacks universally accepted frameworks and little attention has been given to its implementation and measurement (Lambert *et al,* 1998; Mentzer, 2004). There is the argument that operationalizing supply chain in practice is difficult (Lockamy and McCormack 2004). The problem of tradition and culture also influenced supply chain enterprise management systems. Also, another problem which may affect SCM is that of sharing information through internet and other networks.

2.4 Security and Privacy Needs

The wide range of business transactions taking place in the internet have created room for worldwide internet based architecture for facilitating the exchange of supply chain information in international supply chain networks (Weber 2009). Privacy is the ability to concealed supply chain information and also how this information must be used. The Privacy Enhancing Technologies (PET) has developed information privacy goals for the fulfilment of customer privacy requirements. This technology uses Virtual Private Networks (VPN) and Transport Layer Security (TLS) (Fabian *et al.* 2009). According to Supply Chain Security Guidelines 2003, information security assures that information is protected against the exchange, loss, introduction of erroneous information.

3 Supply Chain Security

Supply chain security can be described as the process which involves application of programs, procedures, technology as well as people to prevent threats to the information. The security also enhances protection of economic state of the society, social and physical well-being of humans.
ISO/PAS 28000:2005 specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. Specification for security management systems for the supply chain by the International Standards Organization (ISO); the development of the Framework of Standards to Secure and Facilitate Global Trade by members of the World Customs Organization(WCO). The avoidance of Excess in Global Supply Chain Security Policy (2009) “has raised concerns about supply chain security overdue”. According to Chen *et al*. (2006), information sharing in supply chain management is a key element and it is significant in improving performance and enhancing competitive advantage of supply chain in an organization. Many organizations are reluctant when it comes to sharing supply chain information due to fact that such information might leak due to lack of security.

Furthermore, following terrorist attacks in recent years, for example the terrorist attacks on September 11, 2001 on the US Nation; closer analysis reveals that a recent series of security breaches and disruptions that threaten her national security. In October 2002 U.S. west coast longshoremen’s lockout, utility failures in the U.S. and Europe in 2003. The Madrid bombing and the tsunami in 2004 all explain the inherent vulnerability that exists in global supply chains, and the global scope and scale of impact (Rice *et al*. 2005). Supply chain security is defined as “The application of policies, procedures, and technology to protect supply chain assets (product, facilities, equipment, information, and personnel) from theft, damage, or terrorism and to prevent the introduction or unauthorized contraband, people or weapons of mass destruction (WMD) into the supply chain” (Closs and McGarrell (2004). The definition above view supply chain security from both physical and information thefts.

An illustration of Layered Security is shown in figure 3 and example of Points of Vulnerability is depicted in figure 4.

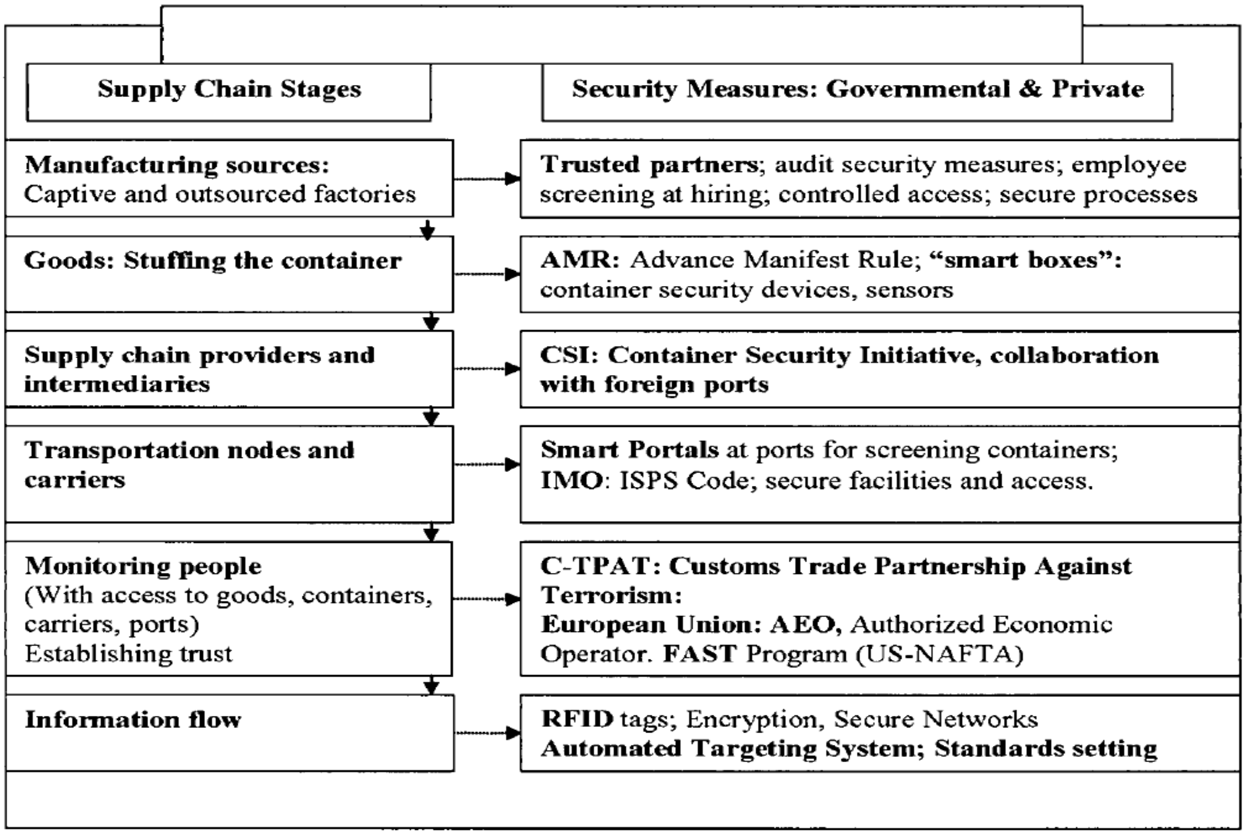

Supply Chain Stages
Security Measures: Governmental & Private
Manufacturing sources: Captive and outsourced factories
Trusted partners; audit security measures; employee screening at hiring; controlled access; secure processes
Goods: Stuffing the container
AMR: Advance Manifest Rule; "smart boxes": container security devices, sensors
Supply chain providers and intermediaries
CSI: Container Security Initiative, collaboration with foreign ports
Transportation nodes and carriers
Smart Portals at ports for screening containers; IMO: ISPS Code; secure facilities and access.
Monitoring people (With access to goods, containers, carriers, ports) Establishing trust
C-TPAT: Customs Trade Partnership Against Terrorism: European Union: AEO, Authorized Economic Operator. FAST Program (US-NAFTA)
Information flow
RFID tags; Encryption, Secure Networks Automated Targeting System; Standards setting

Figure 3 Layered Security (adapted from RAVI SARATHY. (2009))

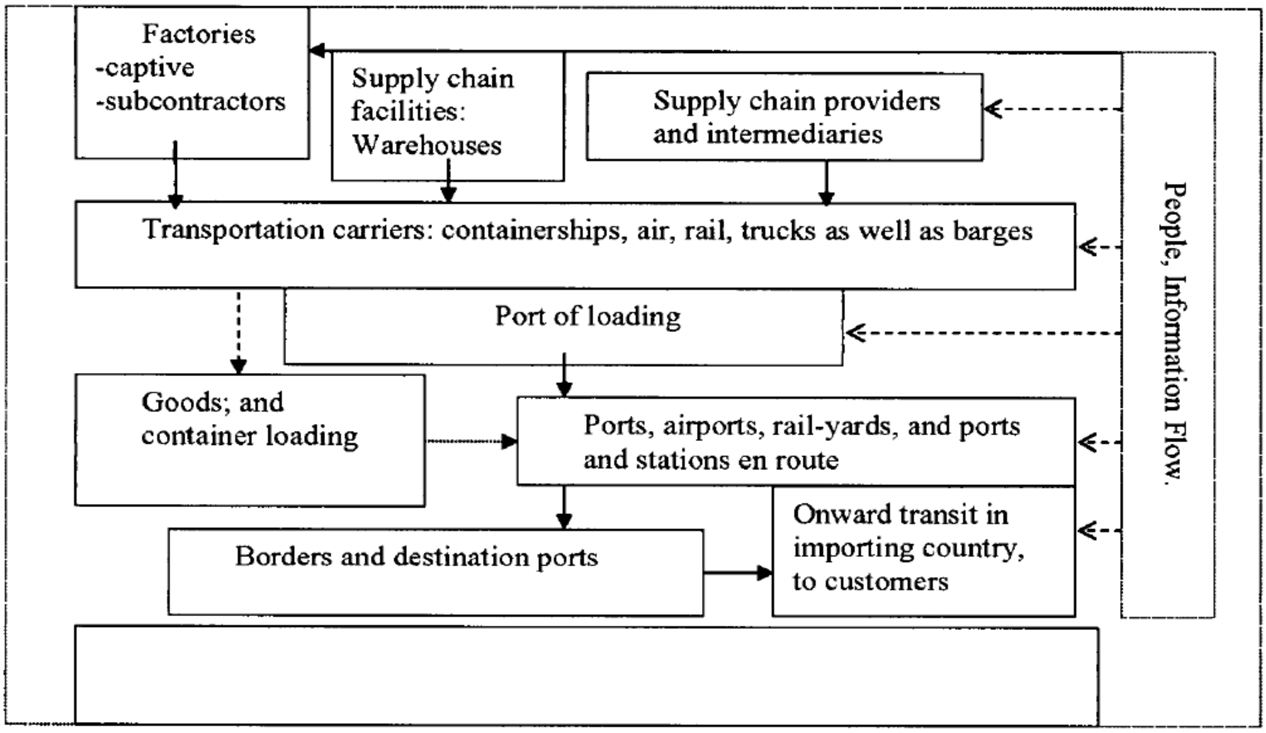

Factories
-captive
-subcontractors
Supply chain facilities: Warehouses
Supply chain providers and intermediaries
Transportation carriers: containerships, air, rail, trucks as well as barges
Port of loading
Goods; and container loading
Ports, airports, rail-yards, and ports and stations en route
Onward transit in importing country, to customers
Borders and destination ports
People, Information Flow.

Figure 4 Points of Vulnerability (RAVI SARATHY. (2009)

The detection of WMD inside containers is also a reason that facilitates better supply chain security (O'Hanlon 2002, Gerencser et al. 2002). They estimate that WMD explosion can lead to port closure and could cost $1 trillion. In addition, the undetonated WMD can lead to a twelve day port closure and could also cost $58 billion (O'Hanlon 2002, Gerencser et al. 2002). According to Society for Industrial Security and Pricewaterhouse-Coopers (ASIS/PWC) joint survey 1999, reported that over five billion dollars are lost by 1000 companies round the world due to theft.

The survey came out with the following findings:

- 45 percent said that they had experienced a financial loss as because of information loss, theft, or misappropriation.
- The responding companies reported, in average, 2.45 incidents with an approximate cost of $500,000 for each incident.
- The number of reported incidents had risen over the last seventeen months.

The threats to supply chain came from both inside and outside the supply chain (Juhel 2009).

3.1 Supply Chain Security Programs

Some initiatives all over the world are put in place to address the issues of supply chain security. These initiatives are:

1. The Customs Trade Partnership against Terrorism (C-TPAT). It is a voluntary program that enables companies to enhance the security of their corporate supply chains. The program originally started in 2001 and it was led by the Customs and Border Protection (CBP) of the USA. The aim of this program is to protect and enhance the security of private companies supply chains. According to Secretary of the Department of Homeland Security Michael Chertoff, the program started with initially seven participants in 2001. In 2005, there were more than 9000 companies participating in the program. Today, there are over 10,000 participating members of the program which is a great success.

2. The World Customs Organization (WCO). It is formally known as the Customs Cooperation Council (CCC) operating since 1952. It ensures that better international trade and security are provided.

3. The Container Security Initiative (CSI). It focuses on container screening at the ports of foreign countries.

4. The World Customs Organization (WCO). It focuses on a lot of areas and supply chain security is one of them.

5. The International Ship and Port Facility Security Code (ISPS Code).

6. The International Organization for Standardization: ISO/PAS 28000 is a standard for security management for both private and public supply chains.

7. EU Authorized Economic Operator (AEO) (2008). The main objective of AEO is to improve the security of the supply chain.

8. World Customs Organization SAFE Framework of Standards (2005). It is a standards designed to secure and facilitate global trade.

9. Tracking and monitoring the integrity of cargo being shipped using RFID and GPS technologies is a pilot initiative by private companies all over the world.

3.2 Supply Chain Information Security

In this thesis, it is concentrated on supply chain information security. Global supply chains are exposed to diverse types of risks that rise along with increasing globalization and the E-supply chains will be more vulnerable from information security (IS) aspect among other types of supply chains (Bolhari, 2009). E-Supply chain is defined as “the supply chain that is built via electronic linkages and structurally based on technology-enabled relationships” (Williams et al 2002). Poirier and Bauer (2000) define E-supply chain as an automatic information flow in supply chain is due to regular improvements in the supply chain. Importantly, the internet has the ability to transfer large amount of information accurately and with high speed (Elliman and Orange 2000). The role of the

Internet help in building commercially feasible supply chains so that the challenges posed by virtual enterprises will be overcome (Graham and Hardaker 2000). The quality needed in supply chain framework ensured that IT on quality management impact measured were designed (Ang *et al.* 2000)). Few literatures wrote about IT in supply chain management and IT is needed to achieve effective supply chain (Gunasekaran and Ngai, 2003). There is the need for companies to invest huge amount of capital to ensure that technical processes and internal organization are redesigned to achieve IT-enabled supply chain (Motwani *et al.* 2000). The e-businesses applications integrated with physical processes are necessary for achieving effective SCM (Van Hooft and Stegwee, 2001). The overall principle for IT-enabled redesign of supply chains was proposed by Christiaanse and Kumar (2000). The buyer-supplier interfaces in inter-organizational processes have being affected by the use of electronic commerce (McIvor *et al*. 2000). The implication of e-commerce for managing supply chain and also how effective is this e-commerce on supply chain management (Murillo 2001). Several downstream effects are needed for security to interrupt supply chain. Proven security technologies can satisfy the core needs around data security and integrity, especially authentication of trading partners, control of access to sensitive data between trading relationships, and encryption of data in transmission (VeriSign 2005). Information security as the process of ensuring that physical security like proper network security management system is also given adequate concern and protecting properties from outsiders must not be given full concern (Canavan 2001).

3.3 IT Supply Chain Risks

Some supply chain models at all levels of complexities and risks that both suppliers and receiver encounter in the supply chain needs adequate attention (Cachon 2003). Some propose methods from the finance domain to risk management within supply chain exist. A lot of risks to information systems have been introduced due to over reliance on global supply chain. In system development life cycle, supply chain threats posed problems to every phase of the development cycle (Datta *et* *al* 2007). The following factors are the important threats that can affect global supply chain according to GAO 2012:

1. Installation of hardware or software containing malicious logic, which is hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose;

2. Installation of counterfeit hardware or software, which is hardware or software containing non-genuine component parts or code;

3. Failure or disruption in the production or distribution of critical products resulting from manmade or natural causes;

4. Reliance on a malicious or unqualified service provider for the performance of technical services; and

5. Installation of hardware or software that contains unintentional vulnerabilities such as defects in code that can be exploited.

The above threats if not properly handled can allow attackers to gain access to systems and carry out operation like input, delete and modification of sensitive data and also allowing the attackers cause denial of service remotely. The access to system can make the IT systems less reliable as well as affecting the materials that are required for system development. There are vulnerabilities that lead to exploit in IT systems. The use of unsecure storage and delivery method, the application of updates and software patches that are not tested, entry into IT services agreement with suppliers without properly monitoring their past record, and the acquisition of IT products from companies different from the original manufacturer are vulnerabilities that could cause exploitation. The IT supply chain security risks can be address as follows:

1. To ensure that policy that protect against supply chain threats must be put in place.

2. To ensure that security measures in the policy developed must be implemented

3. To ensure that supply chain security measures are working.

Security is a focal point of the supply chain and also participants involved in the supply chain must devise strategies to ensure that their supply chain security is updated (Banomyong 2005). The cost for supply chain security modification cost about $65 billion in U.S. (Russell and SaIdanha 2003). They advised that firms need to develop intimate partnerships with supply chain members and with government so that supply chain security issues will be tackled effectively. The greater vulnerability that cause disruption can be created when there is an overemphasis on efficiency characterized by one way sourcing reduced slack, buffer stock and poor inventories (Hendricks and Singhal 2005). Security and terrorism related risk can be traced to some purposeful agents and this can cause disruption to normal flow (Mitroff and Alpaslan 2003). The vulnerability map must be adopted in every company, and the map must contain threats that are likely to occur and the consequences of such threats that have a high degree of occurrence with very high degree consequences (Sheffi and Rice 2005). Attentions must also be given on Total Quality Management (TQM) in supply chain risk mitigation especially risks that come from security (Lee and Whang (2005)). There is the need of security concern on how to guard against hackers. Hackers are trying everyday to hack, change, and delete information store in Radio-frequency identification (RFID) (Juels 2005, Weis 2003).

4 Information Security and Network Security

4.1 Information Security

More attention is given to technical issues than soft issues like security awareness and hazards caused by end users (Katz, 2005). Information security (IS) awareness is the process whereby the security mission of an organization is given proper awareness (Siponen, 2000). IS security awareness is very important to organizations information security (Straub and Welke 1998). Recent studies show that staff errors are threats to information assets and they are rated among the top threats in organizations (Whitman and Mattord, 2005). IT staff must be made aware of the imperative need to ensure that information security is enforced in an organization (Pfleeger and Pfleeger, 2003). Consequently, a single abuse to organization information system can be more expensive that designing a security system (Czernowalow, 2005). IS is now being use in integral business operation (Conner and Coviello, 2004).

The privacy laws can be affected because different countries of the world have different privacy laws. This means that the use of politics and individual privacy varies from country to country (Sarathy and Robertson 2003). There will likely be an increase in multilateral cooperative methods for security issues to management in response to terrorism (Fratiann and Kang 2004). The unauthorized intrusion and hacking of active RFID tags that can be reused and rewritten must be protected (Weis 2003; Juels 2005). When container's get to the final destination, for security reason, tag can be completely read, the tag data analyzed and stored or archived, and the tag deactivated so that it can be re-used (Kearney 2004). A large investment is need in a multiyear container life that supports an active tag system (Molar 2004). Several security proposals have been outlines to fight against security weaknesses, these includes;

1. Reducing right to the use of RFID tags through hash locks.
2. Making use of cost effective hash functions (Weis (2003)).

Furthermore, a supply chain is said to be robust if it has the ability to sustain supply chain operations during main disruptions. It also ensures that there is decrease in costs, increase in consumer satisfaction and consumer relations must be ensure during regular supply chain operations (Tang 2006). Supply chain vulnerability and robustness can be measured using matrices needed by firms (Trent and Monczka 2005). Still, models that examine all aspects of the tradeoff between risk mitigation were outlined and costs (Lee and Whang 2005).The connection between different security measures and cost savings, using a queuing model and incorporating inspection and transit lead time, and estimating safety stock levels required based on product demand estimates and replenishment time (Lee and Whang (2005)). The steps that focus on real time operations management and enhancing strategic sourcing, supply base reconfiguration, and finally developing risk management strategies that is needed by enterprises (Elkins et al. (2005)). The supply chain security can be compartmentalizes into distinct stages and they are listed below according to Sheffi (2001);

1. Preparation to guard against disruptions;
2. The occurrence of a disruptive event;
3. The immediate or first response to the disruptive event;
4. The initial impact of the disruption, gradually escalating till the full impact is felt, over a longer period of time;
5. The preparations for recovery; and
6. The final recovery to resume normal operations.

Security issues can lead to risk in supply chain contract with insurance availability and premiums charged (Rosetti and Choi 2005). The offshore manufacturing decisions, outsourcing, and choice of modes of entry decisions can influence security considerations (Lu 2004). However, global supply chain is short-term costs and long-term benefits must be continually assessed by firms in order to enhance security (Sodhi 2003).

4.2 Network Security

The measures that various companies' take to ensure that their computer system is protected from unauthorized access are known as network security. According to dictionary.com, network security is defined as "the protection of a computer network and its services from unauthorized modification, destruction, or disclosure". PC magazine also define network security as "The authorization of access to data in a network, which is controlled by the network administrator which assigned an ID and password to the user that allows them access to information and programs within their authority". Every organization must be very concerned about this if they use computers and computer network. Network security is not only all about security; it deals with business, people and people problems.

4.2.1 Network Security Policy

According to hp.com, network security policy is policy that has been defined to ensured that the network is protected if properly follow. The hp.com defined steps on how network security policy can be implemented. The policy when properly defined and understand can bring about security reality in an organization. The following steps help us to define and understood network security;

1. Understand it; it defined how network security policy and security measures and can be implemented.
2. Plan it; it has to do with how data, network and internet can be accessed and managed in the organization.
3. Do it; there are a lot of security policy templates available. Examples are the Internet DMZ Equipment Policy, the Router Security Policy, and the Server Security Policy.
4. Use it; it has to do with finding out how the security policy can implement i.e. configuring the hardware and software.

5. Buy it; the appropriate products that are needed for the security policy implementation must be bought.

4.2.2 The Importance of Network Security

The computer network security is crucial to every organization (Canavan 2001) because it helps organization;

1. To protect company assets
2. To gain a competitive advantages
3. To comply with regulatory requirements and fiduciary responsibilities and
4. To keep your job (Security failure sometime can lead to company close down)

The basic idea of network security is explained using the security trinity (Canavan, 2001). The security trinity is the foundation that all organization security policies are based. The security trinity is shown in figure 5.

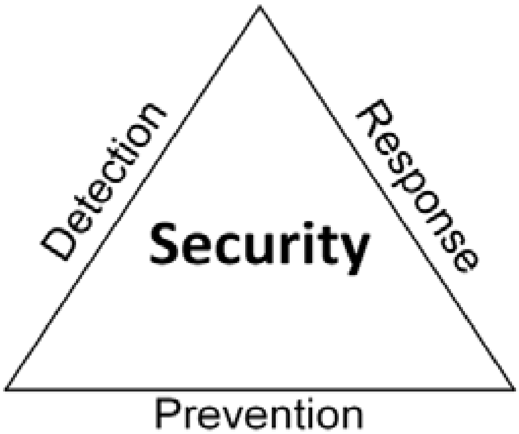


Figure 5; Security Trinity (Bolhari A. 2009)

Prevention

It requires implementing security measures to protect and prevent vulnerabilities i.e. unauthorized adjustment, deletion, and disclosure either accidentally or intentionally. It is in the prevention phase that security policies, controls, process require for the prevention process are developed and implemented. Security breach prevention is economical and easier to prevent than to detect and response to security attach.

Detection

It ensures that appropriate procedures are established to detect potential vulnerabilities in the network. Once preventative measures are applied, procedures need to be established to detect potential vulnerabilities or security breaches; in the event preventative measures not succeed. The sooner a problem is detected the easier it is to correct and cleanup.

Response

In every organization, a map should be created to ensure that security breach is identified and attended to. It is advisable for the map to be in writing indicating various actions and those that are responsible for it.

5 Cryptography

The process of ensuring secure communication in the present of third parties is called cryptography (Rivest 1990). The secrecy of given information can be achieve through the process of known as encryption. With encryption technology, only authorized recipient can read messages. Anyone other than the authorized recipient cannot intercept or read the message. An encryption algorithm is used to secure data transported over public network. Also, clear text is an unencrypted text and plaintext is the text that is inputted into encryption algorithm. So many encryption algorithms exist; some are more secured that the other. Keys distribution is the biggest problem to cryptography. The output of an encryption algorithm that is unreadable is called the cipher text. Decryption on the other hand is the process of reversing the transformation of the encryption transformation. A cryptographic system or a cryptosystem is form from encryption, decryption algorithm, messages format description and keys (Wenbo Mao 2003). Figure 6 below explains how the processes of encryption and decryption are performing in a simple manner.

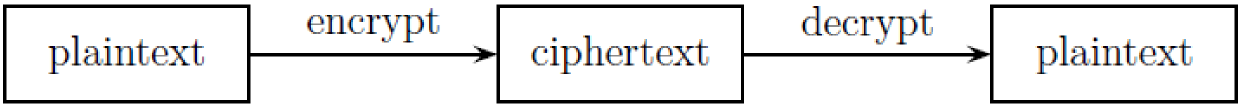


Figure 6: A schema for encryption and decryption (adapted from Minh Van Nguyen, 2008)

5.1 Types of Cryptography

There are two types of cryptography and they are private key cryptography also known as symmetric cryptosystem, and public key cryptography also known as asymmetric cryptosystem. The private key cryptography uses the same keys for encryption as well as decryption. Public key cryptography uses two keys, one key for encryption and the other key for decryption. (Wenbo Mao 2003)

There are some security requirement required in any application to application communication, they are:

Authentication; It is process of ensuring that you are who you prove you i.e. proving one identity. There two primary form of authentication in the internet which is host to host and they are:

1. Name based
2. Address based

Confidentially; it ensures that only the receiver can read the received message.

Integrity; it assured the receivers that the messages received remain unchanged.

Non repudiation; it is a mechanism that assure the sender that the message was sent.

6 Supply Chain and Information Flow

An organized information flow in a business organization contributes to an effective supply chain. Information sharing and collaboration with trading partners is seen as organization's top logistic challenge according to a poll of Supply & Demand Chain Executive's readers (Supply & Demand Chain Executive, 2005). High levels of inventory can be achieved by good information flow in supply chain (Christopher 2005). The inter-firm information flow is an important factor of supply chain management (Chen and Paulraj 2005, Carr and Kaynak 2007). The responsiveness to customer demand, and overall customer satisfaction, cannot be achieved without proper management of both the goods movement and information flow throughout the supply chain (Janak 1996). The flow of information between supply chain members is recognized to be a strategic activity that enhances supply chain performance (Wamba and Boeck 2008). A high level of information flow integration is considered to be a key determinant of a firm's efficiency within a given supply chain (Wamba and Boeck 2008).

The integration of information flow in a given supply chain involves many activities such as the sharing of information about production, inventory level, delivery, shipment, capacity, sales and performance within firms and between supply chain members (Patnayakuni and Rai 2002). Moreover, four types of information are shared among supply chain members: (i) order information (e.g. order quantities and prices), (ii) operation information (e.g. inventory levels), (iii) strategic information (e.g. point-of-sale (POS) information), and (iv) strategic and competition information (e.g. demand information regarding a competitor's products) (Li and Lin 2006). The flow of materials, manpower, money and capital equipment are made possible with effective information flow in the supply chain. The management of information flow in supply chain is very important for every organization. Managing information flows is the key to effective supply chain integration (Sweensey 2006).

6.1 Types of flow in Supply Chain

There are different type flows required in supply chain. According to Forrester (1958), it established a specific link between corporate success and the interactions between five flow systems. These flows include information, materials, money, manpower, and capital equipment. The management of these material (products and services), money and information flows is illustrated below;

Product flow; Is the flow of material (products and services) from the source of materials forward (or upstream) to the end customers in the external chain. It is an important aspect of SCM, which ensure that the right goods and services are available at the right time to the final consumers.

Information flow; Information flows in the supply chain are bidirectional. The effective information flow in SCM helps to prevent the effect of bullwhip. Forrester (1958) reported that, bullwhip effect referred to as the product of poor information management in the supply chain and that leads to excessive inventory levels. According to Christopher (2005) it was stated that good information effectively becomes a substitute for high levels of inventory. An example of product flow and information flow is depicted in figure 7 below.

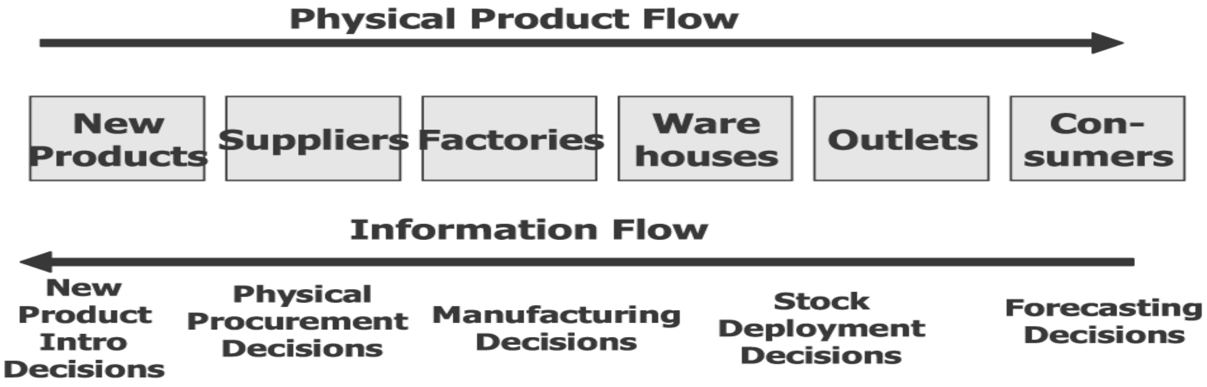


Figure 7 An example of product flow and information flow (Susan (2005))

Money flow; It flows from the final consumer of the product back down through the chain in the supply chain. The time of flows is very important in ensuring that supply chain organization meets up their ongoing operational expenditure commitments. Keown *et. al*. (2004) provides a useful diagrammatic representation of money flows in a supply chain shown in figure 8 below.

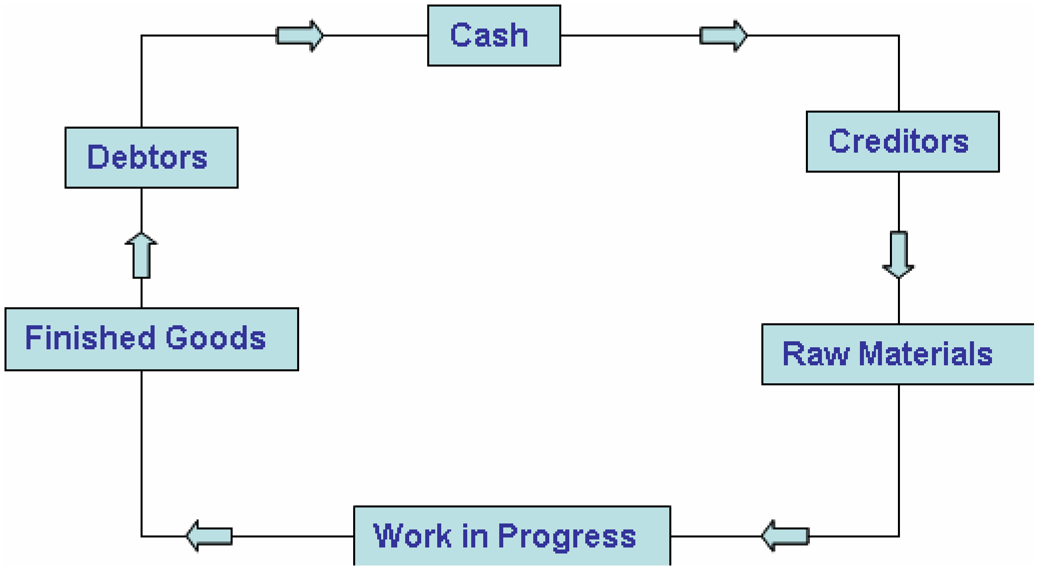


Figure 8: An example of money flow in supply chain (Keown *et. al*. (2004))

6.2 Managing Information Flow in a Construction Company

The construction industry has always been affected with difficulties in sharing information among its participating members. The construction industry is a complex information field, with information being produced, transferred, and analyzed throughout the design and construction process (Haas *et al.* 2000). The time sensitivity and accuracy of this information are critical to successful completion of a project (Haas *et al*. 2000). Due to dispersed projects undertaken by a construction firms, effective information flows among project teams for a firm is very important in implementing quality assurance (Jaggar *et al.*, 2001). Information management has been a key factor affecting the effective implementation of the ISO 9000 standards (Cipriano, 1995). The ISO 9000 is a quality management standards and they are designed to assist organizations make sure that customers wants are satisfied. The introduction of ISO 9000 in 1987, the number of organizations certified under the scheme has drastically increased all over the world (Zheng *et al.* 2007). Examples of construction information are contracts, drawings, specifications, requests for information, change orders, transmittals, cost reports, crew time reports, daily reports, safety logs, injury reports, pay request, and material invoices (Haas *et al.* 2000). Also, in construction industry, contractors have to collect much external and internal information as input for quality management. Information flow up through and authority is expected to flow down through an organization chart (Haas *et al.* 2000). Recently, majority of construction companies have introduced computers into the job-site office. The use of computers have eased the complexity in handling information exchange process in construction companies and also contributed in the creation of more reliable information. An example of information flow chart is shown in figure 9.

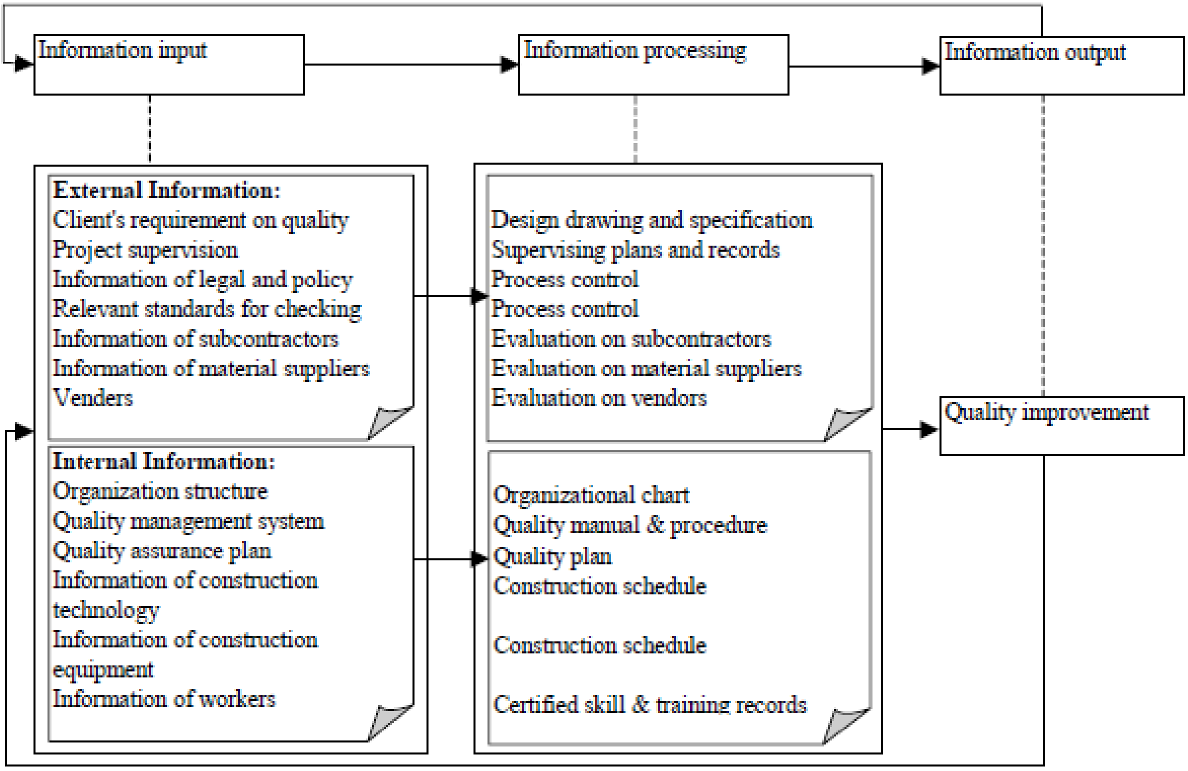

Information input
Information processing
Information output
External Information:
Client's requirement on quality
Project supervision
Information of legal and policy
Relevant standards for checking
Information of subcontractors
Information of material suppliers
Venders
Internal Information:
Organization structure
Quality management system
Quality assurance plan
Information of construction technology
Information of construction equipment
Information of workers
Design drawing and specification
Supervising plans and records
Process control
Process control
Evaluation on subcontractors
Evaluation on material suppliers
Evaluation on vendors
Organizational chart
Quality manual & procedure
Quality plan
Construction schedule
Construction schedule
Certified skill & training records
Quality improvement

Figure 9: Information flow chart (Zheng *et al* (2007))

6.3 The Problems of Information Flow in Construction Company

In an industry, there are unequal information sharing exists between contractor, subcontractors and suppliers. The presences of barrier in an information flow can lead to poor quality management in Construction Company. The most critical risk in supply chain is information flow risk. The risk associated with information flow greatly affects inventory behavior cash flow variations (Tsai, 2008). There are four types of barrier in an information flow.

Organization barrier; these are barriers as a results of organizational structures of the industries involved in the construction projects. These includes horizontal communication barrier, multiple level structure, align the numerous unrelated processes across various supply chain and complexities in program of activities.

Technical barrier; these are barriers as a results of technical attributes of information in a construction projects. These include hardware and software, information security, lack of information cooperation system and different application project.

Financial barriers; it involved high cost of implementing and maintaining IT powered supply chain.

Behavioral barrier; it is unwilling to share information with one another, lack of incentives mechanisms and unnecessary liabilities.

6.4 Privacy and Security in Supply Chain Information Flow

Electronic Privacy Information Center compartmentalized privacy into four groups (www.epic.org). They are:

Information privacy; it have to do with the various ways data is handled in organization.

Body privacy; it is the protection of ourselves against invasive measures.

Communication privacy; it is the privacy of messages sent over the internet and telephones.

Territorial privacy; It deals with the restrictions on invasions into an environment.

The lack of appropriate information security technology can lead to consumer privacy compromised. Privacy standard, legal and regulatory on information privacy and security vary from country to country. The toughest privacy and data protection law in the world is practiced by the European Union. Industry must not involve in any fraudulent act that will compromised consumer privacy (Garfinkel 2002). Also, stakeholders must promote privacy guideline in order to avoid mistake in supply chain information flow privacy. E-service personalization and customization can effectively reduce the risks of customer privacy and security. Privacy and security can affect the way consumers control situations online which can lead to better e-service quality (Zeithaml *et al.* 2000).

6.5 Information Security and Supply Chain Information Flow

Information is important to supply chain processes because good direct line of sight is needed by supply chain manager to manage supply chain processes. Information flows ensure that products are delivered on time, in right quantity and also to meet customer's specification. IT is the key to successful supply chain information flow. Also, increase information accuracy, diffusion, complexity, proliferation and velocity are possible by IT in supply chain (Yogesh 2000). Effective supply chain management is achieved by accurate and timely information delivery with the help of networked computer, mobile phones, laptops computer and other information delivery devices (Yogesh 2000). Recent years IT has positively contributed to rapid developments used to facilitate SCM. McDonnell *et al.* (2004) proposed taxonomy of supply chain IT solutions which identifies four primary categories as follows:

1. Point solutions: used to support the execution of one link (or point) in the chain (e.g. warehouse management systems or WMS);

2. ‘Best of breed’ solutions: where two or more existing stand-alone solutions are integrated, usually using middleware technology;

3. Enterprise solutions: based on the logic of enterprise resource planning (ERP), these solutions attempt to integrate all departments and functions across a company into a single computer system that can serve all those different departments’ particular needs; and,

4. Extended enterprise solutions (XES): refers to the collaborative sharing of information and processes between the partners along the supply chain using the technological underpinnings of ERP.

7 Supply Chain Management and RSA Security

One of the greatest problems of supply chain information sent over the public networks and the internet is access by unauthorized users. The RSA techniques can be used to ensure that supply chain information is properly secured so that partners involved in supply chain can maximize and benefit from the gigantic information super highway. The RSA technique is used in RFID to ensure that there is better visibility in supply chain. RFID is a technology use for identification with a wide range of applications in the supply. In supply chain, RFID is used by the supplier to attached RFID tags to store information of outgoing products in manufacturing facilities (Rosselló. 2008). RFID have a cloaking system for ensuring that proprietary data that are located on product information carrying chips are properly guarded. The RSA techniques used in RFID ensures that supply chain information authentication (Matt Hines 2004, Ari Juels 2009). Also, with unique identifier, it is possible to keep track of every item in supply chain. The product information which is relevant at each stage of the supply chain can be tracked so that quality, timely delivery and fast reordering can be secured. RFID is a clever technology that ensures that security as well privacy uses proper key management techniques (i.e. RSA key management) and also, RFID is dependent on application (Ari Juels 2009). NSCCA (Nested Supply Chain Cryptographic System) uses public key cryptography to develop nested cryptography with the following objectives;

1. Authentication; It is the process of verifying true identity of someone
2. Privacy that is the seclusion of organization information
3. Protection in the supply chain

NSCCA protects data using a set of cyphertexts which are nested. RSA technology is a public key cryptography and NSCCA uses public key cryptography which RFID read and write into tags memory (Daniel Moreno Rosselló. 2008).

Since supply chain information is usually sent over the internet, there is the need for the network to be secure with the RSA public key cryptography using IP Security (IPSEC) and Internet Key

Exchange (IKE) protocols. The Internet security protocol also uses the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocol to secure web server which contain supply chain sensitive information. This protocol uses the RSA public key cryptography techniques to ensure that supply chain information is protected. The Pretty Good Privacy (PGP) is used to secure supply chain information sent via email. This is used when two or more supply chain partners are sending sensitive information via email. The Secure Shell (SSH) uses the RSA techniques and it ensures that remote access into a network that contain supply chain sensitive information is protected using terminal connection security. The Secure Internet Live Conferencing (SILC) is also used by supply chain partners to communicate vital information and it provides security through the process known as RSA encryption and authentication of the messages in the network.

The RSA technique is used in electronic commerce to ensure that supply chain ordered from many vendors and also ensure that supplies is properly secure and monitor. It also ensures that supply chain production schedule as well as inventory are properly inspected and secured. The RSA technique is used in supply chain to secure the following e-commerce activities:

1. Security of E-Commerce
2. Electronic Data Interchange
3. Secure Electronic Transaction Protocol
4. Electronic Cheque Payment (Minoli 2009).

7.1 RSA Technique

The RSA algorithm is used to send encrypted message and it do not require the exchange of separate secret keys. It is a public key algorithm that can also be used to ensure that message can be signed (DI anagement). In 1977, Ron Rivest, Adi Shamir and Len Adleman invented the RSA algorithm and it was named after them (Rivest et al 1978). The basic technique behind the RSA algorithm was discovered by Clifford Cocks [COCK73] of CESG (part of the British GCHQ) in 1973. The secret of the RSA technique that was hidden was discovered in 1997. The most widely used public key cryptography in the world is the RSA cryptosystem. It does not need a separate exchange of secret key for message to be encrypted. It is used for encrypting, signing and message key agreement. The arithmetic used in RSA for encrypting and decrypting is known as modular arithmetic. The RSA algorithm security is a function of the difficulty involve in factorizing n to obtain p and q prime numbers. To obtain n is easy i.e. by multiplying p and q but to obtain the prime numbers p and q which is the reverse operation of factorizing n is practically impossible especially when p and q are large numbers. RSA key size should modulus up to 2048 bits as suggested by several organizations (Lenstra and Verheul 2001). The keys size that RSA typically uses is 1024 to 2048. The RSA standard is in specified RFC 3447, RSA Cryptography Specifications Version 2.1 (Dan Boneh 1999).

7.2 RSA Signature

In RSA signature, signing required the use of private key while verification requires the use of public key (Dan Boneh 1999).

The RSA cryptosystem is the best known public-key cryptography. Also, the problem associated with the RSA security is the basis for RSA public key encryption and also RSA digital signature (Boneh 1999 and Katzenbeisse 2001). Moreover, RSA uses from integer factorization problem to obtain it security. RSA uses a public key for message encryption and private key for message decryption.

Furthermore, two decades of research into inverting the RSA function produced some insightful attacks, but no devastating attack has ever been found. The attacks discovered so far mainly illustrate the pitfalls to be avoided when implementing RSA. Presently, it appears that proper implementations can be trusted to provide security in the digital world (Boneh, 1999). Also, RSA attacks can be categorized into four categories and they are;

(1) Elementary attacks that exploit blatant misuse of the system

(2) Low private exponent attacks serious enough that a low private exponent should never be used

(3) Low public exponent attacks

(4) And attacks on the implementation (Boneh 1999).

7.3 RSA Security

RSA security is from factorization of problem. Difficulty of The RSA security is a function of how large is the number to be factorized. It ensure fast factorization algorithms are used like Trial division, Pollard's rho, Pollard's p-1, Quadratic sieve, elliptic curve factorization, Random square factoring and Number field sieve among others. Also, RSA is commonly used in electronic commerce protocols, and is believed to be safe given adequately long keys and the utilization of up-to-date implementations (Borodzhieva and Manoilov 2008).

7.4 RSA Algorithm

The algorithm is summarized into three parts and they are;

1. Key generation
2. Encryption and decryption process
3. Digital signature

Key Generation

1. Choose p and q prime number randomly such that p! = q
2. Compute modulus n = p*q (large prime must be used so that it will difficult to factorize)
3. Compute Φ = (p - 1)(q - 1)
4. Choose exponent e such that 1< e < Φ(n) and gcd (e, Φ(n)) = 1
5. Compute secret exponent $d = e^{-1} \bmod \Phi(n)$ (where (n,e) is the public key and d is the secret key)

Encryption and decryption process; for encryption, compute $c = m^e \bmod n$ and for decryption compute $m = c^d \bmod n$

The integrity of data can be guaranteed with the help of RSA digital signature. It distinctively identifies original sender of the digital signed data. It also ensures that the digital signed data is protected.

7.5 Tools for RSA Implementation

RSA implementation requires some tools and they are;

1. Arbitrary precision arithmetic (multiple precision arithmetic)
2. Pseudo Random Number Generator (PRNG)
3. Prime number generator among others (Garrett 2007)

RSA implementation problems depend on the following;

1. Implementation platform
2. Type of applications used
3. Number of tools needed to implement from start

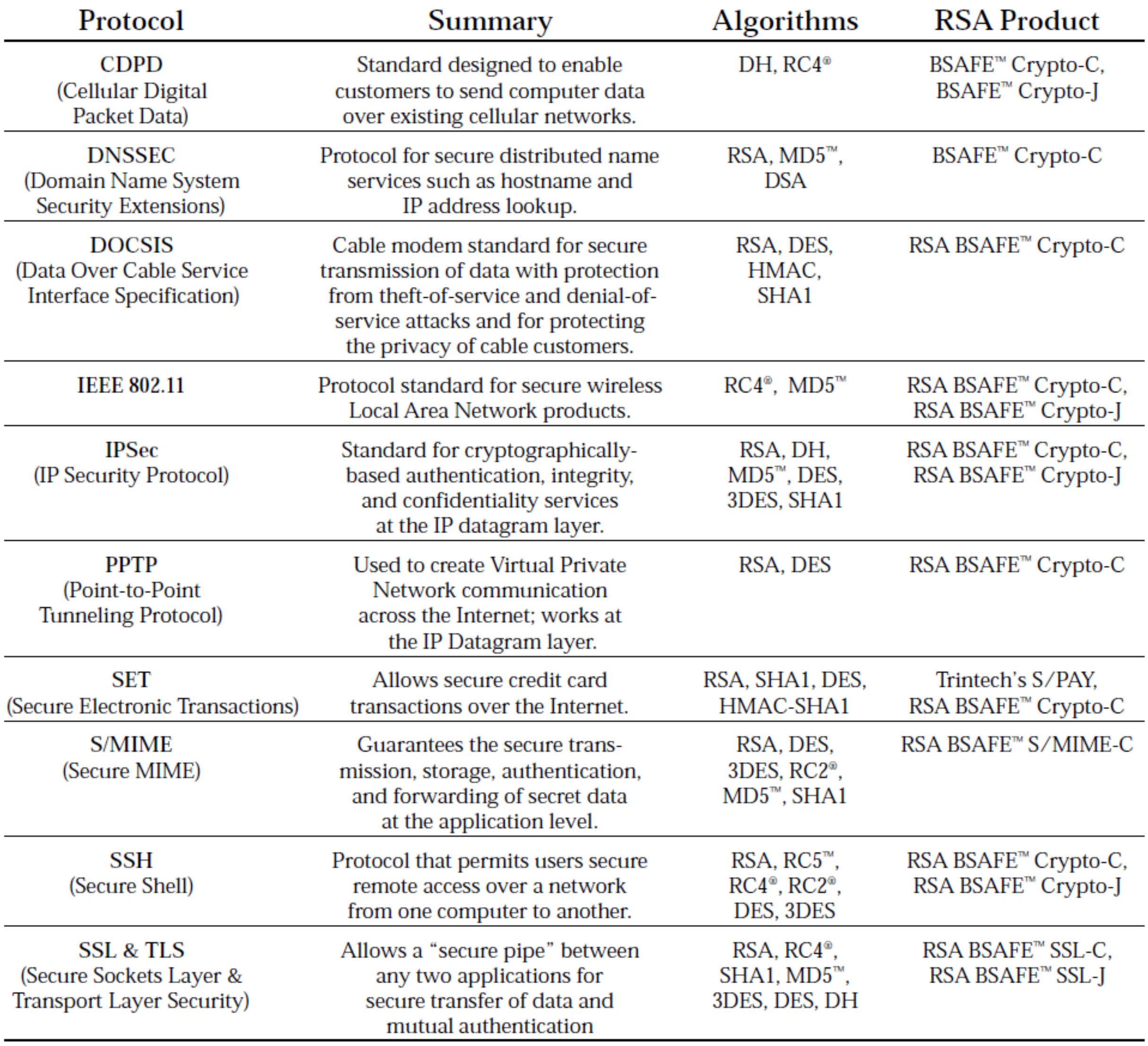
7.6 RSA Usage

RSA is widely used in many protocols that are security oriented. These security oriented protocols are outlined as follow;

1. Transport Layer Security (TLS) and Secure Sockets Layer (SSL) - transport data security (web)
2. Pretty Good Privacy (PGP) - email security
3. Secure Shell (SSH) - terminal connection security
4. Secure Internet Live Conferencing (SILC) - conferencing service security among other.

The table 1 below summarizes some most widely used security protocols and what RSA product developers need to implement them:

Table 1 Security Protocols Overview



Protocol	Summary	Algorithms	RSA Product
CDPD (Cellular Digital Packet Data)	Standard designed to enable customers to send computer data over existing cellular networks.	DH, RC4®	BSAFE™ Crypto-C, BSAFE™ Crypto-J
DNSSEC (Domain Name System Security Extensions)	Protocol for secure distributed name services such as hostname and IP address lookup.	RSA, MD5™, DSA	BSAFE™ Crypto-C
DOCSIS (Data Over Cable Service Interface Specification)	Cable modem standard for secure transmission of data with protection from theft-of-service and denial-of-service attacks and for protecting the privacy of cable customers.	RSA, DES, HMAC, SHA1	RSA BSAFE™ Crypto-C
IEEE 802.11	Protocol standard for secure wireless Local Area Network products.	RC4®, MD5™	RSA BSAFE™ Crypto-C, RSA BSAFE™ Crypto-J
IPSec (IP Security Protocol)	Standard for cryptographically-based authentication, integrity, and confidentiality services at the IP datagram layer.	RSA, DH, MD5™, DES, 3DES, SHA1	RSA BSAFE™ Crypto-C, RSA BSAFE™ Crypto-J
PPTP (Point-to-Point Tunneling Protocol)	Used to create Virtual Private Network communication across the Internet; works at the IP Datagram layer.	RSA, DES	RSA BSAFE™ Crypto-C
SET (Secure Electronic Transactions)	Allows secure credit card transactions over the Internet.	RSA, SHA1, DES, HMAC-SHA1	Trintech's S/PAY, RSA BSAFE™ Crypto-C
S/MIME (Secure MIME)	Guarantees the secure transmission, storage, authentication, and forwarding of secret data at the application level.	RSA, DES, 3DES, RC2®, MD5™, SHA1	RSA BSAFE™ S/MIME-C
SSH (Secure Shell)	Protocol that permits users secure remote access over a network from one computer to another.	RSA, RC5™, RC4®, RC2®, DES, 3DES	RSA BSAFE™ Crypto-C, RSA BSAFE™ Crypto-J
SSL & TLS (Secure Sockets Layer & Transport Layer Security)	Allows a "secure pipe" between any two applications for secure transfer of data and mutual authentication	RSA, RC4®, SHA1, MD5™, 3DES, DES, DH	RSA BSAFE™ SSL-C, RSA BSAFE™ SSL-J

Table 1: Most Widely Used Security Protocols (Security Brief 1999. RSA Data Security, Inc)

7.7 RSA: Is It Safe?

The RSA 2048 bit keys are enough till 2030. Also, RSA 3072 bit keys should be employed if there is need for further security further than 2030 (Burt Kaliski 2003). Moreover, RSA algorithm (Public key algorithm) is a safe algorithm. 2048 bits or more can be used for better security. This is because factorizing a large number is difficult. Due to increase in computer technology, the use of 768 bit RSA module is no longer reliable and 1024 bit module is also not too reliable. Besides, for more security, larger prime's p and q must be used to create the public key (n). The ANSI X9.31

standard recommends that strong primes must be used for RSA module and not safe primes. In cryptography, large safe prime can be considered as strong prime. Also, a prime number p is said to be strong if it satisfy the following conditions;

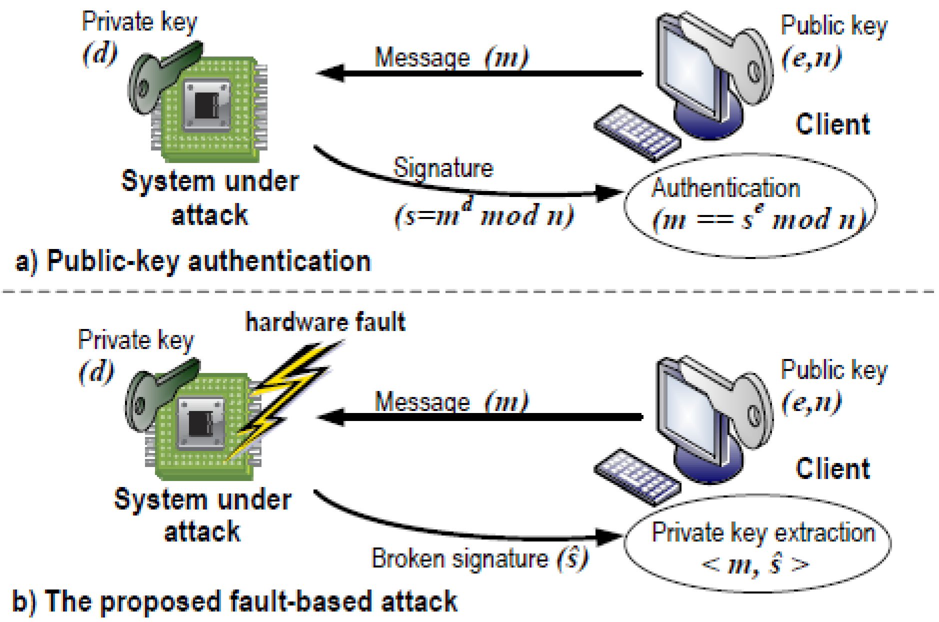
1. p is large
2. p - 1 has large prime factors i.e. $p = a_1q_1 + 1$ for some integer a_1 and large prime q_1
3. p - 1 has large prime factors i.e. $p = a_2q_2 + 1$ for some integer a_2 and large prime q_2
4. p + 1 has large prime factors i.e. $p = a_3q_3 - 1$ for some integer a_3 and large prime q_3 (Ron Rivest and Robert Silverman 2001)

In addition, "the absolute minimum size for n is 2048 bits or if you want to protect your data for 20 years. If you can afford it in your application, let n be 4096 bits long, or as close to this size as you can get it"(Ferguson & Schneier (2003)). (p. 233). Finally, to keep confidential data, it recommended using RSA key size greater than 2048 bits.

7.8 Limitation of RSA Algorithm

The problem with RSA algorithm is slow decryption process due to increase or doubling of key length. The use of small p and q is also a limitation because small key length is insecure i.e. an eavesdropper could recover the plaintext. Another limitation is the encryption speed which can be overcome using a protocol known as the digital envelope. Also, another RSA algorithm limitation that could occur in the near future is design of TWIRL (The Weizmann Institute Relation Locator) which is a hypothetical hardware device that can speed up the sieving step of the general number field sieve integer factorization algorithm. Also, the hardware if built will factor 1024 bit RSA numbers (Adi Shamir and Eran Tromer (the designers)). A research conducted by the University of Michigan suggested that fault based attack of RSA authentication is possible (figure 12). The research demonstrated a way to hack RSA 1024-bit private key encryption use in laptop, Smartphone’s, media players that are used to secure customer information in the internet.

According to the research, it was found that private key used in RSA security can be hacked or obtained by varying voltage on a device. The process subjects the system to transmit faults and then collect the corrupted signature output. The private key is extracted using offline analysis after collecting sufficient number of corrupted messages. It requires less knowledge of system to be hacked (Pellegrini, Valeria Bertacco and Todd Austin. 2010).



a) Public-key authentication

b) The proposed fault-based attack

Figure 12; Fault based attack of RSA authentication (Pellegrini *et al.* 2010).

A cryptographic technique call "salting" can be use to overcome this limitation. It works by changing the digits order randomly or randomly juggling a private key's digits each time a key is requested. The advantage of salted password is to prevent dictionary attack (i.e. a method use for overcoming authentication system by searching likely possibilities in order to determine its decryption key). RSA is a clever algorithm that can survive any attack.

8 RSA Techniques Today

The RSA cryptography is the widely use public key cryptography in the world today. It is the crypto system deployed in thousands of applications today round the world to maintain security. Thus, there have being several records of RSA systems compromised. Moreover, it is still most widely used public key cryptography. This is because standards have been put in place to ensure RSA cryptography survival. Since complicated systems are sometime liable to compromise, there is the need for there to be standards. These standards when follow regularly ensure better and more secure systems. The RSA standards are regularly updated by RSA cryptography professionals worldwide to regularly update RSA crypto system. PKCS #1 version 2.1 is the newest standard used by RSA crypto system today. There exist widely accepted standards for most cryptographic operations, such as the Advanced Encryption Standard (AES) for secret-key encryption and 2048-bit RSA for public-key encryption. These primitives have been widely studied, and hacking them is believed to be computationally impossible on any existing computer cluster (Bernstein et al 2012). Today, SSL Secure Sockets Layer uses 2048 bit encryption to establish secure connection with other application, web browsers and email programs. The secure SSL notify online customers about unsecure application. RSA is extensively used in electronic commerce protocols, and is believed to be safe given adequately long keys and the use of up-to-date implementations (LOKULWAR et al 2012). RSA cryptography is still a suitable security measure for electronic data. Thus, the weakness of the algorithm is due to the used of low private exponent. Low private exponent should never be used because there have been records of low public key attacks ranging from brute force attack, subtle attack among other. RSA cryptography must be correctly employed to avoid attack (Singh et al 2012). Table 2 below shows RSA key lengths that were recommended to protect lifetime of confidential data (Shamir & Tromer's estimate, Kaliski (2003)).

Lifetime of data	RSA key size
Up to 2010	1024 bits
Up to 2030	2048 bits
Up to 2031 onwards	3072 bits

Table 2: RSA Key Lengths (Shamir & Tromer's estimate, Kaliski (2003)).

One of the problems of the use of large prime numbers in RSA cryptography to enhance security is slow encryption and decryption process. A research carry out by Nagar et al 2012 showed that it is possible to enhance the speed of the RSA performance by generating keys offline and storing them in separate databases before RSA key pair in encryption/ decryption processes begin. The research also showed that the use of RSA-Key generations offline algorithm with different keys lengths, the decryption processes is 2.5 times faster than online RSA keys generations. The research used timings on a 2.8GHz Pentium with the following conditions below;

1. Block size is 2048 bits.
2. Different bandwidths:

    (a) 1000 Mbps.

    (b) 100 Mbps.

    (c) 4 Mbps.

Figure 13 show that key generation offline is faster than using normal RSA key generations.

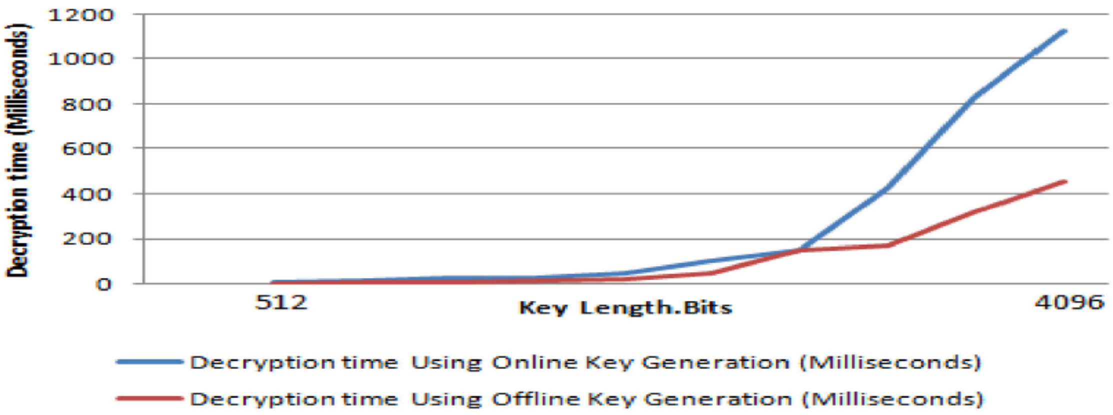


Figure 13: Compare between decryption processes using online and offline RS-key generations (Nagar et al 2012).

A research were conducted recently by Fujitsu Laboratory on the security of RSA encryption which is the widely encryption for internet shopping. The research were able to able to factor 176 digit composite number using software in collaboration with some universities and other institutions to attain a world class record for the size of the factorized number. The result of their experiment also showed that 2048 bit RSA encryption will be safe for at least the next 10 years (Fujitsu Group Information Security Report 2012).

The secure socket layer which is the basis for internet security uses RSA encryption for it authentication. Initially, the secure socket layer used 512 bits RSA key which was modify to 1024 bits RSA key. Moreover, the recommended RSA key now for secure socket layer is 2048 bits RSA key. The RSA algorithm has got numerous vulnerabilities that may possibly be exploited, thus making possible hacking of the algorithm. Also, better security measure has been put in place to avoid exploited breaches.

A modified RSA algorithm was proposed by (Parshotam et al 2012). The modified algorithm implementation, introduce the use of bit stuffing which enable the algorithm to switch from the domain of integer to bit stuffing domain. The introduction of bit stuffing into the algorithm enhances the security of RSA cryptography because it makes accessing the message difficult even after getting the access to the secret key. Also, the use of bit stuffing is an unavoidable requirement for the design of secure communication in cryptography protocols (Parshotam et al 2012). Figure 14 show how bit stuffing is use with RSA cryptography.

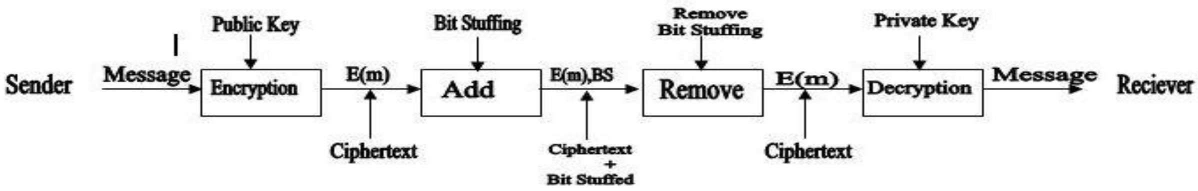


Figure 14: Encryption and Decryption (Parshotam et al 2012).

Conclusions

The advent of computer networks and internet has made it possible to send and receive information with ease. Computer hackers on the other hand have been threats to this technology. Over the years, these threats lead to computer and internet security to prevent malicious users from gaining access to vital information.

This thesis examines supply chain security, supply chain information security and the use of RSA techniques. The RSA technique is a secured standard for public key cryptography. It helps to secure supply chain information. The thesis also shows that supply chain security is very important in supply chain management.

The use of 2048 bits or more RSA techniques are better for high security protection due to difficulties involve in factorizing large prime numbers. It could be infer that, 2048 bits or more bits are recommended for better supply chain security. Moreover, further studies should be carried out on RSA techniques on supply chain security.

References

Andersen T. J. (2001). Information technology, strategic decision making approaches and organizational performance in different industrial settings. *Journal of Strategic Information Systems* 10, 101–119

Ang C. L, Davies M. and Finlay P. N. (2000). Measures to assess the impact of information technology on quality management. *International Journal of Quality & Reliability Management* 17 (1), 42–65.

Ari J. (2005). Attack on a Cryptographic RFID Device, *RFID Journal*

Ari Juels. (2009). RFID Security and Privacy: A Primer. RSA Laboratories. ENISA-FORTH NIS

Ayers J. B. (2001), *Handbook of Supply Chain Management*, St. Lucie Press, Boca Raton, 4-5

Banomyong R. (2005). The impact of port and trade security initiatives on maritime supply-chain Management. *Maritime Policy & Management* 2 (1), 3-13.

Blanchard D. (2010), Supply Chain Management Best Practices, 2nd. Edition, John Wiley & Sons, ISBN:9780470531884

Bolhari A. (2009). Electronic-Supply Chain Information Security: A Framework for Information, Shahid Beheshti University.

Boneh D. (1999). Twenty years of attacks on the RSA cryptosystem. Notices of the AMS, 46(2), 203–213.

Borodzhieva A. and Manoilov P. (2008). Software Tool for Implementing RSA Algorithm, Rousse University “Angel Kanchev”, Rousse, Bulgaria. *International Scientific Conference Computer Science*

Cachon G. P. (2003), Supply chain coordination with contracts, In: Handbooks in Operations Research and Management Science, 11: Supply Chain Management: Design, Coordination and Operation.

Canavan J. E. (2001) Fundamentals of Network Security, Artech House Publishers; 1st edition.

Carr A. and Kaynak H. (2007). Communication methods, information sharing, supplier development and performance”, International Journal of Operations & Production Management 27(4) 346-370.

Chen C.T., Lin C. T. and Huang, S.F. (2006). A fuzzy approach for suppler evaluation and selection in supply chain management. International Journal of Production Economics, 102, 289–301.

Chen I.J. and Paulraj (2004). Towards a theory of supply chain management: the constructs and measurements. Journal of Operations Management, 22, 119-150.

Christiaanse E., Kumar K. (2000). ICT-enabled coordination of dynamic supply webs. *International Journal of Physical Distribution & Logistics Management* 30 (3/4), 268–285.

Christopher, M. G. (1992), *Logistics and supply chain management: strategies for reducing costs and improving services*, London: Pitman.

Christopher, M. (2005) *Logistics and Supply Chain Management: Creating Value-Adding Networks* London: FT Prentice Hall.

Cipriano F. (1995). The impact of information systems on quality performance: an empirical study. International Journal of Operations & Production Management, 15(6) 69 – 83.

Closs D. J. and McGarrell E.F. (2004). Enhancing security throughout the supply chain, Special Report Series, IBM. Center for The Business of Government.

Cocks C. (1973). *A Note on 'Non-Secret Encryption'*, CESG Research Report

Conner F. W. and Coviello A. W. (2004), Information security governance: a call to action, Corporate Governance Task Force Report of 2004.

Cooper M. C., Lambert D. M., and Pagh J. D. (1997). Supply Chain Management:More Than a New Name for Logistics. *The International Journal of Logistics Management* 8(1), 1–13

Council of Supply Chain Management professional 2011 (www.cscmp.org)

Czernowalow M. (2005). Lack of policy causes IT risks. Available at: http://www.itweb.co.za

Datta S., Granger C.W.J., Barari M. and Gibbs T. (2007) Management of supply chain: an alternative modeling technique for forecasting, *Journal of the Operational Research Society*, 58(11) 1459-1469.

Elkins D., Handfield R. W, Blackhurst J. and Craighead C. W. (2005) 18 Ways to Guard against Disruption. Supply Chain Management Review pp. 46-53.

Elliman T., Orange G. (2000). Electronic commerce to support construction design and supply chain management: A research note. *International Journal of Physical Distribution & Logistics.* 30 (3/4), 345–360.

Fabian B. and Günther O. (2009) Security challenges of the EPCglobal network," Commun. ACM, 52(7), 121–125, 2009.

Forrester J. W. (1958) Industrial Dynamics: A Major Breakthrough for Decision Makers Harvard Business Review , 38 37-66.

Fratianni M and Kang H. (2004). Borders and International Terrorism, Working Paper, Kelley School of Business, Indiana University.

Fujitsu Group Information Security Report. (2012) http://www.fujitsu.com/downloads/CSR/management/security/2012/security2012-12-e.pdf

GAO (2012). IT SUPPLY CHAIN National Security-Related Agencies Need to Better Address Risks. GAO-12-361, Mar 23, 2012.

Garrett P. (2003). Cryptographic Primitives, in *Public-key cryptography: American* Pfleeger CP, Pfleeger SL.Security in computing. 3rd ed. Prentice Hall.

Garfinkel S. (2002). Web Security, Privacy and Commerce. Cambridge, MA: O'Reilly and Associates. Review chapter for the New Economy Handbook (Jones, ed.).

Gerencser M.,Weinberg J and Don Vincent.(2002).Port Security War Games: Implications for U.S. Supply Chain. Booz Allen Hamilton.

Graham G. and Hardaker G. (2000). Supply-chain management across the Internet. *International Journal of Physical Distribution & Logistics Management*. 30 (3/4), 286–295.

Gunasekaran A. and Ngai E.W.T. (2004). Information systems in supply chain integration and management. *European Journal of Operational Research*/ 159, 269–295.

Haas C. T., Borcherding J. D., Glover R. W., Tucker R. L., Alemany C.And Fagerlund W. R.(2000).The Effects Of Computers On Construction Foremen.Center For Construction Industry Studiesreport No. 9

Hau L. and Whang S. (2005). Higher supply chain security with lower cost: Lessons from total quality management, International Journal of Production Economics 96, 289-300.

Hendricks K. B. and Singhal V.R (2005).Association between Supply Chain Glitches and Operating Performance. Management Science, 51(5) 695-711

Hewlett-Packard Company. (2003). Modern Cryptography: Theory and Practice. Publisher: Prentice Hall PTR. http://www.hp.com/sbso/productivity/howto/security/index.html

ISO. (2004) The ISO survey of ISO 9001:2000 and ISO 14001 certificates 2003. <http://www.iso.ch/iso/en/iso9000-14000.

Jacoby D. (2009), Guide to Supply Chain Management: How Getting it Right Boosts Corporate Performance (The Economist Books), Bloomberg Press; 1st edition, ISBN 978-1576603451

Jaggar D., Ross A., Love P.E.D. and Smith J. (2001), Overcoming information opacity in construction: a commentary. Logistics Information Management, 14(5/6) 413-420.

Janak S. (1996). The importance of information flow within the supply chain", Logistics Information Management, 9 (4), 28 - 30

Jones T. and Riley D. W. (1985), Using Inventory for Competitive Advantage through Supply Chain Management, *International Journal of Physical Distribution and Materials Management* 15(5), 16-26.

Juels A.(2005) Attack on a Cryptographic RFID Device. RFID Journal

Juhel M. H. (2009). An Introduction to the Supply Chain Security Guide of The World Bank, Transport. The World Bank, 2009.

Katz F. H. (2005) The effect of a university information security survey on instructing methods in information security. In: Proceedings of the second annual conference on information security curriculum development; 43–8.

Katzenbeisser S. (2001). Recent Advances in RSA Cryptography. Kluwer Academic Publishers.

Kearney AT.(2005). "Smart Boxes," Chicago, 2005.

Keown A.J. Martin J.D. Petty J.W. and Scott D.F. (2004). Financial Management :Principles and Applications, 10th Ed., New York: Prentice Hall.

Lambert D. M and Cooper M. C.(2000). Issues in Supply Chain Management. *Industrial Marketing Management* 29, 65–83

Lambert D. M., Cooper M. C. and Pagh J. D. (1998). Supply chain management: implementation issues and research opportunities, *International Journal of Logistics Management*, 9 (2), 1-19.

Lambert D., García-Dastugue S. and Croxton, K. (2005). An evaluation of process-oriented supply chain management frameworks. *Journal of Business Logistics*, 26, (1), 25-51.

Lee H. L. and Whang S. (2005) Higher supply chain security with lower cost: Lessons from total quality management. International Journal of Production Economics, 96, 289-300.

Lenstra A. K and Verheul E. R. (2001). Selecting cryptographic key sizes. Journal of Cryptology, 14255–293

Li S. and Lin B. (2006) Accessing information sharing and information quality in supply chain management. Decision Support Systems, 42(3), 1641-1656.

Lockamy III A. and McCormack K. (2004). Linking SCOR planning practices to supply chain performance, an exploratory study. *International Journal of Operations & Business Management*, 24, (12), 1192-1218.

Lu Chin-Shan. (2004). An Evaluation of Logistics Services' Requirements of International Distribution Centers in Taiwan," Transportation Journal, pp. 53-66.

Luong H. T. and Phien N. H. (2007), *Measure of bullwhip effect in supply chains: The case of high order autoregressive demand process*, European Journal of Operational Research, 183 (1), 197-209

Mark G. W. J. and Vincent D. (2002).Port Security War Games: Implications for U.S. Supply Chain 2002, Booz Allen Hamilton.

Mathematical Society short course, January 13-14, 2003, Baltimore, Maryland.

Matt Hines. 2004. RSA polishes RFID shield. Staff Writer, CNET News. http://news.cnet.com

McDonnell R., Sweeney E. and Kenny J. (2004). The Role of Information Technology in the Supply Chain' Logistics Solutions,7(1) 13-16.

McIvor R., Humphreys P. and Huang G. (2000). Electronic commerce: Re-engineering the buyer–supplier interface. Business Process Management Journal. 6 (2), 122–138.

Mentzer J. T., Witt W. D. And Keebler J. S. (2001) Defining Supply Chain Management. Journal of Business Logistics 22(2) 1-25

Mentzer J.T. (2004). *Fundamental of Supply Chain Management*, Thousand Oaks, California: SAGE Publications

Michael O. H. (2002). Protecting the American Homeland, Washington, DC: Brookings Institution.

Minoli D and Minoli E. (1999). Web Commerce Technology Handbook, Tata McGraw-Hill, New Delhi.

Mitroff I. I. and Alpaslan M. C. (2003) Preparing for Evil, Harvard Business Review pp. 109-115

Molar A. E. (2004). Container Security: Who Pays. Journal of Commerce, Nov. 1, 2004, p. 60.

Motwani, J, Madan M, Gunasekaran A. (2000). Information technology in managing supply chains. Logistics Information Management 13 (5), 320–327.

Murillo L. (2001). Supply chain management and the international dissemination of e-commerce. Industrial Management & Data Systems 101 (7), 370–377.

National Defense University (2002) The Virtual Border: Reducing The Risk Of Sea-borne Container Terrorism," Washington, DC, August 2002.

Oliver R. K. and Webber M. D. (1982). Supply-chain management: logistics catches up with strategy", Outlook, Booz, Allen and Hamilton Inc. Reprinted 1992, in Logistics: The Strategic Issues, ed. M Christopher, Chapman Hall, London, pp. 63-75.

O'Hanlon M. (2002). Protecting the American Homeland. Washington, DC: Brookings Institution

Parshotam and Rupinder Cheema and Aayush Gulat. (2012). Improving the Secure Socket Layer by Modifying the RSA Algorithm. International Journal of Computer Science, Engineering and Applications, 2(3)

Patnayakuni N. and Rai A.(2002) Towards a theoretical framework of digital supply chain integration, European Conference on Information Systems (ECIS), Gdańsk, June, 2002. [Online]. Available: http://is2.lse.a c.uk/asp/aspecis/20020127.pdf

Pfleeger C. P and Pfleeger S.L.(2003) Security in computing. 3rd ed. Prentice Hall

Poirier C. and Bauer M. (2000), E-supply Chain: Using the Internet to revolutionize your business, Berrett-Keohler Publishers, San Francisco, CA.

Prasad Lokulwar, Vivek Shelkhe. (2012). Security aware routing protocol for manet using asymmetric cryptograpy using rsa algorithm. BIOINFO Security Informatics, 2(1) 11-14

Prasant Singh Yadav, Pankaj Sharma, Dr K. P Yadav. (2012). Implementation of rsa algorithm using elliptic curve algorithm for security and performance enhancement. International Journal of Scientific & Technology Research, 1(3)

Sarathy R. and Robertson C. J. (2003). Strategic and Ethical Considerations in Managing Digital Privacy. Journal of Business Ethics, 46(2),111-126.

Supply & Demand Chain Executive (2005), Electronic Newsletter.

Tsai C.Y. (2008). On supply chain cash flow risk. Decision Support Systems 44, 1031-1042.

Rice J. B. and Spayd P. W. (2005). Investing in Supply Chain Security: Collateral Benefits. IBM Center for Business of Government

Rivest R., Shamir A .and Adleman L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, 21 (2)120-126

Rivest R. L. (1990). Cryptology. In J. Van Leeuwen. *Handbook of Theoretical Computer Science*. Elsevier.

Rosetti C. and Choi C. Y. (2005). On the dark side of strategic outsourcing: experiences from the aerospace industry," Academy of Management Executive, 19(1)45-60.

RSA Laboratories.(2002), PKCS#1 v2.1: RSA Cryptography Standard, June 2002, http://www.rsa.com/rsalabs/node.asp?id=2125

RSA Theory. (2006). DI Management. Available at: http://www.di-mgt.com.au/rsa_theory.html

Rosselló D. M. (2008). NSCCA Ccyptographic system over RFID §implementation.DOI:http://hdl.handle.net/2099.1/7423

Russell M. and Saldanha J. P. (2003) Five tenets of Security-Aware Logistics and Supply Chain Operations,Transportation Journal pp. 44-54.

RSA Data Security Inc. (1999). Security Protocols Overview, an RSA Data Security Brief.

Sheffi Y. and Rice J. B (2005). A Supply Chain View of the Resilient Enterprise. Sloan Management Review, pp. 41-48.

Siponen M. T. (2001) Five dimensions of information security awareness. Computers and Society, 31(2), 24–9.

Sodhi M. S. (2003). How to do Strategic Supply Chain Planning, Sloan Management Review pp.69-75.

Specification for security management systems for the supply chain. Available at: http://www.iso.org/iso/catalogue_detail?csnumber=41921

Stock,J. Stefanie L. Boyer S. and Harmon T. (2010). Research opportunities in supply chain management. *Journal of the Academy of Marketing Science*, 38, (1), 32–41.

Straub D. W. and Nance W. D. (1988). Uncovering and disciplining computer abuse: organizational responses and options. Information Age, ISSN: 0261-4103, 10(3), 151–6.

Straub D.W. and Welke R.J. (1998). Coping with systems risk: security planning models formanagement decision making. MIS Quarterly, 22(4) 441-64.

Susan A. S. (2005). From supply-chain management to value network advocacy: implications for e-supply chains, Supply Chain Management: An International Journal, 10(2) 77 - 83

Sweeney E. (2006). From Management of Distribution to Management of Supply Chains: the Evolution of SCM. Logistics Solutions, 9(2), 11-14.

Tang C. S. (2006). "Robust strategies for mitigating supply chain disruptions," International Journal of Logistics: Research and Applications, 9(1), 33-45.

Trent R. J. and Monczka R. M. (2002). Pursuing competitive advantage through integrated global sourcing. Academy of Management Review, 16(2), 66-80.

Tyndall G., Gopal C. Partsch W. and Kamauff, J. (1998). *Supercharging supply chains: New ways to increase value through global operational excellence*, John Wiley and Sons, Inc.

United States Government Accountability Office. (2012). Additional efforts needed by national security-related agencies to address risks.

Van Hooft F.P. C. and Stegwee R. A. (2001). E-business strategy: How to benefit from a hype. *Logistics Information Management*. 14 (1/2), 44–53.

Verisign. 2005. Securing RFID Data for the Supply Chain.

Verton D. (2002). Disaster recovery planning still lags. Computerworld, 36(14), 10.

Wadhwa et al 2009. Information Security in Flexible Supply Chain Network: A Decision Information Security (DIS) Model. Global Journal of Enterprise Information System 1 (2) 25 – 31.

Wamba S. F and Boeck H. (2008) Enhancing Information Flow in a Retail Supply Chain Using RFID and the EPC Network: A Proof-of-Concept Approach.Journal of Theoretical and Applied Electronic Commerce Research,3(1) 92-105.

Weber S. G. (2009). Securing first response coordination with dynamic attribute-based encryption. Privacy, Security, Trust and the Management of e-Business, 2009. CONGRESS'09. World Congress on Pages 58-69

Weis S. A. (2003). Security and Privacy in Radio-Frequency Identification Devices Masters thesis in computer science, Dept. of Electrical Engineering and Computer Science, MIT, May 2003.

Wenbo M. (2004). Modern Cryptography: Theory & Practise. Hewlett-Packard with Prentice Hall.

Whitman M. E. and Mattord H. J. (2005). Principles of Information Security, 2nd ed. © 2005 Course Technology, Boston, MA, ISBN 0-619-21625-5

Williams L. R., Esper T. L. and Ozment J. (2002), The electronic supply chain: Its impact on the current and future structure of strategic alliances, partnerships and logistics leadership. *International Journal of Physical Distribution & Logistics Management*, 32(8), 703-719.

Yogesh V. J. (2000). Information Visibility And Its Effect On Supply Chain Dynamics.Master of Science at the. Massachusetts Institute of Technology. USA.

Yossi S. (2001). Supply Chain Management under the Threat of International Terrorism. The International Journal of Logistics Management, 12(2) 1-11.

Zeithaml V.A., Parasuraman A., and Malhotra A. (2000). A conceptual framework for understanding e-service quality. MSI Working Paper.

Zeng S. X., Lou G. X.and Vivian W.Y. Tam. (2007).Managing information flows for quality improvement of projects. Measuring Business Excellence, 11(3) 30 – 40