MODELING AND ANALYSIS OF INFORMATION SECURITY IN SUPPLY CHAIN MANAGEMENT

A THESIS IN ENGINEERING SYSTEMS MANAGEMENT

Presented to the faculty of American University of Sharjah
School of Engineering
in partial fulfillment of
the requirements for the degree

MASTER OF SCIENCE

by

AHMED MAHER AL-NUNU
B.S. 2001

Sharjah, UAE
June 2006

MODELING AND ANALYSIS OF INFORMATION SECURITY IN SUPPLY CHAIN MANAGEMENT

Ahmed Maher AL-Nunu, Candidate for the Master of Science Degree

American University of Sharjah, 2006

ABSTRACT

This research presents a quantitative information security model using measurable values to describe the security of information system in supply chain management (SCM). The security of supply chain management concerns the security of various interactions among many drivers. Each driver requires a different security level relevant to the services it contributes to the overall supply chain. This research proposes a security model in which each of the basic goals of security, i.e., confidentiality, integrity, availability and accountability, are assigned a different weight appropriate to the driver's mission. A semi-Markov chain model is used to describe a probabilistic nature of different security levels for each driver in the SCM system. A transition matrix representing the semi-Markov chain model of each driver is developed. Then, a system-wide security for SCM is produced using the transition matrices of each agent to reach steady-state probabilities of the organization's information security. Comparison of the steady-state security for SCM model with different levels of attacks is presented, and the obtained results are then analyzed. To achieve higher, reliable and secure SCM information system, each driver should have full control, feedback, availability and recovery for its own security. However, there is a tradeoff between process integration and security of the information shared among

all drivers. There is a demand to have a measuring tool of the security level for each driver and its impact on the other drivers' security. This model is used to present several scenarios with different levels of attackers. The model has been tested for SCM with four drivers where each driver has a different mission so the authors assigned different values of confidentiality, integrity, availability and accountability to each driver as deemed relevant to their mission. In addition, seven levels of attackers (5%, 20% … 95%) were tested to present different security responses. The model runs for steady-state for all combinations. The outcome of this research shows that the SCM sharing security and information has been improved at all level of attacks. Individual driver exposed to higher risk of attack can lead to a higher vulnerability of the SCM. In addition, this model has been tested for wider applications such as; electronic commerce systems; multi agent organizations.

CONTENTS

FIGURES

Figure Page

TABLES

Table Page

GLOSSARY

p_{ij} - Probability of moving from a state i to a state j

$p_{ij}^{(n)}$ - n-step transition probability

π_i - Steady-state probability

P - Initial transition matrix

p_C - Probability of attacking confidentiality

π_C - Steady-state probability of confidentiality

π_{Ssys} - Steady-state system security

P_{sw} - System wide initial transition matrix

d - Deflection factor

CIA - Confidentiality, integrity, and availability

CIAA - Confidentiality, integrity, availability, and accountability

CIO - Chief information officer

CSO - Chief security officer

DoS - Denial of service

ERP - Enterprises resource planning

FTP - File transfer protocol

GTM - General transition matrix

IDS - Intrusion detection system

IS - Information system

IT - Information technology

i-war - Information war

MTSF - Mean time to security failure

SCM - Supply chain management

TM - Threat management

VM - Vulnerability management

ACKNOWLEDGEMENTS

First, I send all my thanks to ALLAH (The GOD) for his endless givens. Second, I send my thanks to our prophet Mohammed (GOD's blessing and peace be upon him). Then, I acknowledge the endless care and support of my mother and father through all my life.

I would like to acknowledge support of this work by Dr. Ibrahim AL Kattan, my advisor and the director of the ESM program. Also, I would like to acknowledge the support of Dr. Kassem Saleh, professor in the computer science department in AUS. Finally, I acknowledge the high level of education provided by the government of Sharjah and UAE through the AUS, which provided me the chance to fulfill my Master Degree.

CHAPTER 1

1. INTRODUCTION

The presence of criminals, terrorists, competitors, state security services, and malicious or curious individuals makes the i-war (information war) threat to organizations a real one (Hutchinson, 2002). Information security of the supply chain management (SCM) is essential and covers a wide scope of organizations. However, the main challenge in supply chain management is information integration, and irregularity; i.e., information that is available to one or more drivers in the chain (e.g., supplier, manufacturer, retailer, and customer) but not available to others, (Chopra et al., 2004). Also, the attacks that could penetrate more than one driver in the supply chain systems through the weakest driver.

The rest of the report goes as follow. Chapter 1 is an introduction to supply chain management and the importance of information to link supply chain drivers. Then it will give an introduction on information security and how it is integrated with supply chain management. Chapter 2 will be the literature review to give a back ground on what has been done in this area. Chapter 3 will explain the proposed information security model and the proposed way to test it with the supply chain information security management. Chapter 4 is a testing of the model in general and chapter 5 is a test and analysis of the supply chain information security. Finally, chapter 6 will be a conclusion and a present of expected future work and development on the security model.

1.1 Supply Chain Management

The flow of information and the transportation of goods are the main bridge to link and integrate all drivers. The performance of information security could be achieved through interactions and smooth flows of information from suppliers to customers (Chopra et al., 2004). Information is needed to have a visible view of what customers want, the estimated level of inventory in the stock, and to know when to produce and ship products, etc. Based on this information, manager can take the right and efficient decisions. On the other hand, information should be accessible, timely, accurate and user friendly to compete in the global market. Improving the performance of information flow among the supply chain drivers has a valuable effect on customer satisfaction. Information sharing is an important factor of cooperation in supply chain management. It can be categorized according to operations areas such as

inventory, sale, demand forecasting, order state, and production plan (Lee et al., 1999). Information sharing of the inventory and production plan is a two-way communication between the downstream and upstream organizations on the supply chain. While, the sale and demand forecasting information flows from downstream companies to their upstream partners. And the order state information is provided by upstream organizations to their downstream partners. In addition, information sharing also includes performance criteria, such as production quality data and early complete date etc., and production capacities among the partners (Gang et al., 2005). But, due to the existence of competitors, hackers, and intruders information should be secured at the supply chain parties while being shared. The process starts with an order of raw materials and/or semi finished parts from the supplier, then they are used for the manufacturing or assembling processes, transported to the distributor, then to the retailer, and to the end users (the customers). Usually the supply chain parties could come from different countries, or regions, with different levels of technologies and levels of securities. In fact, most supply chain management systems are global in nature. For these reasons, sharing information between them will be truly vulnerable to the individual party and to the supply chain security (Knorr et al., 2001). One example is e-commerce: the customer has to insert a credit card number, address, and other information which should be secured during transaction and processing. Figure 1 shows the flow of information, the goals of security, and the physical flow of parts through the SCM drivers.

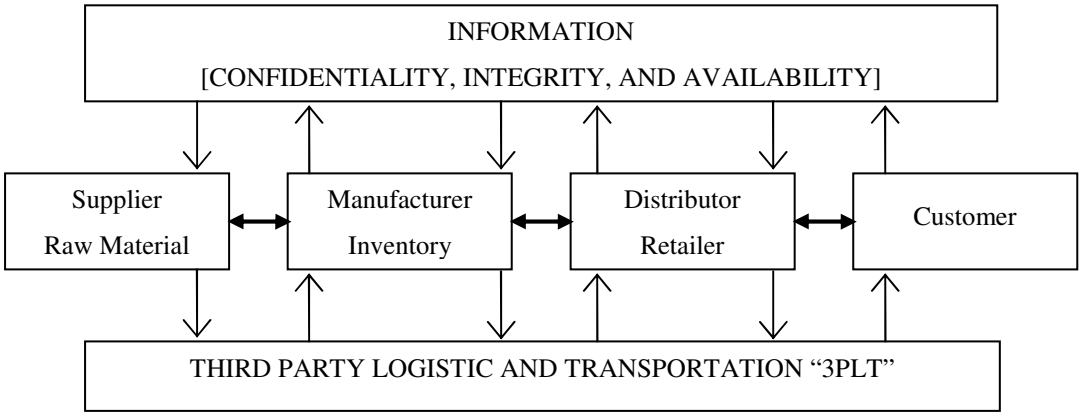


Figure 1 Flow of Information and Physical Parts through the SCM Drivers

The characteristics of the information security in SCM are (Chopra et al., 2004): (1) Integrity: the information must be accurate; (2) Availability: the system is

accessible in a timely manner whenever needed. Hence, the security of supply chain management concerns a variety of decisions about the four drivers; suppliers, inventories, logistics and transportation, facilities and costumers satisfaction. The main functions of the drivers in the SCM are:

1) Supplier: receiving the right quantity; quality; price on right time and right location.
2) Inventory: setting optimal inventory policies requires information that includes demand patterns, cost of carrying inventory, cost of stocking out, and cost of ordering.
3) Transportation: decisions on transportation networks, routings, modes, shipments, and vendors require information including costs, customer locations, and shipment sizes to make good decisions.
4) Facility: determining the location, capacity, and schedules of a facility requires information on the trade-offs between efficiency and flexibility, demand, exchange rates, taxes and so on, (Chopra et al., 2004).
5) Marketing: to set policies for promoting services the sales and determining the potential locations of customers, retailers and distribution centers.

1.2 Information Security

Information security has become more complex than ever before. The rate of new threat emergences, and increasing of attack methods keep security management more essential and dynamic (Ahlm, 2006). We chase hackers in continues close loop; application developers create bugs, hackers create exploits, systems become vulnerable to threats, leads to creating correction patches by software developers (Ahlm, 2006). Securing a system against attacks does not prevent all losses. Still to be; data theft, social engineering, phishing, misuse or other “hacking” methods that do not involve technically exploiting a system are reality (Ahlm, 2006).

Information Security addresses three very important goals related to information system: confidentiality, integrity, and availability (CIA). Confidentiality (C) ensures the information system assets should be accessed only by authorized parties. While Integrity (I) means the information is modified only by authorized parties and/or only in authorized ways. Finally, Availability (A) means the information system assets are always accessible by authorized parties and is contrary to denial of service (DoS). To have a secure system, all three goals of security in CIA

should be met. As an example, it is easy to preserve confidentiality of information simply by setting some limitation on accessibility of the information. However, this is not appropriate, because it does not meet the requirement of availability for proper access. Therefore, there should be a balance between confidentiality and availability, (Pfleeger et al., 2004). Furthermore, new security functions have been identified and added to improve the performance of information system including legal aspects. The Accountability is the most important newly developed goal. All security objectives could be described into the three classical CIA terms. The new goal, the accountability might be expressed as integrity (non-repudiation) of the data identifier of the sender or recipient for any transaction. Note that the four goals are different in nature: confidentiality and integrity are mainly concern about data; availability is primary associated with computer systems and secondarily with the data, while accountability is used to link the subjects (user or application) with the data. Accountability has an important role in e-business (Knorr et al., 2001) and other supply chain transactions. Hence, its integration with CIA enhances the focus of this research, which will be noted as CIAA.

Only when the system is vulnerable then, the attacker may start his attack. The vulnerabilities are cracks or weak points in information systems which avert achieving one or more of the three security objectives in CIAA. The system's hardware, software, and information are the three main resources subject to vulnerabilities; also, vulnerabilities could occur due to human errors or behaviors. (Pfleeger et al., 2004).

The potential elements in information systems that are exposed to attacks are outlined by Denning, 1999 as:

- Containers (stores of data): computers and human memories.
- Transporters (conveyors of data): humans, telecommunication systems.
- Sensors (input devices to the system): scanners, cameras, microphones, human senses.
- Recorders (output devices from the system): disk writers, printers, human processes.
- Processors (manipulators of data): microprocessors, humans, software.

To prevent attacks and/or decrease their effect, several methods are used. First, to protect against harm and close the vulnerability or both, the system could

neutralize the threat instantly. Second, less powerful methods could only alert the security manager that the security has been compromised, by detecting a breach as it happens or after it occurs immediately. There is a wide range of different security levels in between these two. However, the security could be embedded in the control systems for preserving confidentiality, integrity, and availability. In general the possibility for harm could occur and it is called security risk. The defense against harm could be in several forms as described by Pfleeger et al. (2004):

- Prevent it, by blocking the attack or closing the vulnerability.
- Deter it, by making the attack harder, but not impossible.
- Deflect it, by making another target more attractive (or this one less so).
- Detect it, either as it happens or some time after the fact.
- Recover from its effects.

Security vulnerabilities are cracks or weak points in a system which when exploited by an attacker may affect one or more of the three security goals of the CIA security model. Only when the system is vulnerable then, the attacker may launch an attack. In addition to the system's hardware, software, and information as the main resources subject to vulnerabilities; also, humans may be vulnerable in a system (Pfleeger et al., 2004). Vulnerability management (VM) is gathering all knowledge that could be used by a threat source to cause losses to an organization. Threat management (TM) is the practice of stopping threats before they cause any losses (Ahlm, 2006). Combining the two models VM and TM in practice creates an interoperation between a number of technologies that all need to share knowledge with each other. The Laws of Vulnerabilities can improve vulnerability management, helping chief information officer, CIO, chief security officers, CSO, network and IT managers, and security specialists to strengthen and prioritize the protection of internal and external networks. The following are best practices for Vulnerability Management which have been driven from the trends identified in the ‘‘Laws of Vulnerabilities’’ (Eschelbeck, 2005):

1. Classify is the process to identify and categorize all network resources. This classification should categories resources into a hierarchy of assets by their value to the business. Hence, Critical assets should be audited every 5 to 10 days to identify vulnerabilities and protect against exploits.

2. Prioritize remediation efforts based on the asset classification and severity of vulnerabilities.
3. Integrate security technologies with vulnerability management to improve effectiveness. Also report operational progress against vulnerability goals to raise the level of awareness for security within the executive security management team.
4. Measure networks vulnerabilities and track the percentage of vulnerabilities mitigated within a period of time. Then, chart the security team's performance to make sure the end result is risk reduction, especially to critical assets.
5. Audit the results of vulnerability scans to understand a corporation's network security position. Use metrics to evaluate successes and failures of different security policies to improve security performance, and report security status to senior management.

The main tool for VM is the vulnerability scanners. Vulnerability scanners gather data over the network about the known vulnerabilities on operating systems and applications. Next are tools that deal with uncovered system vulnerabilities, which are known as patch management systems. Finally, auditing and compliance reporting tools are used to complete the VM tool kit. Threat management (TM) systems contain a tool kit designed to stop attacks. First, firewall is the main device of TM. Then, intrusion detection system (IDS) assists firewall's administrators to understand incoming attacks, and to configure the firewall well. On the host side, products like personal firewall and anti-virus are considered as TM tools. The problem with traditional methods of dealing with security threats is the lack of knowledge and information sharing and tools that do not automatically inter-operate (Ahlm, 2006).

1.3 Information Security Measurement

Standards of measurement started over 300 years ago to facilitate international trade and communication. Today, measurements are required to gain higher quality in many fields due to the increasing of society's technology and civilization. A hot example in this field is measuring information security (ESPIRIA, 2004). As a result of this, the level of complexity of information security solutions has improved along with their surrounding processes and practices. Consequently, the field of information security measurement and common standards has started to emerge. Today, it is difficult for an organization to answer a basic questions like "how secure are we?" or

"how secure do we need to be?" with precision value (ESPIRIA, 2004). We can see the importance of information security measurement to:

- Have an effective security management.
- Enable the establishment of security objectives and goals.
- Know the level of progress, or when we have reached our goal.
- Develop security program strategies and plans.
- Comparison of results across organizations by a standards-based measurement approach, which is essential in identifying security gaps and prioritizing security program initiatives.

However, gaining a true measurement of security program status for an organization can be complex and involves the following (ESPIRIA, 2004):

- Understanding the organization's business, risks, and infrastructure.
- Determining the process, technology, and people associated with security.
- Identifying the unique groups or parts of the organization requiring individual security measurements.
- Selecting the most appropriate standard of measurement.

One of the fundamental issues in security measurement is selection of the appropriate "standard" as the measurement tool. A number of standards have emerged to assist management for evaluating security program strength. The ISO 17799 standard has emerged as one of the leading security program and management choices. Measurement requires selecting the appropriate standard(s) and evaluating security program status against the security policy. Benchmarking, comparisons across business units and comparing results over time are useful methods in security program management. In many cases, more than one measurement is required due to unique risks or significantly different security processes and implementations across business units. More than one measurement may be required within a single business unit if multiple platforms exist with different security processes (ESPIRIA, 2004).

1.4 Supply Chain Information Security

Kolluru et al., 2001a presented a multi-level supply chain collaboration framework. In addition, Kolluru et al., 2001b suggested different levels of security required at these different levels of collaboration. In level-1 partnerships with their trading partners are engaged in minimal relationships, enabled by asynchronies one-way data push communication. In level-2 the communication architecture is more

mature because of the higher level of collaboration between the enterprise partners. The communication at this level is push and pull, asynchronies and synchronies, point-to-point client-server communication. As a result, additional security threats and vulnerabilities are taking place. Finally, in level-3 the communication architecture is a strategic collaboration within the extended enterprise. Additional security threats in this distributed n-tier environment include the same security threats as level-2, applicable in a distributed peer-to-peer network. The common security goals between the 3 levels are confidentiality, integrity, and non-repudiation or Accountability.

In general the security processes among supply chain drivers are the same. Each supply chain driver has essential information security requirements within the driver and related to other drivers in the supply chain. Information should be available and accurate to all users. Each driver should have an access to specifications and quantities of a product, lead time, source and destination of shipping, method of payment and, other relevant information depending on the supply chain driver's role. This is essential to integrate the processes and reduce the barrier among all drivers. An attacker could be an insider, outsider, or competitors. In any case, the attacker's objective is to exploit the vulnerability of shared information among the supply chain drivers. Hutchinson, 2002 stated that the attacker can use many techniques; such as manipulating, intercepting, disrupting information, making it unavailable, or exposing it to others. The attacker could use differences of security levels to attack supply chain drivers through the driver with low security. "The strength of the chain is the strength of its weakest link" and as stated in the first principle of security "a system is most vulnerable at its weakest point" (Pfleeger et al., 2004).

For example the attacker can pretend to be a customer enters to the web site of a retailer and set up an order with different amounts trying to know the level of inventory available with the retailer. Hence the attacker can use this information to set a large order to have an estimate of the lead time for both the retailer and the manufacturer, and so on. Another example DoS attack where the customer can not access to the information and can not set any order, which cuts down business and may cause customers loss, and so on. From the pervious view, information security is needed for all the supply chain drivers in order to protect themselves and their partners from attacks. In general for both, the supply chain drivers and the attacker, security goals are confidentiality, integrity, availability and accountability, with a

varying level of importance and significance. The most common attack methods on SCM currently available include (Warren et al., 2000):

- Password sniffing/cracking software, one method is by using software packages to access a system via a file transfer protocol (FTP) port and trying to determine password files. Another method is to use software that systematically uses a combination of passwords until success. This attack could damage an organization's SCM function. The unauthorized access to the supply chain network could allow the hacker to; delete; change data relating to orders; pricing; product description; or serving a competitor.
- Spoofing attacks works by faking a message with false address so that the message appears to have originated from somewhere other than its actual source. The false address is trusted by receiving host so that the message will be accepted and executed. This could allow an intruder to penetrate right through a firewall (Denning, 1999). Another type of spoofing is "Web spoofing". This is where an attacker sets up a fake Web site to fool users to steal their credit card numbers or other information. As an example, pretending the hacker's web site as an official supplier. Therefore, the user would disclose information relating his password, customer number, order details, credit cards details, etc. most likely, these information could be used later to access the official supplier on-line service and the hacker will pretend to be a customer and make false orders or they could use the credit card details in other activities. One way to overcome this attack is to use authentication software between the user and the server. Other way is the use of "digital signatures".
- Denial of service (DoS) results when access to a computer or network resource is intentionally blocked as a result of malicious action taken by another user, which purposely compromise the availability of the resources (Howard, 1997). DoS is a very effective attack against an Internet-based company. These types of attacks disrupt the on-line services used with the SCM process. DoS can be enforced by crashing the system, so suppliers cannot access the on-line service. Other way is to send a lot of false e-mail messages to an organization, so it would take hours to delete them and determine which messages are the valid messages.
- Direct attack: A direct attack would take the form of hacking into a computer system and rewriting or stealing information. This would have a great impact on organizations offering on-line services, since these on-line services could be damaged,

modified or destroyed. Another problem is that if the organization were not able to determine where the security risk lies, the direct attacks would be re-occurring. The impact of these attacks would be to publicize the hackers and destroy the trustworthiness of the organization offering the on-line services, especially to current and future customers. Another method of hacking is more concerned with attacking computer files and destroying, modifying or extracting data. These types of hacking attacks may be less apparent to organizations, as they may not realize they have been a victim. Hackers would use direct hacking as an extensive part of their ``attack strategy'' against e-commerce and SCM. By hacking Web sites they will gain a global audience for their actions and they will also be able to damage the reputation of the companies' security and the on-line services. These types of attacks could damage an organization's SCM functionality in a number of ways. Suppliers would not be able to access the on-line system until it is restored. However, the biggest impact is the adverse publicity caused for the organization targeted. Also, it could affect existing customer confidence in the system and reduce the number of future prospective customers.

1.5 Summary

Information security of the supply chain management (SCM) is essential and covers a wide scope of organizations. The performance of information security could be achieved through interactions and smooth flows of information from suppliers to customers. Information sharing is an important factor of cooperation in supply chain management. Information security addresses three very important goals related to information system; confidentiality; integrity; and availability. Security vulnerabilities are cracks or weak points in a system which when exploited by an attacker may affect one or more of the security goals of the CIA model. Measuring information security leads to an effective security management. It enables the establishment of security objectives and goals, and helps to develop security program strategies and plans. Measurement requires selecting the appropriate standard(s) and evaluating security program status against the security criteria.

In general the security processes among supply chain drivers are the same. Each supply chain driver has essential information security requirements within the driver and related to other drivers in the supply chain. The attacker could use differences of security levels to attack supply chain drivers through the driver with

low security. The presence of criminals, terrorists, competitors, state security services, and malicious or curious individuals makes the i-war (information war) threat to organizations a real one (Hutchinson, 2002). Information security of the supply chain management (SCM) is essential and covers a wide scope of organizations. However, the main challenge in supply chain management is information integration, security and attacks that could penetrate more than one driver in the supply chain system.

CHAPTER 2

2. LITERATURE REVIEW

Strategic advantage has gained by controlling supply chains effectively (Ayers, 1999). Well managed supply chains can reduce costs, compress delivery times and reduce irregularity (Beesley, 1996). Hence, Control of supply chain requires extensive investments in information technology (IT). As an example; Enterprises resource planning (ERP) systems integrate information from various departments in a company including production, marketing, finance, purchasing, and accounting. In addition, companies are communicating electronically with suppliers and buyers who have common information systems platforms (Szygenda, 1999). Many organizations and many nations confirm that they have a leading edge only because of their advanced information system (IS) for their business and communications (Clarke et al., 2000). Literatures in modern supply chain are emphasizing on the importance of forming collaborative strategic partnerships among supply chain drivers. The Collaborative Planning, Forecasting and Replenishment (CPFR) process model proposed by the Voluntary Inter-industry Commerce Standards (VICS) Association is based on the widely-accepted statement that businesses will attain long-term cost reduction by forming closer working relationship with select suppliers and customers (CPFR, 2001). Closer or long-term collaboration, among supply chain drivers are enabled through seamless integration and transfer of information up and down the chain. The common usage of the internet had removed the barriers of entry to small and medium enterprises. Increasingly the internet is gaining acceptance as a mechanism for process integration through exchange of business information among supply chain drivers and partners (Lee et al., 1999). Kolluru et al., 2001b had presented an overview of the security architecture issues related to supply chain management. They proposed a three-level classification that is intended to serve as an outline for supply chain partners which can be used to identify ``where'' they belong on the spectrum of collaborative partnerships, and what security level do they need as they advance to higher levels of integration with their supply chains.

In the information era, the use of technology as a means of communication, data storage, and presentation has exposed us to a level of data management and security not experienced before (Hutchinson, 2002). The expansion of the internet and e-mail increased the vulnerability to various types of attacks (Blaise et al., 1999).

Information system with connection to public networks remain vulnerable to various attacks within inside and outside of the organizations (Goan, 1999). Messmer, 1999 defined Information warfare (i-war) as a nation's rigorous use of network hacking, denial-of-service (DoS) attacks, or computer viruses. These techniques are used to gain access or disrupt computer network having applications such as banking, telecommunication and commerce. The presence of criminals, terrorists, competitors, state security services, and malicious or curious individuals makes the i-war threat to organizations a real one (Hutchinson, 2002). Organizations efficiency and effectiveness has drastically improved with the growth of networked, multinational organizations and e-commerce institutions worldwide. Organizations Depend more and more on these networks for day-to-day operations. So, dramatic negative effects are expected in the case of any disruption in their operations by an attack on their information system (Sharam et al., 2002).

In a survey of IT managers in Australia (Hutchinson et al., 1999), 66% thought there was no threat from competitors in this area. This trusting attitude is probably resulted from a positive view to their competitors' intentions, a lack of knowledge of IT attack techniques and a narrow definition of "competitor" (Hutchinson, 2002). So, the definition of a competitor should be an entity that wishes to decrease your share of the market, or obtain the same resources your organization wants. However, other research has shown within Australia that the main concern of the users is security in the electronic commerce applications (DIST, 1998). As a result; direct attacks on SCM systems not only cause initial damage, but more extensively could destroy customer confidence and trust in e-commerce systems.

The overall performance of information security of SCM agents could be improved drastically by adopting suitable security standards. There are many international standards published to deal with information security and its management. The most common standards used in drafting standard-based security policies are ISO17799: 2002 and BS7799, which was updated and replaced by ISO27001:2005 on Oct. 15th 2005. Several tools, such as Callio Secura 17799, are currently available in the market to help companies implement the BS7799 / ISO17799 standards and develop security policies. Consistent measurement using a standards-based approach is the foundation of a well-built security management and control. Historically, security measurement has been "soft" with a lack of accepted standards. Over the past 12-24 months, standards have improved and security

measurement has become more quantitative and effective (ESPIRIA, 2004). Appropriate security management tools bring together a sound methodology, questionnaires, an informational guide and all of the techniques needed to develop an information security management system and accelerate its implementation into multi agent or among supply chain drivers. Security standards could be used to develop measurable values for the security goals; confidentiality, integrity, availability (CIA), and to assess these values when collected. Hence, these values can be used for building a quantitative model for security.

Schechter et al., 2003 relies on the assumption that system security can be measured by cost to acquire a means of breaking into a system. They have introduced a model for estimating the value of a system exploit to outside serial or parallel thieves. There model takes into account investments in intrusion detection and response, both internally and by outside monitoring firms. Schechter et al., 2003 proposed that using the model by an organization can measure its attractiveness to outside thieves and determine how much security is required in the packaged systems purchases. Also it can be used to evaluate the effectiveness of stopping attacks by analyzing the social aspects of intrusion detection and response strategies, such as information sharing.

MacLeod et al., 2000 presented a new method to achieve information sharing coordination by the use of an Information Protection Coordination Center (IPCC). The IPCC provides coordination services to a network comprised of all networks under control of the Information Protection Centers (IPCs). Hence, it creates a Single Virtual Enterprise Network (SVEN) security model. They demonstrated the IPC/IPCC layered security concept that could provide a component of survivable systems. It provides a trusted form of vulnerability prediction to allow the enterprise system to take proactive preventive steps to ensure continuation of service before a vulnerability is exploited. MacLeod et al., 2000, also, stated that the active security cycle is to; prevent, detect, respond, and recover. This cycle provides a methodology to help in effective incident response, the IPCC concept extends this by providing good technical information on time to the system administrators and operators. The initial compromise of any node in the SVEN model triggers a real time response in other nodes. Thus, the amount of the system that has to enter the recover state will be minimized. The SVEN model accepts the fact that individual systems will be compromised despite the best security practices of its designer, administrators and

users. With real time communications among systems, the spread of the compromise can be significantly limited.

Traditionally, Security has not been expressed quantitatively. Instead, security evaluation was based on the classes of various Security Evaluation Criteria, such as NIST:1992, ITSEC, and "Orange book" (Jonsson et al., 1997). Ortalo et al., 1999 are the pioneers in using a quantitative analysis approach of attacker behavior based on empirical data collected from intrusion experiments. They divided the attacker's behavior into three different phases: the learning phase, the standard attack phase, and the innovation phase. The probability for successful attacks is shown to be considerably higher in the standard attack phase. Trivedi, 2001 introduced a stochastic model by using Markov chain to obtain a steady state. The model allows obtaining the mean time to security failure by evaluating the proposed measure of operating security. Wang et al., 2002 considers that the attacker could arrive at a random time, just as a failure may occur randomly. Also, he used a Markov process to estimate the amount of time or effort that an attacker has to spend in injecting an attack. This could be modeled as a random variable that can be described by choosing Poisson distribution functions. Madan et al., 2004 developed a quantitative security model by using semi-Markov model for an intrusion tolerant system. They initiated security attributes for intrusion by applying a quantitative model. The model was tested and run for steady-state behavior leading to measures like mean time to security failure, (MTSF). Madan et al., 2004 used the steady-state to find the probabilities for confidentiality, integrity, availability and the value of absorbing states representing the MTSF. Lambrinoudakis et al., 2005 presented a probabilistic structure, in the form of a Markov model. The model provides detailed information about all possible transitions of the system in the course of time. Lambrinoudakis et al., 2005 stated that the probabilistic structure enables both the estimation of the insurance premium and the evaluation of the security investment. To test the value of security, the system environment, the situations of attack, and the requirements of success need to be created and simulated in order to demonstrate how the security system operates and how it will produce results comparing with security goals (Ahlm, 2006). The traditional approach of this problem is to combine the efforts of vulnerability management (VM) practice with a threat management (TM) practice (Ahlm, 2006).

CHAPTER 3

3. PROPOSED MODEL

This chapter will present an overview of stochastic modeling using Markov chain process and the methods used to find steady-state probabilities of a security system. The proposed model in this research is based on a modified model of the state transition diagram for intrusion tolerant system (Madan et al. 2004). The modified model focuses on the probabilities of attacking the security goals (CIAA) and the relation between these goals. Next, the chapter will introduce the information security model in details with definition of each state and what it reflects in real information systems. Then, an enhanced security model with deflection tool will be covered. The coverage will include a suggested deflection tool, honey-pot, and what effect it will have on improving security. Finally, the chapter will show how the security model can be used in SCM to improve information sharing and security among the supply chain drivers.

3.1 Markov Chain Stochastic Modeling

Attackers behave in an unpredictable and random nature which represents a stochastic process. The security model developed in this research is based on stochastic processes. A stochastic process is an evolution model where the systems are either exhibiting inherent randomness, or operating in an unpredictable environment. This unpredictable behavior of attackers might be in more than one form. The Semi-Markov chain process is considered to be an appropriate modeling tool to illustrate the behavior of attackers. Markov chains have a special property that, the probability of any event moving to future state depends only on the present state; hence it is independent of past events. Attacker's process fits well this description, so Markov chains provide an important kind of probabilistic model for attackers.

The conditional probability of any future event given any past events is independent of the past events and depends only upon the present state. Let the present state denotes to $X_t = i$, then the future state will be $X_{t+1} = i + 1$, and the past state is $X_{t-1} = i - 1$. Conveying these states to conditional probabilities become $P\{X_{t+1} = i + 1 \mid X_t = i\}$ for a Markov chain are called (one-step) transition probabilities. The n-step transition probabilities $p_{ij}^{(n)}$ is the conditional probability

that the system will be in state $j = i + 1$ (future state) after exactly n steps, given that it starts in state i at any time *t*, is $p_{ij} = P\{X_{t+1} = j \mid X_t = i\}$, and for n transition steps is $p_{ij}^{(n)} = P\{X_{t+n} = j \mid X_t = i\}$, (Hillier et al., 2005).

Because the $p_{ij}^{(n)}$ are conditional probabilities, they must be positive, and since the process must make a transition into some state, they must satisfy the properties $p_{ij}^{(n)} \geq 0$, for all i and j; and $\sum_{j=0}^{N} p_{ij}^{(n)} = 1$, for all i; $n = 0, 1, 2 \ldots, M$

The matrix form is

$$P^{(n)} = \begin{array}{c} \\ 0 \\ 1 \\ \vdots \\ M \end{array} \begin{array}{c} \begin{array}{cccc} State & 0 & 1 & \cdots & M \end{array} \\ \begin{bmatrix} p_{00}^{(n)} & p_{01}^{(n)} & \cdots & p_{0M}^{(n)} \\ p_{10}^{(n)} & p_{11}^{(n)} & \cdots & p_{1M}^{(n)} \\ \cdots & \cdots & \cdots & \cdots \\ p_{N0}^{(n)} & p_{N1}^{(n)} & \cdots & p_{MM}^{(n)} \end{bmatrix} \end{array}$$

The transition starts from a particular row state to any column state. However, Chapman-Kolmogorov Equations could be used to solve this type of problem and find the steady-state transition probabilities. CK-equations are method for computing the n-step transition probability $p_{ij}^{(n)}$.

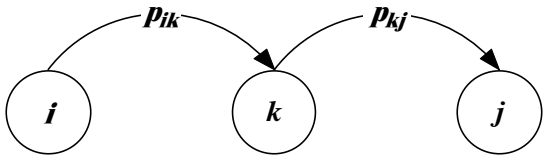


Figure 2 State Transition

$p_{ij}^{(n)} = \sum_{k=0}^{M} p_{ik}^{(m)} p_{kj}^{(n-m)}$, for all states i and j. These expressions enable the n-step transition probabilities to be obtained from the one-step transition probabilities recursively. For $n = 2$

$p_{ij}^{(2)} = \sum_{k=0}^{M} p_{ik} p_{jk}$, for all states i and j, where the $p_{ij}^{(2)}$ are the elements of matrix $P^{(2)}$.

$P^{(2)} = P \bullet P = P^2$.

In the same manner, the above expression for $p_{ij}^{(n)} = P^n$.

Other way to find the steady-state probabilities π_i is to solve the steady-state equations

$$\pi_j = \sum_{i=0}^{M} \pi_j p_{ij} \text{ ,for } j = 0, 1, \ldots, M$$

$$\sum_{j=0}^{M} \pi_j = 1$$

Steady-state probability means that the probability of finding the process in a certain state, j, after a large number of transitions tends to the value π_j, independent of the probability distribution of the initial state. On the other hand, the process continues to make transition from state to state at any time and any step n with the same transition probability p_{ij}, so the process does not settles down into one state (Hillier et al., 2005).

3.2 Information Security Model

The structure of a generic model for the security of any driver in the SCM is shown Figure 3, which is the modification of the state transition diagram for intrusion tolerant system (Madan et al. 2004). The eight states of the security system are indicated in Figure 3. The numbering in the model is only for notation, and does not imply the process sequence. The security system starts in the normal state (0), where the system is working in a secure mode or with no threat. Assuming vulnerability is found then the system moves to state 1. However, the system could be fixed and then returns to normal condition, state 0. On the other hand, the vulnerability could be exploited by an attacker leading the system to state 2. Depending on the level of the attacker and the type of the vulnerability, the attacker may attack one of the security goals, confidentiality, integrity, availability or accountability (CIAA). There are five possibilities to move out from state 2. First, the system could stop the attack at an early stage and return back to the normal state (state 0), with minimal loss in security. Second, the attacker may infiltrate the confidentiality of the system and move to state 3. From state 3, other security goals could be attacked as well, such as integrity, availability and accountability moving to states 4, 5, and 6 respectively.

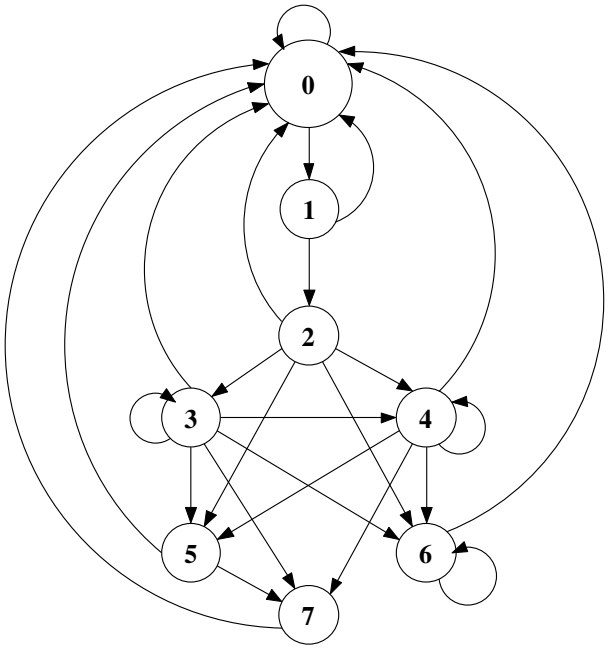


Figure 3 Security State Diagram of a Driver under Attack

Third, the attacker may alter the integrity of the system, state 4, where the attacker's goal is to change, delete, or add information. Also, from state 4 the attacker can attack the other two security goals; availability or accountability. Fourth, is the scenario of moving to state 5 by attacking the availability of the system, where the attacker would cause denial of service (DoS) for all users. In this case, the system incurs big losses with no further attacks and with the possibility of a total system failure by moving to state 7. Fifth, in state 6, the attacker falsifies the accountability to make it ineffective or inaccurate. In this case, there is no harm to the other states, but it has a considerable effect on the system security. Finally, state 7 is a total failure of the system. From all the states, the system can return back to state 0, the normal state, with different level of probability and with different degrees of loss.

P in Matrix 1 is a matrix formulation of the relation between the states and their probability. Driver information security may have at least the following security devices; blockers such as firewalls, intrusion detection systems, and deflectors such as honey-pot. The firewall acts as a gate controller. It consists of hardware and/or software that use access lists to distinguish between the authorized and unauthorized Uses. An intrusion detection system is a device that is placed inside a protected network to monitor what occurs within the network. An intrusion detection system

offers the opportunity to enhance the system protection from attackers' ability to penetrate through the firewall or other security devices by giving more information about attacks. In additions, honey-pots can be used as deflectors for developed scenarios. A honey-pot is one of the most powerful defense techniques used to deflect attackers. The honey-pot is a security resource that does not perform any production or functional activity. It mimics the real information network and makes it very simple to attack.

$$P = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{array} \begin{array}{c} \begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\ \begin{bmatrix} \bar{p}_0 & p_{01} & 0 & 0 & 0 & 0 & 0 & 0 \\ \bar{p}_1 & 0 & p_{12} & 0 & 0 & 0 & 0 & 0 \\ \bar{p}_2 & 0 & 0 & p_{23} & p_{24} & p_{25} & p_{26} & 0 \\ \bar{p}_3 & 0 & 0 & p_{33} & p_{34} & p_{35} & p_{36} & p_{37} \\ \bar{p}_4 & 0 & 0 & 0 & p_{44} & p_{45} & p_{46} & p_{47} \\ \bar{p}_5 & 0 & 0 & 0 & 0 & 0 & 0 & p_{57} \\ \bar{p}_6 & 0 & 0 & 0 & 0 & 0 & p_{66} & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}, \text{ where, } \begin{array}{l} p_{01} + \bar{p}_0 = 1 \\ p_{12} + \bar{p}_1 = 1 \\ p_{23} + p_{24} + p_{25} + p_{26} + \bar{p}_2 = 1 \\ p_{33} + p_{34} + p_{35} + p_{36} + p_{37} + \bar{p}_3 = 1 \\ p_{44} + p_{45} + p_{46} + p_{47} + \bar{p}_4 = 1 \\ p_{57} + \bar{p}_5 = 1 \\ p_{66} + \bar{p}_6 = 1 \end{array}$$

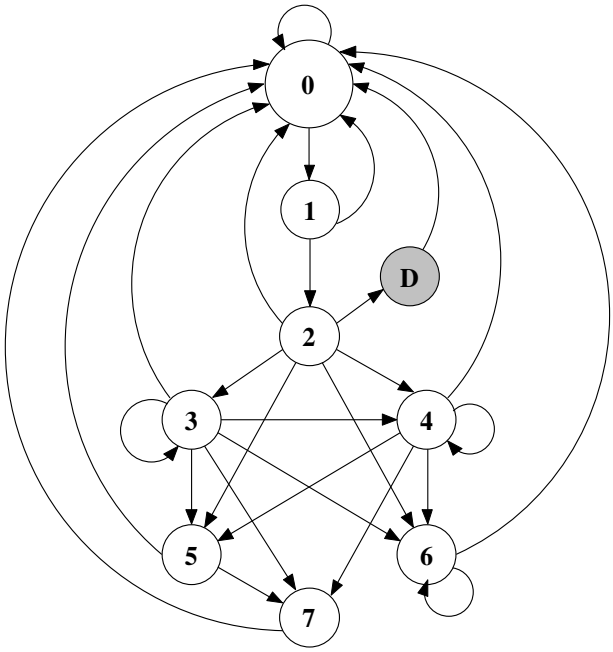
Matrix 1 Security State Matrix

The design of honey-pot's enhanced by the simplicity and anticipation to compromise the real information network. The traffic going to or from the real information network will be reduced by deflecting and trapping the attackers into a honey-pot. Any time a connection is sent to the honey-pot, it is most likely to be a probe, scan, or even identify the attacker. Hence, useful data about the attackers could be collected by a honey-pot. This information could be used to extract the intrusion detection signature, as stated in (Urjita et al., 2005).

A honey-pot is used mainly for the following reasons as suggested in Pfleeger et al., 2004:

- To watch what attackers do, in order to learn about new types of attacks.
- To trap an attacker in place to learn enough, to identify and stop the attacker
- To provide an attractive but diversionary playground, hoping that the attacker will leave the real system alone

The protection may take place at the beginning, during the progress, or after the attack has occurred. An Intrusion Detection System (IDS) activates an alarm, which can activate defensive action.



0 Normal state
1 Vulnerability found
2 Attack start
D Deflect
3 Attack Confidentiality
4 Attack Integrity
5 Attack Availability
6 Attack Accountability
7 Failure

Figure 4 Security State Diagram with Deflection

Deflection is presented as a state in the security state diagram, where the attacker in state 2; the attack state, can be deflected to the deflection state which take the system to the normal state, state 0, and prevent the attack on the security states. The model assumes that the attacker can be deflected in the beginning of the attack only, but in the case of attacking other security goals the attacker can not be deflected. As is the attacker could by bass the deflection tool. The security state diagram with the added deflection state is shown in Figure 4, followed by the matrix presentation of the state probabilities.

$$P = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ \boldsymbol{D} \end{array} \begin{array}{c} \begin{array}{ccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & \boldsymbol{D} \end{array} \\ \begin{bmatrix} p_{00} & p_{01} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \overline{p}_1 & 0 & p_{12} & 0 & 0 & 0 & 0 & 0 & 0 \\ \overline{p}_2 & 0 & 0 & p_{23} & p_{24} & p_{25} & p_{26} & 0 & p_{2D} \\ \overline{p}_3 & 0 & 0 & p_{33} & p_{34} & p_{35} & p_{36} & p_{37} & 0 \\ \overline{p}_4 & 0 & 0 & 0 & p_{44} & p_{45} & p_{46} & p_{47} & 0 \\ \overline{p}_5 & 0 & 0 & 0 & 0 & 0 & 0 & p_{57} & 0 \\ \overline{p}_6 & 0 & 0 & 0 & 0 & 0 & p_{66} & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

Matrix 2 Security State Matrix with Deflection

where,

$$p_{00} + p_{01} = 1$$
$$p_{12} + \bar{p}_1 = 1$$
$$p_{23} + p_{24} + p_{25} + p_{26} + p_{2D} + \bar{p}_2 = 1$$
$$p_{33} + p_{34} + p_{35} + p_{36} + p_{37} + \bar{p}_3 = 1$$
$$p_{44} + p_{45} + p_{46} + p_{47} + \bar{p}_4 = 1$$
$$p_{57} + \bar{p}_5 = 1$$
$$p_{66} + \bar{p}_6 = 1$$

This security model is useful for an organization of single or multi drivers. Organization's historical data can be used to measure the CIAA, and could be used to estimate the level of attack and run the model in order to get the steady state of system security. The organization can claim its level of security and study the processes of improving it.

3.3 Security Analysis of Supply Chain

The security of supply chain management is an application which concerns a variety of decisions about the interactions and security of several drivers. The steady state probabilities of supply chain management could be developed by generating an individual Markov chain for each driver. The proposed probabilities for attacking CIAA (p_C, p_I, p_A, p_{Acc}) for each driver are depending on its mission as shown in Table 1. In addition, each driver has given different level of vulnerability (p_V). As will as, different values for attacking CIAA assigned for four drivers to implement and test the security model on the SCM drivers. The SCM consists of four drivers. Driver 1, supplier, concerned more with confidentiality and integrity, so high weights are given to both (p_C = 0.30/0.60 and p_I = 0.20/0.60). Driver 2, manufacturer, also is concerned more with confidentiality and integrity, therefore, a very high value is assigned for (p_C = p_I = 0.20/0.50). Driver 3, retailer, is concerned more with availability, therefore a high value of p_A = 0.20/0.40 is assigned. Finally, driver 4, customer, has a very high confidentiality and accountability requirement, therefore high (p_C = 0.3/0.70 and p_{Acc} = 0.20/0.70) are assigned. However, the reader can use this model for more drivers and use corresponding CIAA data. Next step to develop a generic transition matrix GTM for each driver (i) created by substituting the parameters of p_C, p_I, p_A, p_{Acc} from Table 1.

Transition probabilities notation and assumptions:

0. Normal state ;
1. Vulnerability is found p_V
2. Attack is started, $p_{attack} = p_{12} = \{0.05, 0.20, 0.35, 0.50, 0.65, 0.80, 0.95\}$
3. Attack on Confidentiality, $p_C = p_{23} = p_{33}$
4. Attack on Integrity, $p_I = p_{24} = p_{34} = p_{44}$
5. Attack on Availability, $p_A = p_{25} = p_{35} = p_{45}$
6. Attack on Accountability, $p_{Acc} = p_{26} = p_{36} = p_{46} = p_{66}$
7. Failure, $p_F = p_{37} = p_{47} = p_{57} = 0.10$

The notation p_{12} is read as the probability of moving from state 1 to state, as indicated in the diagram in Figure 3.

Table 1

Proposed CIAA for SCM

SCM Drivers	p_V	p_C	p_I	p_A	p_{Acc}	$\bar{p}_{CIAA}$
Driver 1 - Suppliers	0.25	0.30	0.20	0.05	0.05	0.40
Driver 2 - Manufacturer	0.15	0.20	0.20	0.05	0.05	0.50
Driver 3 - Retailers	0.10	0.05	0.05	0.20	0.10	0.60
Driver 4 - Customers	0.30	0.30	0.15	0.05	0.20	0.30

The following steps are used to develop the study state security for SCM drivers:

1. Develop 4 matrices of GTM for each driver.
2. Use GTM for each driver at seven attack levels (0.05, 0.20, 0.35, 0.50, 0.65, 0.80, 0.95)
3. Solve for the steady state probabilities (SSP) for individual drivers.
4. Find the system wide SW security by multiply each driver's GTM to get the SW transition Matrix.
5. Run the SW transition matrix to get the study state for the SCM system as a security unit.

Table 2

Generic Transition Matrix (GTM) for Driver i

From \ To	N (0)	V (1)	Att (2)	C (3)	I (4)	A (5)	Acc (6)	F (7)
(0)	p_{00}	p_{01}	0	0	0	0	0	0
(1)	p_{10}	0	p_{12}	0	0	0	0	0
(2)	p_{20}	0	0	p_{23}	p_{24}	p_{25}	p_{26}	0
(3)	p_{30}	0	0	p_{33}	p_{34}	p_{35}	p_{36}	p_{37}
(4)	p_{40}	0	0	0	p_{44}	p_{45}	p_{46}	p_{47}
(5)	p_{50}	0	0	0	0	0	0	p_{57}
(6)	p_{60}	0	0	0	0	0	p_{66}	0
(7)	1	0	0	0	0	0	0	0

The steady states of SCM system can be achieved by multiplying the matrices of all drivers. The steady states probability of SCM system, system security, π_S and CIAA could be calculated using the following relationships:

Security $\pi_S = \pi_0 + \pi_1$; confidentiality $\pi_C = 1 - \pi_3$; integrity $\pi_I = 1 - \pi_4$; availability $\pi_A = 1 - (\pi_5 + \pi_7)$; and accountability $\pi_{Acc} = 1 - \pi_6$.

Table 3

Initial Transition Matrix for Driver 1, P_{d1} at Attack Level of 0.05

From \ To	N (0)	V (1)	Att (2)	C (3)	I (4)	A (5)	Acc (6)	F (7)
(0)	0.75	0.25	0	0	0	0	0	0
(1)	0.95	0	0.05	0	0	0	0	0
(2)	0.40	0	0	0.30	0.20	0.05	0.05	0
(3)	0.30	0	0	0.30	0.20	0.05	0.05	0.10
(4)	0.60	0	0	0	0.20	0.05	0.05	0.10
(5)	0.90	0	0	0	0	0	0	0.10
(6)	0.95	0	0	0	0	0	0.05	0
(7)	1.00	0	0	0	0	0	0	0

Table 3 presents an initial transition matrix for driver 1 (P_{d1}). Table 3 is generated by substituting the values of p_C, p_I, p_A, p_{Acc} from Table 1 to obtain the general transition matrix (GTM) for driver 1 using the probability of 0.05 for level of attack.

Table 4

Transition Matrix for Driver 1, $\boldsymbol{P}_{d1}^{2}$ At Attack Level of 0.05

From \ To	N (0)	V (1)	Att (2)	C (3)	I (4)	A (5)	Acc (6)	F (7)
(0)	0.8000	0.1875	0.0125	0.0000	0.0000	0.0000	0.0000	0.0000
(1)	0.7325	0.2375	0.0000	0.0150	0.0100	0.0025	0.0025	0.0000
(2)	0.6025	0.1000	0.0000	0.0900	0.1000	0.0250	0.0275	0.0550
(3)	0.6275	0.0750	0.0000	0.0900	0.1000	0.0250	0.0275	0.0550
(4)	0.7625	0.1500	0.0000	0.0000	0.0400	0.0100	0.0125	0.0250
(5)	0.7750	0.2250	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
(6)	0.7600	0.2375	0.0000	0.0000	0.0000	0.0000	0.0025	0.0000
(7)	0.7500	0.2500	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

Table 4 shows the second transition matrix that was obtained by raising the initial transition matrix to power 2 ($\boldsymbol{P}_{d1}^{2}$). Table **5** shows the steady state of driver 1 with an attack level of 5%. MATLAB Excel Link has been used to reach steady-state matrix $(SSM)_i$ by obtaining the outcome matrix $\boldsymbol{P}_{d1}^{n}$. The steady state is reached when the values under all columns corresponding to each state (N, V, Att, C, I, A, Acc, F) are identical, hence indicating reaching a steady-state.

Table 5

Steady-State Matrix for Driver 1, $\boldsymbol{P}_{d1}^{n}$ At Attack Level of 0.05

From \ To	N (0)	V (1)	Att (2)	C (3)	I (4)	A (5)	Acc (6)	F (7)
(0)	0.7839	0.1960	0.0098	0.0042	0.0035	0.0009	0.0009	0.0009
(1)	0.7839	0.1960	0.0098	0.0042	0.0035	0.0009	0.0009	0.0009
(2)	0.7839	0.1960	0.0098	0.0042	0.0035	0.0009	0.0009	0.0009
(3)	0.7839	0.1960	0.0098	0.0042	0.0035	0.0009	0.0009	0.0009
(4)	0.7839	0.1960	0.0098	0.0042	0.0035	0.0009	0.0009	0.0009
(5)	0.7839	0.1960	0.0098	0.0042	0.0035	0.0009	0.0009	0.0009
(6)	0.7839	0.1960	0.0098	0.0042	0.0035	0.0009	0.0009	0.0009
(7)	0.7839	0.1960	0.0098	0.0042	0.0035	0.0009	0.0009	0.0009

The other way of finding the steady-state probabilities is to solve the probability equations. The equation of the security model is shown below. These equations used in developing an interactive application with MS Excel solver.

$$\pi_0 = p_{00}\pi_0 + p_{10}\pi_1 + p_{20}\pi_2 + p_{30}\pi_3 + p_{40}\pi_4 + p_{50}\pi_5 + p_{60}\pi_6 + \pi_7$$
$$\pi_1 = p_{01}\pi_0$$
$$\pi_2 = p_{12}\pi_1$$
$$\pi_3 = p_{23}\pi_2 + p_{33}\pi_3$$
$$\pi_4 = p_{24}\pi_2 + p_{34}\pi_3 + p_{44}\pi_4$$
$$\pi_5 = p_{25}\pi_2 + p_{35}\pi_3 + p_{45}\pi_4$$
$$\pi_6 = p_{26}\pi_2 + p_{36}\pi_3 + p_{46}\pi_4 + p_{66}\pi_6$$
$$\pi_7 = p_{37}\pi_3 + p_{47}\pi_4 + p_{57}\pi_5$$
$$1 = \pi_0 + \pi_1 + \pi_3 + \pi_3 + \pi_4 + \pi_5 + \pi_6 + \pi_7$$

Figure 5 Probability Equations

3.4 Supply Chain System Security

As presented by Kolluru et al., 2001a, supply chain management has different levels of collaboration. At level-1 partnership with their trading drivers engage in minimal relationships, enabled by asynchronous one-way data push communication. In level-2, the communication architecture is more mature because of the higher level of collaboration between the enterprise drivers. The communication at this level is push and pull, asynchronous and synchronous, point-to-point client-server communication. As a result, additional security threats and vulnerabilities may exist. Finally, in level-3 the communication architecture is a strategic collaboration within the extended enterprise. Additional security threats in this distributed n-tier environment include the same security threats as level-2, applicable in a distributed peer-to-peer network. As a result, the system security could be obtained depending on two cases:

Case 1:

Supply chain management drivers; supplier; manufacturer; distribution center; retailer; and end user may share business information without sharing security and vulnerability information. In this case, the system wide security will be very low. This can be considered as having a series system information security or independent information security systems. Therefore, the total security is a multiplication of all individual driver security values;

$$\pi_{Ssys} = \pi_{S1}\,\pi_{S2}\,\pi_{S3}\,\pi_{S4} \qquad \text{..... (1)}$$

Case 2:

Supply chain management drivers; supplier; manufacturer; distribution center; retailer; and end user may share their business information as well as security

information. In this case, the level of vulnerability will be reduced, hence increasing the security level. We will refer to the sharing of both the business and security information as an integrated or dependant information security system. The integrated system is obtained mathematically by multiplying each master transition matrix for all drivers to obtain the transition matrix for the system, P_{sw} shown in Equation 2.

$$P_{sw} = P_{a1}.P_{a2}.P_{a3}.P_{a4} \quad \text{..... (2)}$$

Then the steady state matrix will be found by obtaining the outcome matrix $P_{sw}^{(n)}$.

3.5 Summary

The chapter presented an introduction to stochastic modeling using Markov chain process and the two methods used to find steady-state probabilities of a system. The first method is to multiplying the initial transition matrix n times to reach the steady-state. The second method is to solve the transition equations to find the steady-state probabilities. Next, the chapter introduced the information security model in details, and gave a definition for each state and what it reflects in real information systems. Also the chapter gave an overview of the devices and tools that can be used to stop attacks and control security like, firewalls, IDSs, and honey-pots. Then, the enhanced security model with deflection tool was covered. This coverage included a suggested honey-pot as deflection tool, and described the effect it will have on improving security. Finally, the chapter showed how the security model can be used in SCM to improve information sharing and security among the supply chain drivers. This was included in the two cases of information sharing among the supply chain drivers.

CHAPTER 4

4. TESTING THE SECURITY MODEL

This chapter tests the proposed security model. First, it tests and illustrates the relation between the security goals and how they affect each other in the model and their effect on the security level. Second, it compares between the security model with and without a deflection tool. Finally, the chapter presents an interactive application that was developed using MS Excel. The application is used to calculate the security level depending on the expected attack level and probabilities of attacking the CIAA.

4.1 Testing the Relations between CIAA

The model was built on the assumption that compromising one security goal could lead to a compromise of other security goals. First, through attacking confidentiality all the other security goals could be attacked. On the other hand none of them can attack back the confidentiality. Second, attacking integrity can be used to attack availability and accountability. And it can be attacked only through confidentiality. Third, availability can't be used to attack other security goals, but it is attacked by confidentiality and integrity only. Consequently, any attack on confidentiality, integrity, or availability leads the information system to a total failure and hence to the system itself. However, compromising accountability means security failure but will not lead to information system failure.

Table 6

Initial Transition Table for Testing CIAA

State	Normal 0	V 1	Att 2	C 3	I 4	A 5	Acc 6	F 7
0	0.5	0.5	0	0	0	0	0	0
1	0.5	0	0.5	0	0	0	0	0
2	p_{20}	0	0	p_C	p_I	p_A	p_{Acc}	0
3	p_{30}	0	0	p_C	p_I	p_A	p_{Acc}	0.1
4	p_{40}	0	0	0	p_I	p_A	p_{Acc}	0.1
5	0.9	0	0	0	0	0	0	0.1
6	p_{60}	0	0	0	0	0	p_{Acc}	0
7	1	0	0	0	0	0	0	0

In this research, testing these assumptions will be by fixing three probabilities and changing the forth. The initial transition matrix for the test is shown in Table 6.

For testing, the probability of finding vulnerability p_V is set to 0.5. Also the level of an attack p_{Att} is set to 0.5. And the probability of total failure p_F is set to 0.1. The first test will set the probability of attacking integrity, p_I, attacking availability, p_A, and attacking accountability, p_{Acc}, to 0.05 each. The probability of attacking confidentiality p_C is set to 0.3, 0.4, 0.5, 0.6, and 0.7. Then the model is solved for the steady-state probabilities π_i. The probabilities of security goals are then calculated as follow: confidentiality, $\pi_C = 1 - \pi_3$; integrity, $\pi_I = 1 - \pi_4$; availability, $\pi_A = 1 - (\pi_5 + \pi_7)$; and accountability, $\pi_{Acc} = 1 - \pi_6$. Next the values will be illustrated in a chart taking the confidentiality as a dependent variable and the other three goals as the independent variables. The same procedure is taken over to the other three security goals to present four different figures. In general, the figures will show how the security goals are affected by each other.

4.1.1 Confidentiality vs. Integrity, Availability, and Accountability

Table 7

Steady-State Probabilities vs. Attack on Confidentiality

p_C Level	Normal π_0	V π_1	Att π_2	C π_3	I π_4	Av π_5	Acc π_6	F π_7
0.30	0.5184	0.2592	0.1296	0.0555	0.0097	0.0097	0.0103	0.0075
0.40	0.4988	0.2494	0.1247	0.0831	0.0109	0.0109	0.0115	0.0105
0.50	0.4738	0.2369	0.1184	0.1184	0.0125	0.0125	0.0131	0.0143
0.60	0.4406	0.2203	0.1102	0.1652	0.0145	0.0145	0.0153	0.0194
0.70	0.3946	0.1973	0.0986	0.2302	0.0173	0.0173	0.0182	0.0265

Table 7 shows that at transition probability p_C level of 30%, the steady-state probability of attacking confidentiality, π_3, is 5.55%, the steady-state probability of attacking integrity, π_4, is approximately 1%, the steady-state probability of attacking availability, π_5, is approximately 1%, the steady-state probability of attacking accountability, π_6, is 1.03%, and the steady-state probability of total failure, π_7, is 0.75%. When p_C level increases to 70%; π_3 increases to 23.02%, π_4 increases to 1.73%, π_5 increases to 1.73%, π_6 increases to 1.82%, and π_7 increases to 2.65%.

Table 8

Confidentiality vs. IAA

π_C	π_I	π_A	π_{Acc}
0.7698	0.9827	0.9562	0.9818
0.8348	0.9855	0.9661	0.9847
0.8816	0.9875	0.9732	0.9869
0.9169	0.9891	0.9786	0.9885
0.9445	0.9903	0.9828	0.9897

Table 8 shows the calculated values of the steady-state probabilities of confidentiality (π_C), integrity (π_I), availability (π_A), and accountability (π_{Acc}). These values are calculated from the steady-state probabilities in Table 7 as mentioned earlier. These values are illustrated in Figure 6.

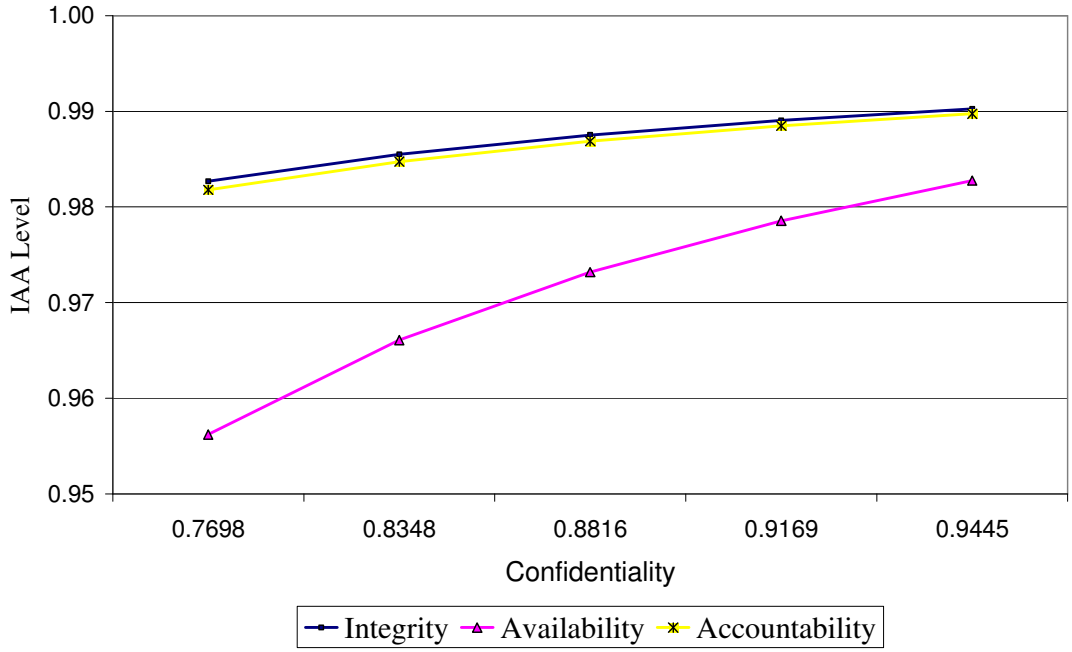


Figure 6 Confidentiality vs. IAA

Figure 6 shows that improving the system's confidentiality will lead to improve in integrity, availability, and accountability. This could be explained from the fact that, for example, only authorized users are accessing to the information due to the high confidentiality; which leads to having a secure information system with high level of integrity, availability, and accountability.

4.1.2 Integrity vs. Confidentiality, Availability, and Accountability

Table 9

Steady-State Probabilities vs. Attack on Integrity

p_I Level	Normal π_0	V π_1	Att π_2	C π_3	I π_4	Av π_5	Acc π_6	F π_7
0.30	0.5184	0.2592	0.1296	0.0068	0.0585	0.0097	0.0103	0.0075
0.40	0.4988	0.2494	0.1247	0.0066	0.0875	0.0109	0.0115	0.0105
0.50	0.4738	0.2369	0.1184	0.0062	0.1247	0.0125	0.0131	0.0143
0.60	0.4406	0.2203	0.1102	0.0058	0.1739	0.0145	0.0153	0.0194
0.70	0.3946	0.1973	0.0986	0.0052	0.2423	0.0173	0.0182	0.0265

Table 9 shows that at transition probability p_I level of 30% the steady-state probability of attacking confidentiality, π_3, is 0.68%, the steady-state probability of attacking integrity, π_4, is 5.85%, the steady-state probability of attacking availability, π_5, is approximately 1%, the steady-state probability of attacking accountability, π_6, is 1.03%, and the steady-state probability of total failure, π_7, is 0.75%. When p_I level increases to 70%; π_4 increases to 24.23%, π_5 increases to 1.73%, π_6 increases to 1.82%, and π_7 increases to 2.65%. But π_3 decreases to 0.52%.

Table 10

Integrity vs. CAA

π_I	π_C	π_A	π_{Acc}
0.7577	0.9948	0.9562	0.9818
0.8261	0.9942	0.9661	0.9847
0.8753	0.9938	0.9732	0.9869
0.9125	0.9934	0.9786	0.9885
0.9415	0.9932	0.9828	0.9897

Table 10 shows the calculated values of the steady-state probabilities of confidentiality (π_C), integrity (π_I), availability (π_A), and accountability (π_{Acc}). These values are calculated from the steady-state probabilities in Table 9 as mentioned earlier. These values are illustrated in Figure 7.

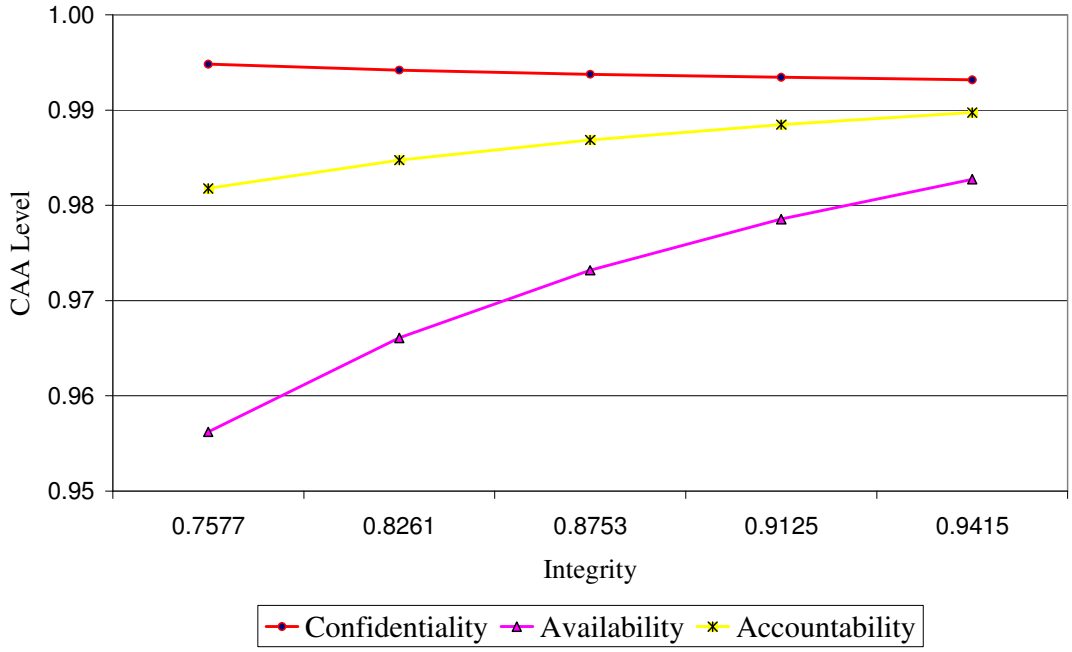


Figure 7 Integrity vs. CAA

Figure 7 shows that as the integrity increases, the availability and the accountability are increasing, but confidentiality is decreasing. This could be explained from the fact that, for example, checking the integrity of a file by requiring a two-person control; meaning that more than one user to confirm the update of the file, leads to a lower confidentiality and to an increase in availability and accountability.

4.1.3 Availability vs. Confidentiality, Integrity, and Accountability

Table 11

Steady-State Probabilities vs. Attack on Availability

p_A Level	Normal π_0	V π_1	Att π_2	C π_3	I π_4	Av π_5	Acc π_6	F π_7
0.30	0.5303	0.2652	0.1326	0.0070	0.0073	0.0441	0.0077	0.0058
0.40	0.5219	0.2609	0.1305	0.0069	0.0072	0.0578	0.0076	0.0072
0.50	0.5137	0.2569	0.1284	0.0068	0.0071	0.0712	0.0075	0.0085
0.60	0.5058	0.2529	0.1264	0.0067	0.0070	0.0841	0.0074	0.0098
0.70	0.4981	0.2491	0.1245	0.0066	0.0069	0.0966	0.0073	0.0110

Table 11 shows that at transition probability p_A level of 30% the steady-state probability of attacking confidentiality, π_3, is 0.7%, the steady-state probability of attacking integrity, π_4, is 0.73%, the steady-state probability of attacking availability, π_5, is 4.41%, the steady-state probability of attacking accountability, π_6, is 0.77%,

and the steady-state probability of total failure, π_7, is 0.58%. As p_A level increases to 70%; π_5 increases to 9.66% and π_7 increases to 1.10%. Whereas, π_3 decreases to 0.66%, π_4 decreases to 0.69%, and π_6 decreases to 0.73%.

Table 12

Availability vs. CIA'

π_A	π_C	π_I	π_{Acc}
0.8924	0.9934	0.9931	0.9927
0.9062	0.9933	0.9930	0.9926
0.9203	0.9932	0.9929	0.9925
0.9350	0.9931	0.9928	0.9924
0.9501	0.9930	0.9927	0.9923

Table 12 shows the calculated values of the steady-state probabilities of confidentiality (π_C), integrity (π_I), availability (π_A), and accountability (π_{Acc}). These values are calculated from the steady-state probabilities in Table 11 as mentioned earlier. These values are illustrated in Figure 8.

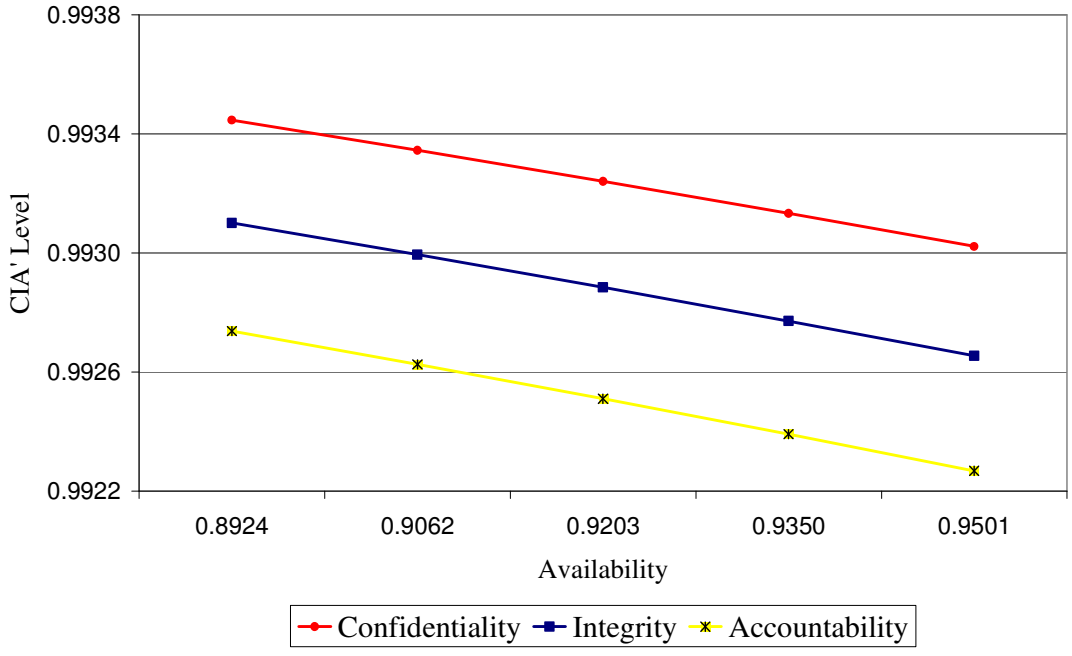


Figure 8 Availability vs. CIA'

Figure 8 shows that when the system become more available the confidentiality, integrity, and accountability, remains almost the same. This is a desirable property of the system security, since one aim to make the system always available (i.e. the internet) while maintains the other security goals.

4.1.4 Accountability vs. Confidentiality, Integrity, and Availability

Table 13

Steady-State Probabilities vs. Attack on Accountability

p_{Acc} Level	Normal π_0	V π_1	Att π_2	C π_3	I π_4	Av π_5	Acc π_6	F π_7
0.30	0.5226	0.2613	0.1306	0.0069	0.0072	0.0072	0.0620	0.0021
0.40	0.5051	0.2526	0.1263	0.0066	0.0070	0.0070	0.0933	0.0021
0.50	0.4826	0.2413	0.1207	0.0064	0.0067	0.0067	0.1337	0.0020
0.60	0.4524	0.2262	0.1131	0.0060	0.0063	0.0063	0.1880	0.0018
0.70	0.4096	0.2048	0.1024	0.0054	0.0057	0.0057	0.2648	0.0017

Table 13 shows that at transition probability p_{Acc} level of 30% the steady-state probability of attacking confidentiality, π_3, is 0.69%, the steady-state probability of attacking integrity, π_4, is 0.72%, the steady-state probability of attacking availability, π_5, is 0.72%, the steady-state probability of attacking accountability, π_6, is 6.2%, and the steady-state probability of total failure, π_7, is 0.21%. When p_{Acc} level increases to 70%; π_6 increases to 26.48%. However, π_3 decreases to 0.54%, π_4 decreases to 0.57%, π_5 decreases to 0.57%, and π_7 increases to 0.17%.

Table 14

Accountability vs. CIA

π_{Acc}	π_C	π_I	π_A
0.7352	0.9946	0.9943	0.9927
0.8120	0.9940	0.9937	0.9919
0.8663	0.9936	0.9933	0.9913
0.9067	0.9934	0.9930	0.9909
0.9380	0.9931	0.9928	0.9906

Table 14 shows the calculated values of the steady-state probabilities of confidentiality (π_C), integrity (π_I), availability (π_A), and accountability (π_{Acc}). These values are calculated from the steady-state probabilities in Table 13 as mentioned earlier. These values are illustrated in Figure 9.

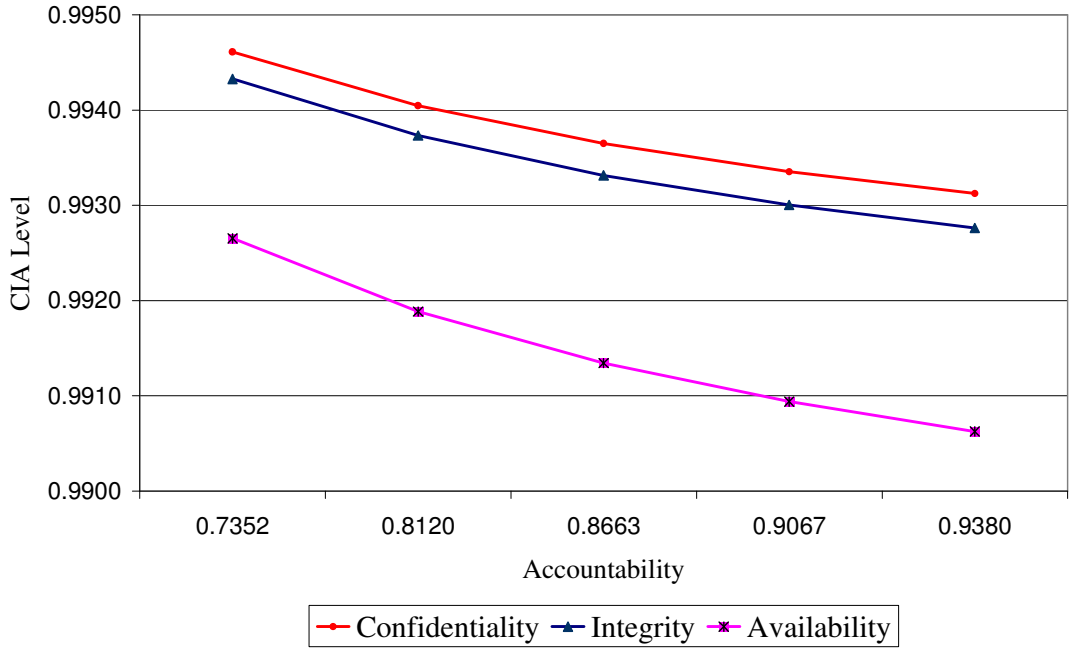


Figure 9 Accountability vs. CIA

Figure 9 shows that an increase in accountability leads to a slight decrease (0.12%) in CIA. This can be explained by the fact that, for example, an attack on accountability (i.e. an attacker viewing the log files) leads to the exposure of audit information showing who did what and when.

4.1.5 Information Security vs. CIAA

Table 15

Information Security vs. CIAA

CIAA attack level	Probability of Security π_S			
	Vs. C	Vs. I	Vs. A	Vs. Acc
0.30	0.7776	0.7776	0.7955	0.7838
0.40	0.7483	0.7483	0.7828	0.7577
0.50	0.7107	0.7107	0.7706	0.7240
0.60	0.6609	0.6609	0.7587	0.6786
0.70	0.5919	0.5919	0.7472	0.6144

Table 15 shows the calculated values of the steady-state probability of security ($\pi_S = \pi_0 + \pi_1$). These values are calculated from the steady-state probabilities from Table 7, 9, 11, and 13. These values are corresponding to the change in the level of attacking confidentiality, integrity, availability and accountability. The values are illustrated in Figure 10.

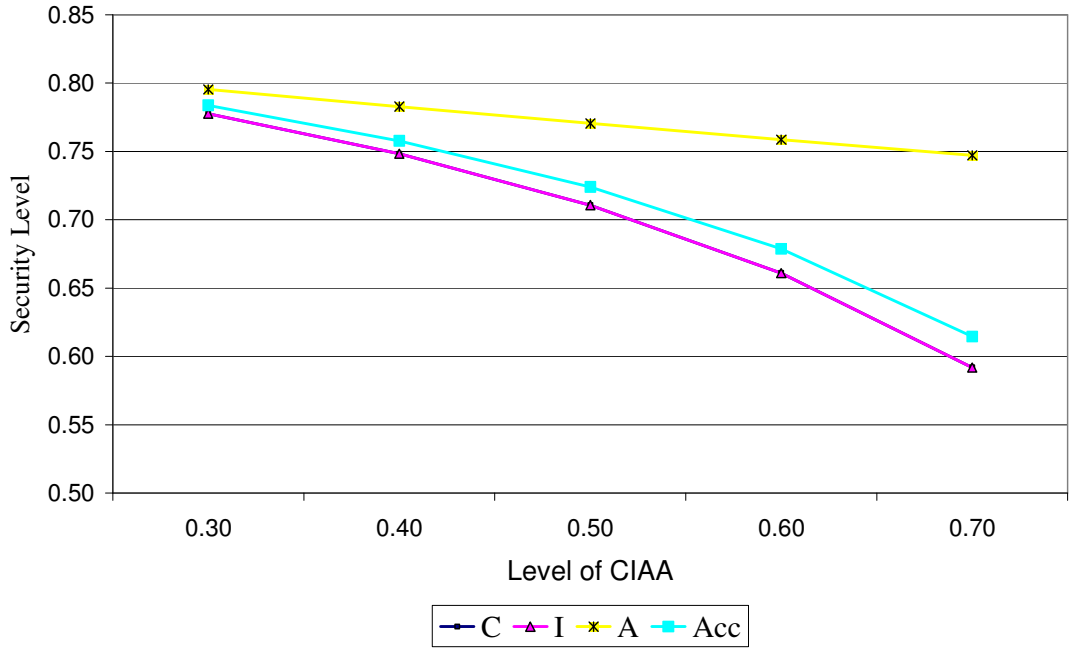


Figure 10 Information Security vs. CIAA

Figure 10 presents the relation between the probability of security and the level of CIAA. Each curve represents the probability of security against one of the security goals and the other goals are fixed to 0.05. The level of each security goal was changed by (0.3, 0.4, 0.5, 0.6, and 0.7) as presented in Table 15.

Figure 10 shows that security decreases as the attack of CIAA levels increase, but with different degree. The effect of confidentiality and integrity on security is the same and has a large effect ranges from 77.7% to 59%. Accountability has a parallel curve with confidentiality and integrity but with little difference that ranges from 78% to 61%. On the other hand, availability has a less effect on security that ranges from 80% to 75%.

4.2 Test the Security Model with Deflection

As mentioned in chapter 3, the information security system can be improved by adding a deflection tool. This can be tested by the security model as mentioned in chapter 3. Figure 4 shows the security model with the deflection state. One of the deflection tools is a honey-pot. It is one of the most powerful defense techniques used to deflect attackers. The honey-pot is a security resource that does not perform any production or functional activities. It mimics the real information network and makes it very simple to attack. The traffic going to or from the real information network will be reduced by deflecting and trapping the attackers into a honey-pot. Any time a connection is sent to the honey-pot, it is most likely to be a probe, or scan, that can

identify the attacker. Hence, useful data about the attackers could be collected by a honey-pot. This information could be used to extract the intrusion detection signature, as stated in (Urjita et al., 2005). A honey-pot can be used to watch, trap, and trick the attacker (Pfleeger et al., 2004).

Table 16

Initial Transition Matrix for Driver 1 P_{d1} with Deflection State

From \ To	N (0)	V (1)	Att (2)	C (3)	I (4)	A (5)	Acc (6)	F (7)	D (D)
(0)	0.75	0.25	0	0	0	0	0	0	0
(1)	0.95	0	0.05	0	0	0	0	0	0
(2)	0.40	0	0	0.18	0.12	0.03	0.03	0	0.24
(3)	0.30	0	0	0.30	0.20	0.05	0.05	0.10	0
(4)	0.60	0	0	0	0.20	0.05	0.05	0.10	0
(5)	0.90	0	0	0	0	0	0	0.10	0
(6)	0.95	0	0	0	0	0	0.05	0	0
(7)	1.00	0	0	0	0	0	0	0	0
(D)	1.00	0	0	0	0	0	0	0	0

In this test the initial transition matrixes form Table 3 and Table 16 for a system without deflection and the same system with deflection, respectively, will be solved for steady-state security. The probability p_{2D} for the attack to be deflected depends on the level of the deflection tool. It will be calculated by the formula $p_{2D} = d * (p_C + p_I + p_A + p_{Acc})$, where d is the parentage of deflection and the values of p_C, p_I, p_A, and p_{Acc} are for driver 1 from Table 1.

Table 17

Comparing Security Level with and without Deflection

Attacker level	Security no deflection	Security with 0.4 deflection	Security with 0.8 deflection
0.05	0.9798	0.9840	0.9881
0.20	0.9240	0.9392	0.9546
0.35	0.8742	0.8989	0.9242
0.50	0.8294	0.8624	0.8964
0.65	0.7891	0.8292	0.8709
0.80	0.7524	0.7989	0.8475
0.95	0.7190	0.7711	0.8258

The value of p_{2i}, where i = 3, 4, 5, 6, will be decreased by the same percentage d, but the rest of the transition probabilities will not change e.g. $p_{33} = p_C$

and $p_{34} = p_{44} = p_I$. In this test d = 0.4 and 0.8, the probability of vulnerability p_V = 0.25, and the probability of total failure p_F = 0.1. In the case of the deflection model the security is calculated by $\pi_S = \pi_0 + \pi_1 + \pi_d$.

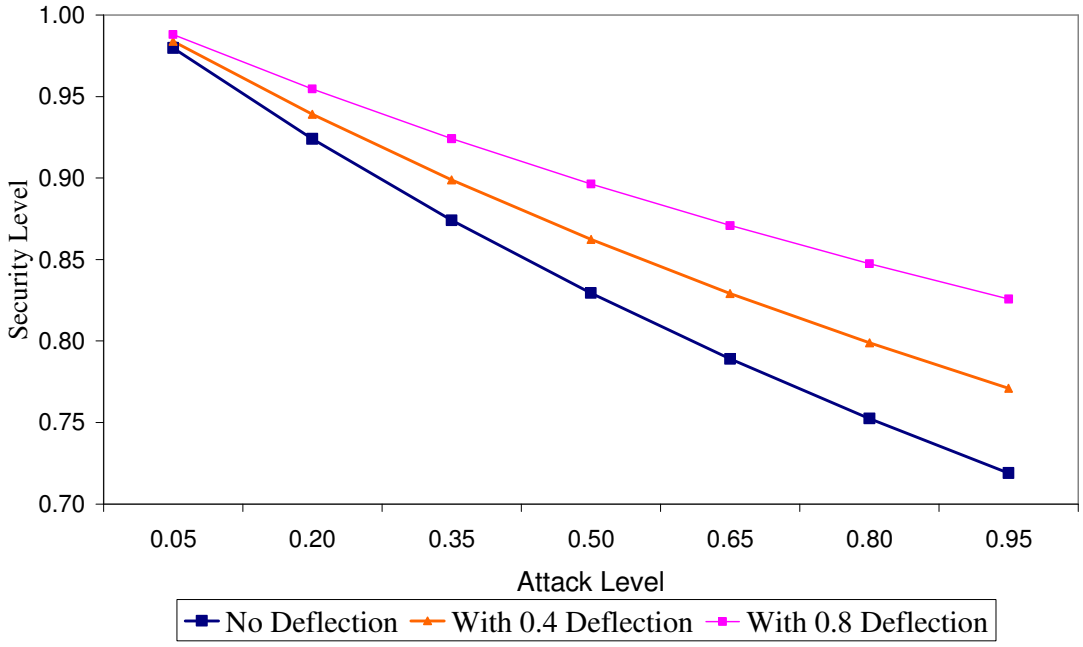


Figure 11 Security Level for Driver 1 with and without Deflection

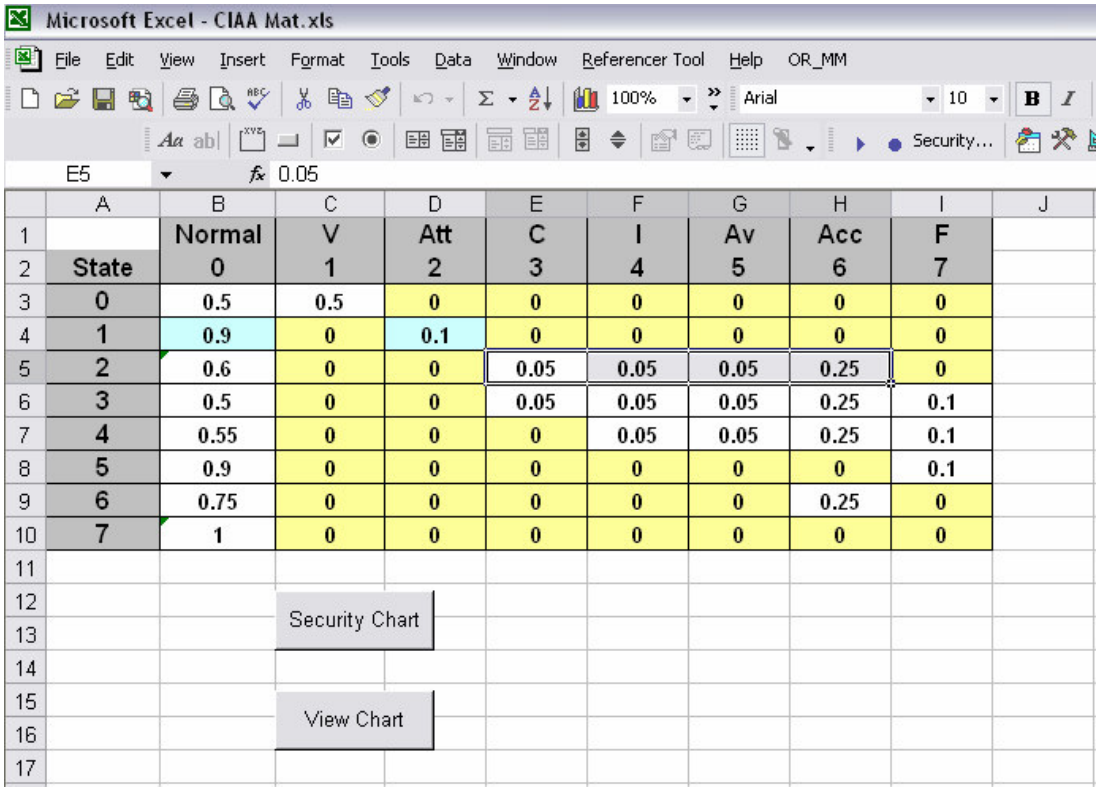
Table 17 compares the steady-state security for each system depending on the level of attack. At the very high attack level of 95% the security increased by from 72% to 77% at only 40% deflection and increased to 83% with 80% deflection as shown in Table 17. Figure 11 shows the improvement in the steady-state security after using the deflection in the system.

4.3 Interactive Application

An interactive application is developed using MS Excel. The application is used to calculate the security level depending on the expected attack level and probabilities of attacking the CIAA. The application starts with the general security matrix. The user is asked to enter all the probabilities in the blank white cells as shown in Figure 12.

First, the user will input the probability of vulnerabilities in the system, and the probability of recovering from vulnerabilities. Second, the recovery level for the system against attacks, and the expected probability for attacking CIAA are specified. The sum of the recovery and CIAA levels should be equal to one. Finally, it is required to specify the probability of a total failure under an attack. This application

will assume that the CIAA levels are the same for all stages of an attack as highlighted in Table 2.



	A	B	C	D	E	F	G	H	I	J
1		Normal	V	Att	C	I	Av	Acc	F	
2	State	0	1	2	3	4	5	6	7	
3	0	0.5	0.5	0	0	0	0	0	0	
4	1	0.9	0	0.1	0	0	0	0	0	
5	2	0.6	0	0	0.05	0.05	0.05	0.25	0	
6	3	0.5	0	0	0.05	0.05	0.05	0.25	0.1	
7	4	0.55	0	0	0	0.05	0.05	0.25	0.1	
8	5	0.9	0	0	0	0	0	0	0.1	
9	6	0.75	0	0	0	0	0	0.25	0	
10	7	1	0	0	0	0	0	0	0	
11										
12										
13										
14										
15										
16										
17										

Figure 12 General Matrix of the Security Model In Excel

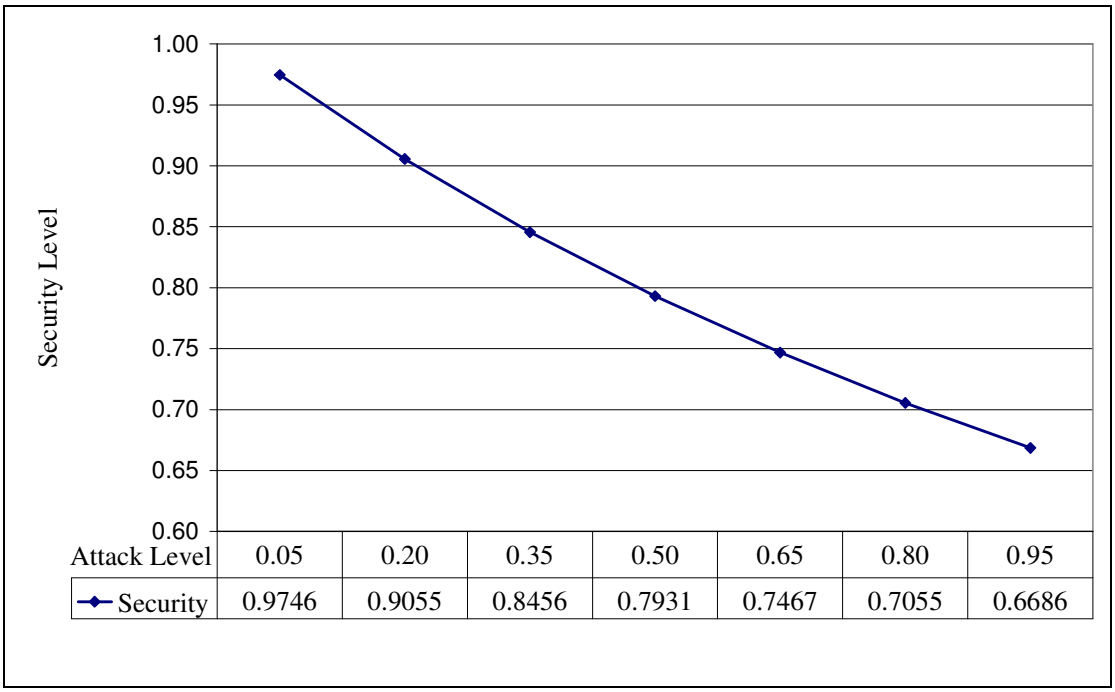


Figure 13 Security Chart and Table for Customer

After filling all the probabilities, the user can press on the security chart button to show the security chart and table as shown in Figure 13. Once the user fills the blanks of the matrix, the application will use this matrix to run the model for the specified levels of attack, (5%, 20%… 95%).

4.4 Summary

This chapter presented some testing on the security model. It illustrated the relation between the security goals and how they affect each other in the security model. Also how the security goals affect the probability of security. Then it compared between the security model with and without a deflection tool and showed how honey-pot tool could be used for deflecting the attacker. Finally, the chapter presented the interactive application that was developed using MS Excel. The application is used to calculate the security level depending on the expected attack level and probabilities of attacking the CIAA.

CHAPTER 5

5. APPLICATION TO SUPPLY CHAIN SECURITY

The chapter will test the proposed initial probabilities for each driver in SCM. It will study the effect of the integrated security system and how it is used to improves the information system security and ability to find vulnerabilities and reduces attacks. This chapter will introduce how the security model can be used to evaluate the security for the individual supply chain drivers and how this security can be affected by the type of interaction and information sharing among the drivers. Also, the chapter will study the affect of sharing information about the vulnerability and how it will affect the probability of having an attack. Finally, the chapter will give a model of e-commerce as a special case of supply chain management to show how the security model can be applied to different areas of information security.

5.1 Supply Chain Security Testing

The steady states of SCM system can be achieved by multiplying the matrices of all drivers as presented. The steady states probability of SCM system, π_S and CIAA could be calculated using the following relationships:

$\pi_S = \pi_0 + \pi_1$; and $\pi_C = 1 - \pi_3$; $\pi_I = 1 - \pi_4$; $\pi_A = 1 - (\pi_5 + \pi_7)$; $\pi_{Acc} = 1 - \pi_6$

Table 3 presents an initial transition matrix for driver 1 (P_{d1}). Table 3 is generated by substituting the values of p_C, p_I, p_A, and p_{Acc} from Table 1 to obtain the general transition matrix (GTM) for driver 1, supplier. The other way of finding the steady-state probabilities is to solve the probability equations presented in Figure 5 at chapter 3.

The summary of steady-state security for diver 1, (supplier) is given for seven scenarios of attack levels in Table 18. Each row in this table represents a steady-state for a corresponding attack level. Where; π_0 is system security without an attack; π_1 is steady-state probability of finding a vulnerability in the system. Table 18, includes the steady-state probabilities such as, attack is initiated, π_2, attack on Confidentiality, π_3, attack on Integrity, π_4, attack on Availability, π_5, attack on Accountability, π_6, and finally total Failure of the security system. π_7. The last column π_S represents the steady-state system security, where $\pi_S = \pi_0 + \pi_1$. Similarly, Table 19, 20 and 21 are developed for drivers 2, manufacturer, 3, retailer, and 4, customer, respectively.

Table 18

Driver 1 - Supplier Steady-State Security

Attacker Level	Normal π_0	V π_1	Att π_2	C π_3	I π_4	A π_5	Acc π_6	F π_7	Security π_S
0.05	0.7839	0.1960	0.0098	0.0042	0.0035	0.0009	0.0009	0.0009	0.9798
0.20	0.7392	0.1848	0.0370	0.0158	0.0132	0.0033	0.0035	0.0032	0.9240
0.35	0.6993	0.1748	0.0612	0.0262	0.0219	0.0055	0.0058	0.0054	0.8742
0.50	0.6635	0.1659	0.0829	0.0355	0.0296	0.0074	0.0078	0.0073	0.8294
0.65	0.6312	0.1578	0.1026	0.0440	0.0366	0.0092	0.0096	0.0090	0.7891
0.80	0.6019	0.1505	0.1204	0.0516	0.0430	0.0107	0.0113	0.0105	0.7524
0.95	0.5752	0.1438	0.1366	0.0586	0.0488	0.0122	0.0128	0.0120	0.7190

Table 18 shows that the security for the supplier is approximately 98% at a very low attack level, 5%. On the other hand, when the attack level increases to 95%, the security is decreased to 71.9%. Although the attack level increases by 90%, however the system security decreases by only 26.9%. This difference is due to the interaction among the security states and the ability of the security system to recover form the attack. Nevertheless, the 26.1% gab in security is considered to be a threat to the security that could cause a lot of damages.

Table 19

Driver 2 - Manufacturer Steady-State Security

Attacker level	Normal π_0	V π_1	Att π_2	C π_3	I π_4	A π_5	Acc π_6	F π_7	Security π_S
0.05	0.8595	0.1289	0.0064	0.0016	0.0020	0.0005	0.0005	0.0004	0.9885
0.20	0.8308	0.1246	0.0249	0.0062	0.0078	0.0019	0.0020	0.0016	0.9555
0.35	0.8040	0.1206	0.0422	0.0106	0.0132	0.0033	0.0035	0.0027	0.9246
0.50	0.7788	0.1168	0.0584	0.0146	0.0183	0.0046	0.0048	0.0037	0.8956
0.65	0.7552	0.1133	0.0736	0.0184	0.0230	0.0058	0.0061	0.0047	0.8684
0.80	0.7329	0.1099	0.0879	0.0220	0.0275	0.0069	0.0072	0.0056	0.8428
0.95	0.7119	0.1068	0.1014	0.0254	0.0317	0.0079	0.0083	0.0065	0.8187

Table 19 shows that the security for the manufacturer is approximately 99% at a very low attack level, 5%. On the other hand, when the attack level increases to 95%, the security is decreased to 81.9%. Although the attack level increases by 90%, however the system security decreases by only 17.1%. This difference is due to the interaction among the security states and the ability of the security system to recover form the attack. Nevertheless, the 17.1% gab in security is considered to be a threat to the security that could cause damages.

Table 20

Driver 3 - Retailer Steady-State Security

Attacker level	Normal π_0	V π_1	Att π_2	C π_3	I π_4	A π_5	Acc π_6	F π_7	Security π_S
0.05	0.9030	0.0903	0.0045	0.0002	0.0003	0.0010	0.0006	0.0001	0.9933
0.20	0.8852	0.0885	0.0177	0.0009	0.0010	0.0039	0.0022	0.0006	0.9737
0.35	0.8681	0.0868	0.0304	0.0016	0.0017	0.0067	0.0037	0.0010	0.9549
0.50	0.8516	0.0852	0.0426	0.0022	0.0024	0.0094	0.0052	0.0014	0.9367
0.65	0.8357	0.0836	0.0543	0.0029	0.0030	0.0120	0.0067	0.0018	0.9193
0.80	0.8204	0.0820	0.0656	0.0035	0.0036	0.0145	0.0081	0.0022	0.9025
0.95	0.8057	0.0806	0.0765	0.0040	0.0042	0.0170	0.0094	0.0025	0.8863

Table 20 shows that the security for the retailer is approximately 99% at a very low attack level, 5%. On the other hand, when the attack level increases to 95%, the security is decreased to 88.6%. Although the attack level increases by 90%, however the system security decreases by only 10.4%. This difference is due to the interaction among the security states and the ability of the security system to recover form the attack. Nevertheless, the 10.4% gab in security is considered to be a threat to the security that could cause damages.

Table 21

Driver 4 - Customer Steady-State Security

Attacker level	Normal π_0	V π_1	Att π_2	C π_3	I π_4	A π_5	Acc π_6	F π_7	Security π_S
0.05	0.7497	0.2249	0.0112	0.0048	0.0028	0.0009	0.0047	0.0009	0.9746
0.20	0.6965	0.2090	0.0418	0.0179	0.0105	0.0035	0.0176	0.0032	0.9055
0.35	0.6504	0.1951	0.0683	0.0293	0.0172	0.0057	0.0287	0.0052	0.8456
0.50	0.6101	0.1830	0.0915	0.0392	0.0231	0.0077	0.0384	0.0070	0.7931
0.65	0.5744	0.1723	0.1120	0.0480	0.0282	0.0094	0.0471	0.0086	0.7467
0.80	0.5427	0.1628	0.1302	0.0558	0.0328	0.0109	0.0547	0.0100	0.7055
0.95	0.5143	0.1543	0.1466	0.0628	0.0370	0.0123	0.0616	0.0112	0.6686

Table 21 shows that the security for the customer is approximately 97.5% at a very low attack level, 5%. On the other hand, when the attack level increases to 95%, the security is decreased to 66.9%. Although the attack level increases by 90%, however the system security decreases by only 30.6%. This difference is due to the interaction among the security states and the ability of the security system to recover form the attack. Nevertheless, the 30.6% gap in security is considered to be a real threat to the security that could cause a lot of damage. This could be cased through the

weakest link in security; where the customer has the lowest security among all drivers due to its high level of vulnerability with $p_V = 0.30$ from Table 1.

Table 22

Integrated Steady-State Security for SCM System

Attacker level	Normal π_0	V π_1	Att π_2	C π_3	I π_4	A π_5	Acc π_6	F π_7	Security π_S
0.05	0.7197	0.2703	0.0043	0.0020	0.0011	0.0004	0.0018	0.0004	0.9900
0.20	0.7012	0.2607	0.0164	0.0075	0.0042	0.0014	0.0069	0.0017	0.9619
0.35	0.6847	0.2520	0.0272	0.0124	0.0070	0.0023	0.0114	0.0029	0.9367
0.50	0.6773	0.2394	0.0341	0.0143	0.0089	0.0030	0.0165	0.0066	0.9167
0.65	0.6675	0.2310	0.0403	0.0176	0.0110	0.0037	0.0205	0.0084	0.8985
0.80	0.6598	0.2231	0.0449	0.0205	0.0129	0.0043	0.0243	0.0102	0.8829
0.95	0.6541	0.2157	0.0479	0.0231	0.0146	0.0049	0.0278	0.0119	0.8699

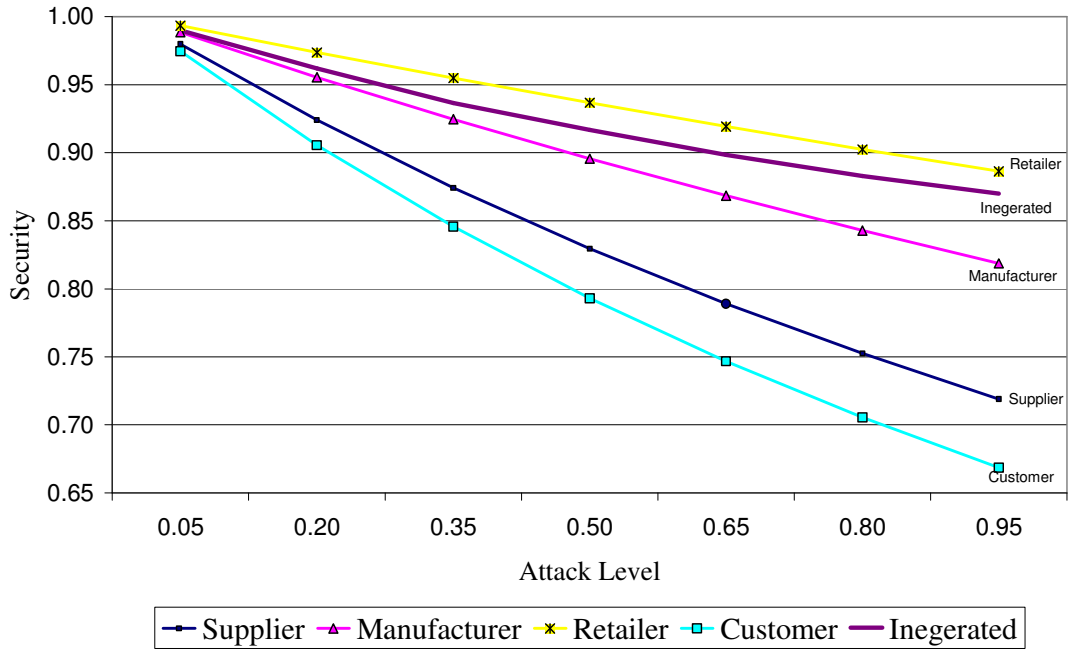


Figure 14 Comparing SCM vs. Individual Driver

Table 22 represents the system security when all drivers are sharing both business and security information as an integrated security system. The data from Table 18, 19, 20, and 21 are used for graphical illustration of the relationship among the four drivers and the SCM integrated security. In Figure 14, the curve for integrated security shows improvements for all levels of attack (05% - 95%). These curves show much lower security for all drivers. On the other hand, when each driver represents individual business where their security information are not shared, each of

them will be more vulnerable by an attacker as shown in Figure 14. The supply chain system security could be obtained depending on two cases:

Case 1:

Supply chain drivers that share business information without sharing security or vulnerability information. This research refers to the series security system when only business information is shared among all SCM drivers. In this case, the system wide security will be very low. Therefore, the total security is a multiplication of the corresponding steady-state probabilities of individual driver security;

$$\pi_{Ssys} = \pi_{S1}\,\pi_{S2}\,\pi_{S3}\,\pi_{S4}.$$

Case 2:

Supply chain drivers share business information as well as security information. In this case, the level of vulnerability will be reduced; therefore, the security level is improved. This research refers to the integrated security system when both business and security information are shared among all SCM drivers. The integrated system is obtained by multiplication of the corresponding matrices of individual driver as an individual unit of security.

$$P_{sw} = P_{d1}.P_{d2}.P_{d3}.P_{d4}$$

Then the steady state matrix will be found by obtaining the outcome matrix $P_{sw}^{(n)}$, where the values under all columns are identical. Repeating the same process for each attack level (0.05, 0.20 … 0.95) to have seven steady state matrices. Finally, Table 23 shows the comparison between these two cases. The two columns in this table represent the steady-state security for seven levels of attacks.

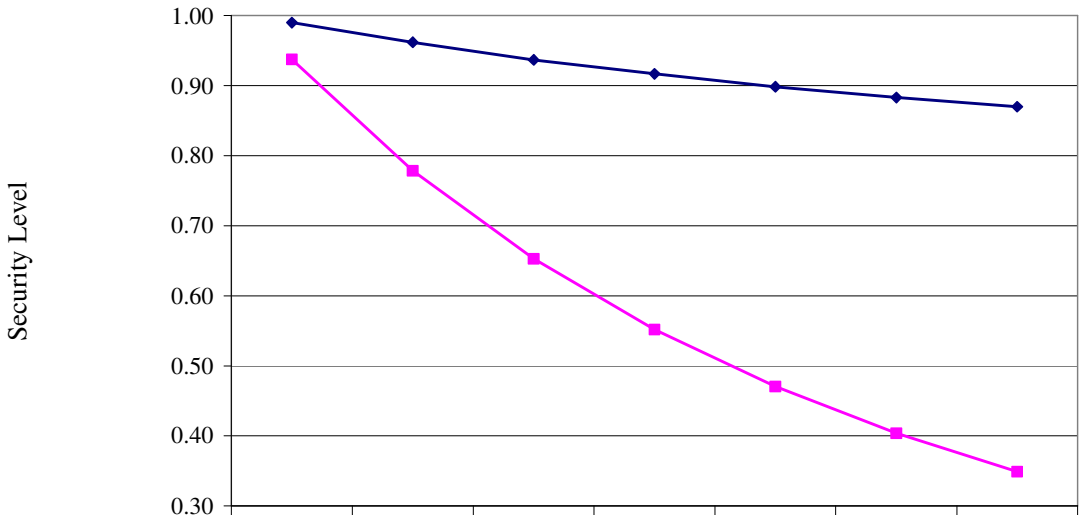
Table 23

System Security at Different Level of Attackers

Attack level	Type of system security	
	Case 1 - Series	Case 2 - Integrate
0.05	0.9376	0.9900
0.20	0.7784	0.9619
0.35	0.6526	0.9367
0.50	0.5519	0.9167
0.65	0.4704	0.8985
0.80	0.4038	0.8829
0.95	0.3488	0.8699

At very low level of attack, 5%, the SCM security is approximately 94% for case 1, (series security) as shown in Table 23. On the other hand, when the attack

level increases to 95%, the security has decreased to approximately 35%. Although the attack level increases by 90%, the system security decreases by 60%. This difference is mainly due to not sharing security information among the SCM drivers. The second Column represents Case 2, integrated security, which has 99% at attack level, 5%. On the other hand, when the attack level increases to 95%, the security has decreased to approximately 87%. Although the attack level increases by 90%, however the system security decreases by only 12%.



Attack Level	0.05	0.20	0.35	0.50	0.65	0.80	0.95
Integrated Sys.	0.9900	0.9619	0.9367	0.9167	0.8985	0.8829	0.8699
Series Sys.	0.9376	0.7784	0.6526	0.5519	0.4704	0.4038	0.3488

Figure 15 Wide Security Improvement with Information Sharing

The main cause of improving SCM security is due to sharing and interaction of information among the SCM drivers. Nevertheless, the 12% gab in security is considered to be a threat to the security that could cause damages. This research observes that the security has improved between the two cases by 52% (from 0.3488 to 0.8699 at the high attack level 95%) as shown in Figure 15. Similarly for low level of attack the difference in security improvement is about 5% which is vital for SCM security.

The integrated system security for (SCM) has less vulnerability which leads to better security due to sharing information about attackers. Once an attack on a driver occurs, the information about this attack could be shared among the remaining drivers. Therefore, an individual driver is more vulnerable than an integrated SCM. Figure 15 comparing two curves; one represents integrated security for a SCM as

indicated in Figure 14; and the other is when a SCM drivers working together, but without sharing security information and becoming much more vulnerable.

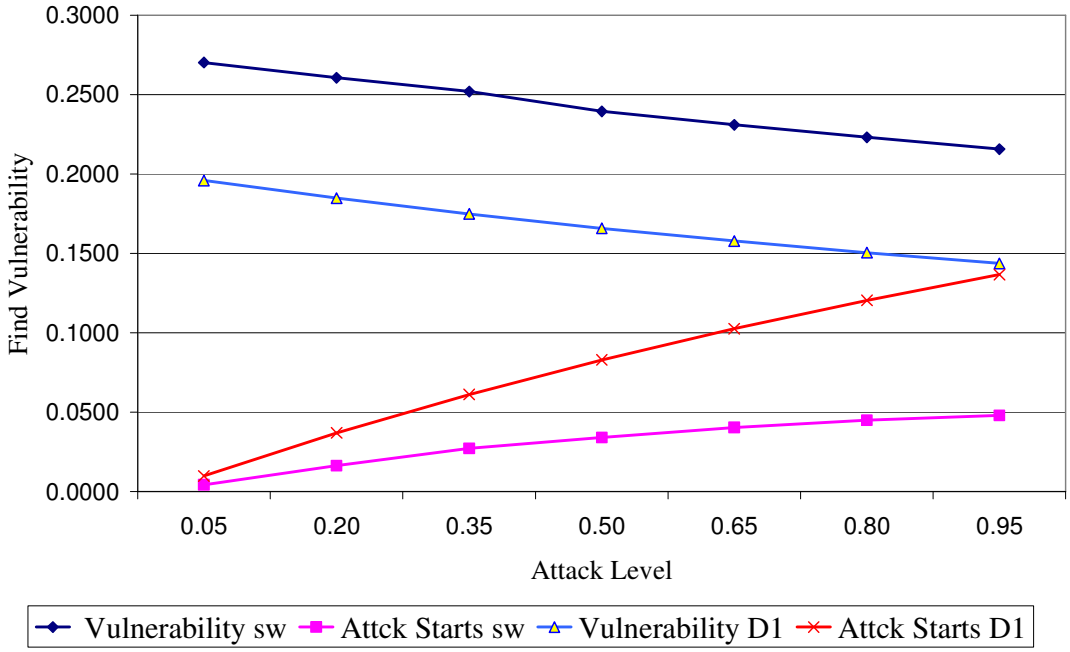


Figure 16 The Relation between Attack and Vulnerability

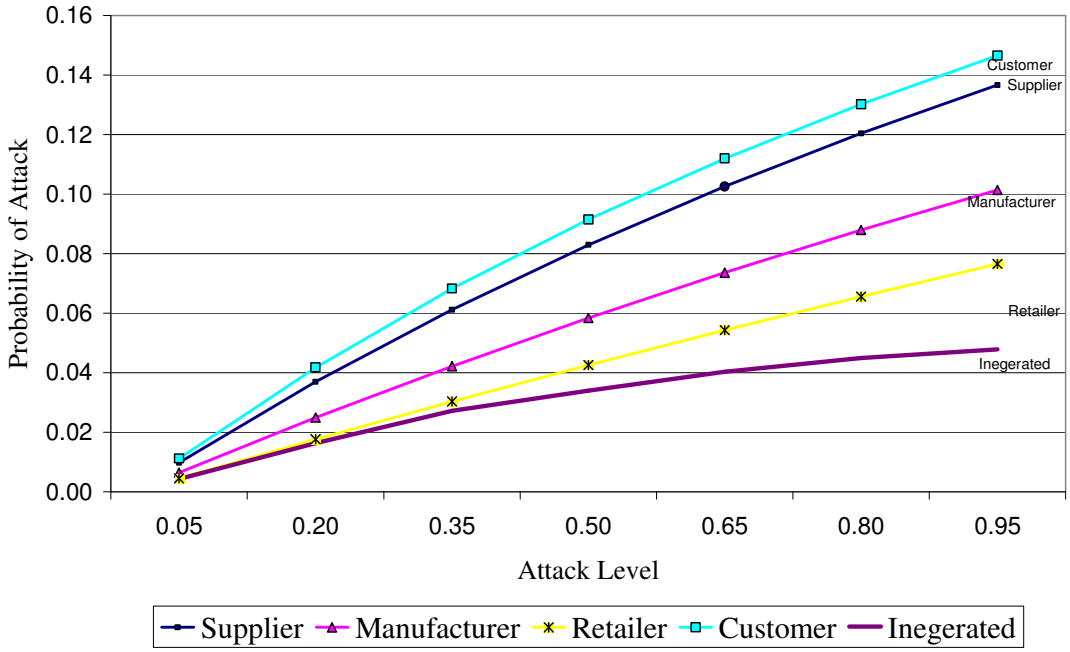


Figure 17 Comparing the Steady-State Probability of Attack

Figure 16 shows the effect of sharing security information among the supply chain drivers. The inner two curves is for driver 1, supplier. As the level of finding the vulnerability decreases the level of having an attack increases. On the other hand, the outer two curves are for the integrated system. The level of finding the vulnerability is increased as well as the level of having an attack decreases highly. Figure 17 shows

that with the integrated system security the probability of having an attack decreases to a very low level comparing to the individual supply chain drivers.

5.2 Free-rider and Supply Chain Information Security

Free-ride in security is that when all parties agrees to share their security information to improver there level pf security, but one or more of the parties take their information and do not share his information. This leak in information sharing could result in affecting the system security very much and reduces its strength. In supply chain information security management the same case could be appearing. For example the driver 4, customer, could be a free-rider. This could be calculated by finding the intenerated system of the first three drivers $P'_{sw} = P_{d1}.P_{d2}.P_{d3}$ and find the intenerated system wide security π'_{Ssw} then multiple it with the individual security of the forth driver π_{S4} , so the security will be $\pi_S = \pi'_{Ssw}\pi_{S4}$.

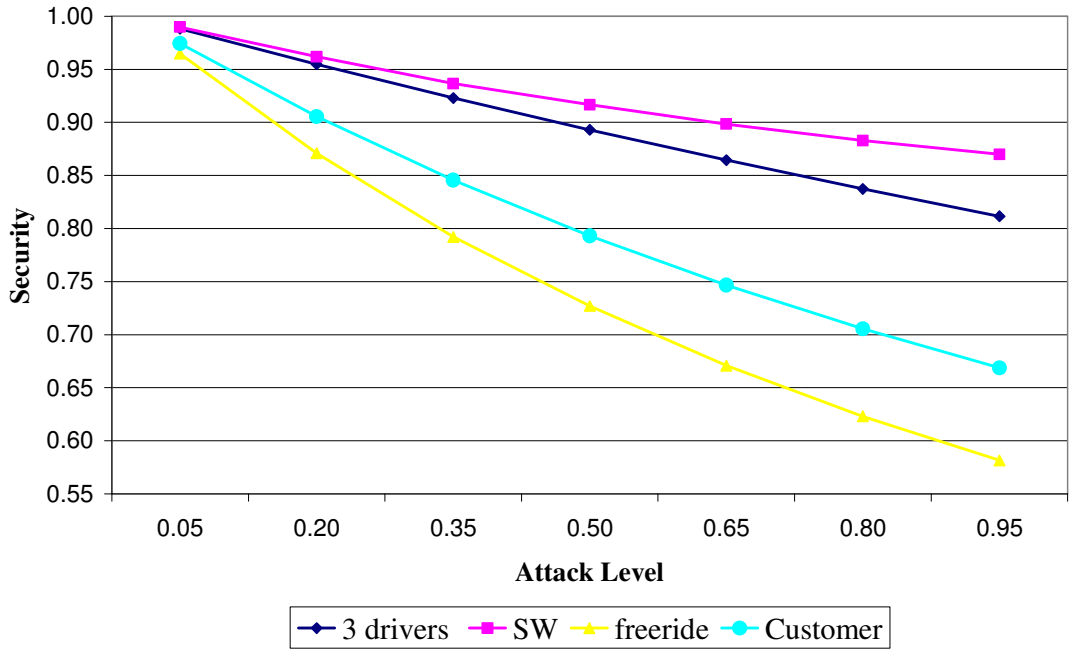


Figure 18 The Effect of Free-Ride on Security

Figure 18 compares between the expected system wide security and the security of only three drivers and the resulting security when the forth driver become a free-rider to the system. As can be seen from the figure above the security is decreasing dramatically at all the level of attacks, which affect all the drivers not only the free-rider.

5.3 Special Case in Supply Chain: e-commerce

An e-commerce system is viewed as a system of interactions among mostly geographically distributed parties, like customers, banks, distribution centers or warehouses, banks, payment servers and shopping storefront (Saleh, 2002). The security of an e-commerce system concerns the security of the participating parties and the security of the interactions among them. Each party requires a different security level relevant to the services it contributes to the overall e-commerce system. Using the security model helps recognizing the weak points of the e-commerce security, and means to improve it.

The process starts with an order from a customer, where he/she has to insert a credit card number, address, and other information which should be secured during transaction processing. It is not unusual to have e-commerce parties residing in or operating from different countries, with different levels of technologies and different levels of security. In fact, most e-commerce systems are global in nature. Therefore, sharing information among the e-commerce parties will be vulnerable depending on the vulnerability of the individual party, and hence affecting the overall e-commerce system security (Knorr et al., 2001). Figure 19 shows the interactions and the flow of information in an e-commerce system.

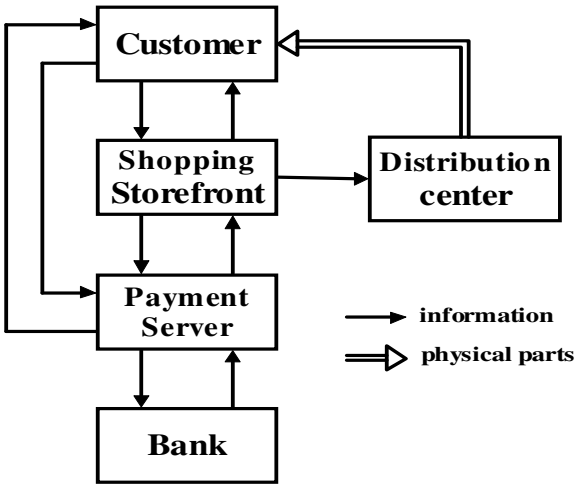


Figure 19 Interactions and Flow of Information among e-Commerce Parties

A typical e-commerce transaction proceeds as follows. First, the consumer browses the shopping storefront web page and once ready to place an order for a product, the storefront redirects the request to a payment server which interacts with the customer to get payment information. The payment server then channels the customer's payment information to the bank to obtain a transaction approval code.

Once approval is obtained from the bank, the payment server then informs the customer and the storefront about the success of the transaction. The storefront then informs the distribution center to arrange for the delivery of the ordered product.

The proposed values of the transition probabilities p_C, p_I, p_A, p_{Acc} for each driver (depending on its mission) are shown in Table 24. However, the reader can use this model for many multi-party systems, and can use the appropriate CIAA data. The next step involves developing a generic transition matrix GTM for each driver (i) created by substituting the parameters of p_C, p_I, p_A, p_{Acc} from Table 24. The model proposed five different levels of attacks to present scenarios of attacks. These five levels of attacks (10% low, 30% more or less low, 50%, medium, 70% more or less high, 90% high) are used to find the system security at the corresponding level. By repeating the same process on the GTM for each attack level, we obtain five steady-state probabilities corresponding to five levels of attacks.

Table 24

Proposed CIAA for e-Commerce System

E-commerce party	p_C	p_I	p_A	p_{Acc}	p_{CIAA}
Customer	0.35	0.05	0.05	0.15	0.60
Shopping Storefront	0.10	0.10	0.15	0.05	0.40
Payment Server	0.02	0.05	0.02	0.06	0.15
Bank	0.05	0.05	0.05	0.05	0.20
Distributor	0.05	0.05	0.05	0.25	0.40

The e-commerce system consists of five interacting parties. The attack on each party depends on its role in the system. First, the customer is concerned more with confidentiality and accountability, so a high weight is given to the probabilities of attacking them (p_C = 0.35/ 0.60 and p_{Acc} = 0.15/0.60). Second, the shopping storefront is concerned more with availability, therefore, a high value is assigned for it (p_A = 0.25/0.50). Third, Payment server has high integrity and accountability requirements. Forth is the bank is concerned with securing all the security goals CIAA, therefore a high value of $p_{20} = 0.80$ and $p = 0.05$ for each CIAA are assigned. Fifth, the distribution center has a very high accountability requirement, therefore a high $p_{Acc} = 0.40$ is assigned.

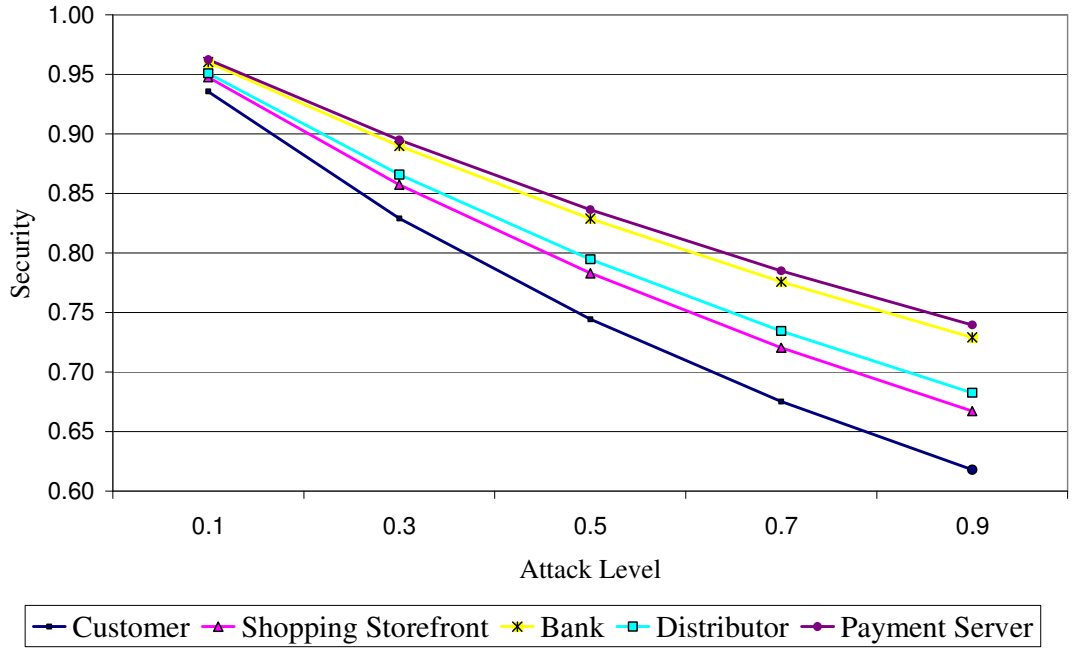


Figure 20 Steady-State Security e-Commerce Parties

Figure 20 shows the attack level versus the security steady-state probabilities corresponding to each party; customer, shopping storefront, bank, and distribution center.

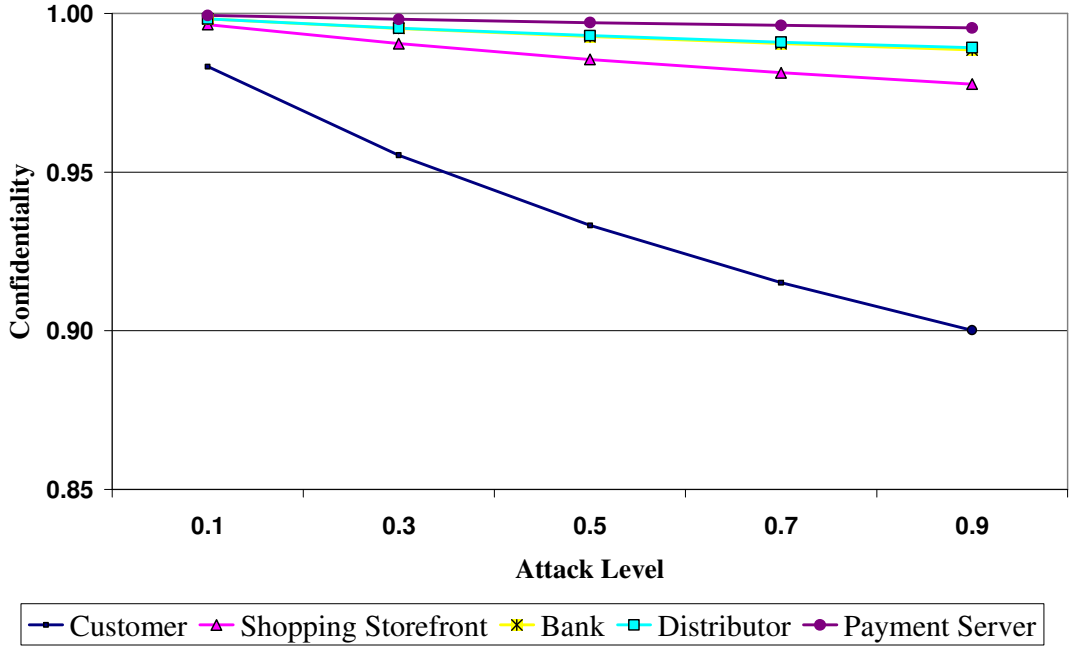


Figure 21 Steady-State Confidentiality for All Parties

Figure 21 and Figure 22 show the attack level versus the confidentiality and Accountability for steady-state probabilities relevant to each party. These probabilities can be calculated by $\pi_C = 1 - \pi_3$ and $\pi_{Acc} = 1 - \pi_6$ for confidentiality and

accountability, respectively. The customer confidentiality is very low comparing to other parties as shown in Figure 21.

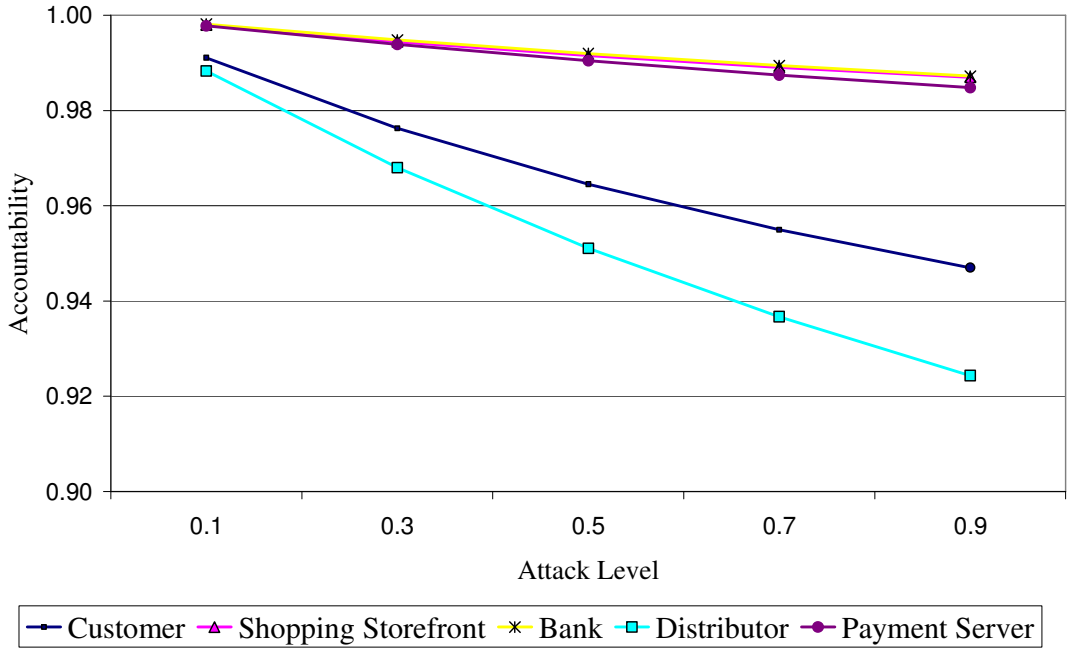


Figure 22 Steady-State Accountability for All Parties

The distribution center has a low level of accountability as shown in Figure 22. Consequently, the low customer confidentially and distribution center accountability may facilitate the attacker to penetrate the system and risk the security of the system. Using this model may help to recognize the weak point of the security and means to improve it. This model can be used for larger scale of IT security application using new input values. Once the weak points of the system discover the higher security could be achieved by implementing honey pots or other deflection and detection devices.

5.4 Summary

The chapter tested the proposed initial probabilities for each driver in SCM that depends on the functionality of the driver. It studied the effect of integrating security system among the SCM drivers and how it is used to improve the information system security and ability to find vulnerabilities and reduces attacks. The overall performance of the security of SCM system could be improved drastically by recognizing the weak points of the security and means to improve it.

The chapter studied the e-commerce system is an application of SCM. The model proposed five different levels of attacks (0.10, 0.30, 0.50, 0.70 and 0.90). The research found that low customer confidentially and distribution center accountability

may help the attacker to penetrate the system and risk the security of the system. The use of this model may help to recognize the security behavior and means to improve it. This model can also be used for larger scale e-commerce system security. Once the weak points of the system are discovered, the higher security could be achieved by implementing honey pots or other deflection and detection devices. The model may help the individual party exposed to higher risk of attack and leading to a higher vulnerability of the e-commerce system, if the information about its own vulnerability and risk level are not shared with other parties.

CHAPTER 6

6. CONCLUSION AND FUTURE WORK

6.1 Conclusion

Information security of the supply chain management (SCM) is essential and covers a wide scope of organization's performance. Higher performance of information security could be achieved through interactions and smooth flow of information from suppliers to customers. Information sharing is an important factor for collaboration in supply chain management. Information security addresses very important goals related to information system; confidentiality, integrity, availability, and accountability (CIAA). Security vulnerabilities are weak points in any system which could be exploited by attackers. This may affect one or more of the security goals of the CIAA model. Measuring information security will lead to an effective security management. It enables the enforcement of security objectives and goals. This helps to develop security program strategies and plans. Measurement requires selecting the appropriate standard(s) and evaluating security program status along with the security criteria.

In general, the security requirement of information interaction processes within each driver and among all supply chain drivers are almost the same. Each supply chain driver has essential information security requirements within the driver. Usually, the attacker could use the differences of security levels to attack supply chain drivers by attacking the driver with the lowest security. Information security of the supply chain management (SCM) is essential and covers a wide scope of organization's performance. However, the main challenges in supply chain management are; integration of security information; and attacks that could penetrate more than one driver in the supply chain through the weakest driver.

This research presents an introduction to stochastic modeling using Markov chain process with two approaches used to find steady-state probabilities of the system. The first approach is to obtain a steady-state security system, which could be reached by multiplication of the initial transition matrix n times. The second approach is to solve the transition equations. This research has introduced the information security model in details and defined each state and the reflections it has on real information systems. Also, it suggested devices and tools that can be used to stop attacks and control security, such as; firewalls, IDS, and honey-pot. Then, an

enhanced security model with deflection tool was discussed. The model suggested a honey-pot as deflection tool and showed how it will improve security.

The proposed model has been tested for SCM with four drivers where each driver has a different mission so the author assigned different values of confidentiality, integrity, availability and accountability to each driver as deemed relevant to their mission. In addition, seven levels of attackers (5%, 20%, 35%, 50%, 65%, 80% and 95%) were tested to present different security responses. The model runs for steady-state for all combinations. The analysis of the model and its graphical representation show that the SCM sharing security and information has been improved at all level of attacks. Individual driver exposed to higher risk of attack may lead to a higher vulnerability of the SCM, if the information about its own vulnerability and risk level are not shared with other drivers. Moreover, the quantitative model used to analyze instances of E-commerce, systems.

6.2 Remarks

Organizations with lack of expertise to understand security risks have to transfer their security risks to insurance companies. Therefore, insurance companies are required to understand security risks before pricing their policies. Hence, an insurance company will have the power and encouragement to force organizations to pay for better security and to provide the knowledge to help them. The insurance company has benefit when organizations sharing information to have a feedback about attacks, which help to prevent future attacks. Complete security is not feasible regardless of the amount invested for security measurements. However, full information security is almost impossible. The security model presented in this research could be a continuation to the work done by Lambrinoudakis et al., 2005, where they tried to present a simple model for the insurance company to calculate the fair amount of money that will be charged for this insurance service.

6.3 Future Work

For future work the security model could be enhanced by adding the time dimension to the security measurements. This will help to evaluate the time needed by the attacker to break the system and the recover time from the attack. Another dimension that could be added to the security model is the economical factor. The economical factor could be used to estimate the cost of having a certain level of security and the corresponding cost charged by the insurance companies for

information system assets. There is also a cost due to the system failure with additional cost due to recovery from damages occurred in the security goals.

.

REFERENCES

Ahlm, E. (2006). Emerging Intelligent Information Security Systems. *Scientific Computing,* 26-27.

Ayers, J. (1999). Supply Chain Strategies. *Information Strategy: The Executive's Journal, 15,* 3-8.

Beesley, A. (1996). Time Compression in the Supply Chain. *Industrial Management & Data Systems, 96,* 12-17.

Blaise, C., & Holly, C. (1999). Raising the intelligence stakes: corporate information warfare and strategic surprise. *Competitive Intelligence Review, 10,* 58-66.

BS 7799. (2002). British Standard of Information Security Management. UK .

Callio Secura 17799. (2005).

Chopra, S., & Meindl, P. (2004). *Supply Chain Management*. (2nd ed.) Prentice Hall.

Clarke, A., & Gallo, V. (2000). The Software Colander-holes in Messaging. *Computer and Security, 19,* 692-697.

CPFR, C. P. f. a. R. (2001). Voluntary Inter-industry Commerce Standards Association.

Denning, D. E. (1999). *Information Warfare and Security*. Addison-Wesley.

Eschelbeck, G. (2005). The Laws of Vulnerabilities: Which security vulnerabilities really matter? *Information Security Technical Report, 10,* 213-219.

ESPIRIA. (2004). Executive Brief: Information security Measurement.

Gang, L., Hong, Y., Shouyang, W., & Yusen, X. (2005). Comparative analysis on value of information sharing in supply chains. *Supply Chain Management: an International Journal, 1,* 34-46.

Goan, T. (1999). A Cop on the beat: Collecting and Appraising Intrusive Evidence. *Communications of the ACM, 42,* 46-52.

Hillier, F. S. & Lieberman, G. J. (2005). Markov Chains. In *Introduction to Operation Research* (8th ed., pp. 732-759). McGraw Hill.

Howard, J. (1997). *An analysis of security incidents on the Internet.* PhD thesis Carnegie Mellon University, Pittsburgh, PA.

Hutchinson, W. (2002). Concepts in information warfare. *Logistics Information Management, 15,* 410-413.

Hutchinson, W., & Warren, M. (1999). Attacking the Attackers: Attitudes of Australian IT Managers to Retaliation Against Hackers. In Wellington.

Jonsson, E., & Olovsson, T. (1997). A Quantitative Model of the security Intrusion process Based on Attacker Behavior. *IEEE Transaction on Software Engineering, 23,* 235-245.

Knorr, K., & Rohrig, S. (2001). Security requirements of e-business processes. In (pp. 73-86).

Kolluru, R., & et al. (2001a). An Extended Enterprise Framework for Supply Network Management. *International Journal of Agile Manufacturing, 3*.

Kolluru, R., & Meredith, P. H. (2001b). Security and trust management in supply chains. *Information Management & Computer Security, 5,* 233-236.

Lambrinoudakis, C., Stefanos, G., & Petros, H. (2005). A formal model for pricing information systems insurance contracts. *Computer Standards & Interfaces, 27,* 521-532.

Lee, H. L. & Whang, S. (1999). *Information Sharing in a Supply Chain, Research Paper.* Stanford University, Stanford, CA.

MacLeod, D., & Whyte, D. (2000). Towards System Survivability using the Single Virtual Enterprise Model and Layered Security through Information Protection Co-ordination Centres. In.

Madan, B. B., Katerina Goseva-Popstojanova, Kalyanaraman Vaidyanathan, & Kishor S.Trivedi (2004). A method for modeling and quantifying the security attributes of intrusion tolerant systems. *Performance Evaluation, 56,* 167-186.

Messmer, E. (1999). Threat of 'Infowar' Brings CIA Warnings. *Network World, 16,* 10.

NIST, N. I. o. S. a. T., & NSA, N. S. A. (1992). Federal Criteria for Information Security Technology, Draft.

Ortalo, R., & et al. (1999). Experiments with quantitative evaluation tools for monitoring operational security. *IEEE Transaction on Software Engineering, 25,* 633-650.

Pfleeger, C. P., & Pfleeger, S. L. (2004). *Security in Computing*. (3rd ed.) Prentice Hall.

Saleh, K. (2002). Documenting electronic commerce systems and software using the Unified Modeling Language. *Journal of Information and Software Technology, 44,* 303-311.

Schechter, S. E., & Smith, M. D. (2003). How much security is enough to stop a thief? In *Financial Cryptography Conference*.

Sharam, S. K., & Gupta, J. N. D. (2002). securing information infrastructure from information warfare. *Logistics Information Management, 15,* 414-422.

Szygenda, R. (1999). Information's Competitive Edge. *Information Week, Executive Report: IT Value Chain,* 4-7.

Trivedi, K. S. (2001). *Probability and Statistics with Reliability, Queuing, and Computer Science Applications*. (2nd ed.) New York: Wiley.

Urjita, T., Sudarshan, V., & Ramani, A. K. (2005). HoneyAnalyzer - Analysis and Extraction of Intrusion Detection Patterns & Signatures Using Honeypot. In UAE.

Wang, C., & Wulf, W. A. (2002). Towards A framework for security measurement. *Logistics Information Management, 15,* 414-422.

Warren, M., & Hutchinson, W. (2000). Cyber attacks against supply chain management systems: a short note. *International Journal of Physical Distribution & Logistics, 30,* 710-716.

VITA

Ahmed Maher AL Nunu was born in Gaza, Palestine, on 25th of July 1978. He was raised in Qatar by Maher A. AL-Nunu and Najah K. EL-Hindi. In Qatar, he received the degree of Bachelor of Science in Electrical Engineering, Concentration on Computer & Networking, with GPA of 3.92/4 from the University of Qatar in the period from September 1996 to June 2001. He earned the Rank #1 on the dean's list of honor from the engineering department through the five years. During the following years, he was employed as a computer engineer. In January 2004 he joined the American University of Sharjah, Sharjah, UAE, to acquire a Master of Science in Engineering Systems Management. He has a Cisco Qualified Security certificate from Cisco Academy in AUS and holds CCNA (Cisco Certified Network Associate).