جـامـعـة الـشـرق الأوسـط
MIDDLE EAST UNIVERSITY
Amman - Jordan عمان - الأردن

A Model for Outsourcing Monitoring System

By

Anas Ali Al-Kasasbeh

Supervised by

Dr. Hussein Hadi Owaied

Master Thesis

Submitted in Partial Fulfillment of the

Requirements for

Master Degree in computer Science

Department of Computer science

Faculty of Information Technology

Middle East University

August, 2010

Authorization

I, Anas Ali Al-Kasasbeh, authorize **Middle East University (MEU)** to provide copies of my dissertation to libraries, organizations, institutes and individuals upon request.

Name: Anas Ali Al-Kasasbeh

Signature: ____________

Date: 2 / 8/2010 .

أنا الطالب، انس علي الكساسبه، أفوض جامعة الشرق الأوسط لتزويد نسخ من هذا البحث إلى المكتبات، المؤسسات، المعاهد والأشخاص وحسب الطلب.

الاسم : انس علي الكساسبه.

التوقيع: ____________

التاريخ: 2010/8/2

Thesis Committee Decision

This Thesis "A model for Outsourcing Monitoring System" was discussed and certified on 2-8-2010.

Thesis committee		**Signature**
Prof. Nidal F. Shilbayeh	Chairperson	....
Dr. Hussein Hadi Owaied	Supervisor & Member	............Owaied............
Dr. Mahmoud Malek AbuArra	Member	....

Acknowledgements

I thank Allah the Almighty for His blessings in enabling me to complete this research work and giving me this opportunity to become a student once again after years of work. The successful completion of this thesis is due to the mode of supervision, timely encouragement and efficient guidance received from my supervisor **Dr. Hussein Al-Shamery**. I deem it a blessing from the Almighty to have the right person for my research guidance. I also wish to express my deepest gratitude to the members of the committee for spending their precious time on reading my thesis and giving me encouragement and constructive comments. Also I thank all Information Technology faculty freshmen at Middle East University. I am so grateful for my mother and father for their constant prayers. They are wonderful educators although they did not complete their study. Also many thanks to my brother, Emad, for his effective contribution in completing this research. I acknowledge with gratitude the benevolence of all those who helped me in this research work.

Dedication

To my beloved country, Jordan.

To my father and mother.

To my brothers and sisters.

To all my friends.

Table of Contents

List of Figures

Abbreviations

AES	Advanced Encryption Standard
CSO	Chief Security Officers
DDoS	Distributed Denial-of-Services
DES	Data Encryption Standard
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GISRA	Government Information Security Reform Act
GLB	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act
PK	Port-Knocking
HPK	Hybrid Port-Knocking
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection Systems
ISS	Information Securities Services
MAC	Message Authentication Code
MD5	Message Digest Algorithm
MSM	Managed Security Monitoring
MSS	Managed Security Services.
MSSP	Managed Security Service Provider.
PK	Port Knocking
SHA	Secure Hash Algorithm
SLA	Service Level Agreement
SOC	Standard Occupational Classification
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

A Model for Outsourcing Monitoring System

Abstract in English

There are many problems related to the outsourcing relationship, these problems are divided into tow categories: Provider problems and outsourced company (client). It is very important to give permission to departments for access to use these services and not allow the other departments, in order to reduce the cost of using the outsource software. Also the provider's staff should access client systems only from specific parts. On the other hand the provider must assure that the services are safely delivered to the client and that these services are not exposed to hackers. In this thesis, we designed a model for monitoring the outsourcing system. The model consists of three sub-models, which are: the Client sub-model, the Provider sub-model and Provider-Client relationships sub-model. Each part in this model aims to solve the set of problems in outsourcing system, especially those problems mentioned in the problem statement. The proposed model asserts that the necessary time and effort must also be spent on negotiating and establishing the outsourcing process, with respect to management structures and systems for monitoring and evaluating the relationship. The model states that regardless of how the activity is handled in-house outsourcing must be managed differently, often requiring new management.

A Model for Outsourcing Monitoring System

Abstract in Arabic

يوجد عدد من المشاكل في عملية الاستعانة بالمصادر الخارجية بين طرفي العلاقة والتي تصنف الى مشاكل مرتبطة بالمزود ومشاكل مرتبطة بالعميل. من المهم اعطاء الصلاحية للاقسام لاستخدام هذة الخدمات وعدم السماح للاقسام الاخرى التي لا تحتاج لهذة الخدمات بهدف تخفيض تكلفة الاستخدام. ايضا فريق العمل التابع للمزود يجب ان يطلع على انظمة العميل من اجزاء محددة. وعلى الجانب الاخر، يجب على المزود التاكد من عملية توصيل الخدمات بامان وعدم تعرضها للسرقة. في هذا البحث، تم تصميم نموذج لمراقبة نظام الاستعانة بمصادر خارجية. هذا النموذج يتكون من ثلاثة اجزاء: نموذج العميل، نموذج المزود و نموذج العلاقة بين المزود والعميل. كل جزء في هذا النموذج يهدف الى حل جزء من المشاكل وخصوصا تلك المشاكل التي تم ذكرها في جزء تعريف المشكلة. ياتي النموذج المقترح لمعالجة الوقت والجهد ومراقبة مختلف النشاطات في عملية الاستعانة بالمصادر الخارجية وكذلك كيفية التعامل مع النشاطات في عملية الاستعانة بمصادر خارجية والتي يجب أن تدار بشكل مختلف وتتطلب في كثير من الأحيان الإدارة الجديدة.

Chapter One: Introduction

1.1 Overview

In this century there are many software applications available that can be used by different organizations. These software are usually very expensive to buy, but the availability of the infrastructure of Information Technology using the internet, makes it possible to rent them in specific time with less expenses, this is called outsourcing. The outsourcing can be defined as a relationship between two groups of companies, the first group is called the client who requests a collection of services from the second group, which is the second group and is called the provider. These services can not be achieved efficiently without a framework of network security. Therefore any organization has the choice of outsourcing according to their needs, and should make the agreement with the provider of the software establishing such framework of network security.

The outsourcing concept also allows the client to focus on their business issues while the rest of details are managed by the provider. This means that a large amount of resources and attention might fall on the shoulders of the management professionals, which can be used for more important, broader issues within the company. The specialized company that handles the outsourced work is often streamlined, and often has world-class capabilities, and access to new technology that a company couldn't afford to buy on their own. Plus, if a company is looking to expand, outsourcing is a cost-effective way to start building foundations in other countries. There are some advantages and disadvantages of using outsourcing. One of these is that outsourcing often eliminates direct communication between the providers and their clients. This prevents a company from building good relationships with their customers, and often leads to dissatisfaction on one or both sides. There is also the danger of not being able to control some aspects of the company, as outsourcing may lead to delayed communications and project implementation.

The sensitive information is more vulnerable, and a company may become very dependent on the providers, which may lead to problems that might make the outsource provider back out on their contract.

The outsourcing concept will create many opportunities for the providers. In fact, many of the companies that exist today would not have survived after the recession due to the fact that their customers asked them to cut costs by a large sum.

There are various benefits of using the outsourcing which often include one or more of the following: Minimum cost, increase the staff productivities, visually have many resources, the flexibility of applying many resources efficiently and effectively.

1.2 The Terminology

There are many terms have been used through this thesis, in the following are the description of the most common terms:

1. **Security**: The security of a system is the ability of the system to support the system availability, data integrity and confidentiality. So if the system fails to support these three characteristics or protect them, then the system amounts to a security violation or weakness (Stallings 2003).
2. **Network Security:** The network security is the protection of a computer network and its services from unauthorized modification, destruction, or disclosure. In other words, the network security is the process to make sure that the data or services will reach the target workstation and data, services will be protected from hackers (Stallings 2007).
3. **Availability**: The availability is the characteristic of a resource that is committable, operable, or usable upon demand to perform its designated or required function. In computing, it is the percentage of time a computer system available for use. In quality control it is the ability of an item to perform its designated function, whenever required (Gao, Yu et al, 2008).

4. **Threat**: The threat can be defined as an action or potential occurrence (whether or not malicious) to breach the security of the system by exploiting its known or unknown vulnerabilities. It may be caused by (1) gaining unauthorized access to stored information, (2) denial of service to the authorized users, or (3) introduction of false information to mislead the users or to cause incorrect system behavior (called spoofing). See also attack (Stallings 2007).

5. **Monitoring**: Monitoring is the regular observation and recording of activities taking place in a project or program. It is a process of routinely gathering information on all aspects of the system (Vincent 2009)

6. **Outsourcing**: Contracting, sub-contracting, or 'externalizing' non-core activities to free up cash, personnel, time, and facilities for activities where the firm holds competitive advantage. Firms having strengths in other areas may contract-out data processing, legal, manufacturing, marketing, payroll accounting, or other aspects of their businesses to concentrate on what they do best and thus reduce average unit cost. Outsourcing is often an integral part of downsizing or reengineering. Also called contracting out (Deshpande 2005).

7. **Attack:** Malicious action taken by a hacker, intruder, or unauthorized user to cause damage to the system and/or to the data stored in it, through exploitation of one or more system vulnerabilities (Deshpande 2005).

8. **Hacker:** Skilled computer programmer who breaks (hacks) a password code, or otherwise gains remote access to a protected computer system, mainly for the thrill of it. Unlike a 'cracker,' a hacker may or may not also perform a criminal action such as alteration or stealing of data, or transfer of funds (Deshpande 2005).

9. **Client**: Hardware device (such as a personal computer) or a software application (such as a word-processor) that requests and makes use of services (such as file-transfer and storage) provided by another computer called the

server. Normally, a user interacts (interfaces) only with a client whereas the server might be out of sight (Stallings 2007).

10. **Decision Making**: The thought process of selecting a logical choice from the available options. When trying to make a good decision, a person must weight the positives and negatives of each option, and consider all the alternatives. For effective decision making, a person must be able to forecast the outcome of each option as well, and based on all these items, determine which option is the best for that particular situation (Gold and Shadlen 2007).

11. **Risk Assessment:** As a component of risk analysis, it involves identification, evaluation, and estimation of the levels of risks involved in a situation, their comparison against benchmarks or standards, and determination of an acceptable level of risk (Eom, Park et al. 2007).

12. **Access Control:** The Access Control can be defined as the degree to which the system limits access to its resources only to its authorized externals (e.g., human users, programs, processes, devices, or other systems) (Firesmith 2004).

13. **Virus:** The virus is a piece of programming code inserted into another programming to cause some unexpected and, for the victim, usually undesirable event. Viruses can be transmitted by downloading programs from websites. They can be sent by other users via e-mail, or in recent cases, can identify vulnerable systems and infect them through a network or the Internet. The virus lies dormant until circumstances cause its code to be executed by the computer. Some viruses can be quite harmful, erasing data or causing your hard disk reformatting (Deshpande 2005).

14. **Worms:** The worms are designed to gain control over all of the endpoints such as servers or notebook and desktop computers in order to investigate an attack, steal data, send spam, or initiate a DoS attack. While the worms are primarily designed to sabotage endpoints, their scanning activities can overwhelm the network. For example, with SQL Slammer, User Datagram

Protocol (UDP)-based unicast traffic directed to multicast addresses caused high rates of network device processing Their slowed down regular TCP/IP traffic and leads to denials of services which are compromising both hosts and the availability of business applications (Deshpande 2005).

15. **DDoS Attacks:** A DDoS attack is propagated by a hacker targeting a network device. Once the hacker has control of the device, he or she can instruct it to flood the network, thereby preventing legitimate network traffic or disrupting connections to a specific system individual. DDoS attacks can also cause the destruction or alteration of configuration information and the physical destruction or alteration of network components (Deshpande 2005).

16. **Man in the Middle Attacks:** In a man in the middle attack, attackers abuse weak or nonexistent authentication mechanisms between two endpoints. In these endpoints, the attackers can view information passing back and forth, and can even modify or inject data going into such a connection. These attacks are used to intercept passwords, account numbers, or financial records (Deshpande 2005).

1.3 Outsourcing Monitoring Significance

There are some benefits of outsourcing security functions or part of them to provider. By outsourcing security to a provider, a company can improve the readiness of its systems to any threats while avoiding investments in resources and technology. Following are some of the benefits of company (client) in relationship with a provider:

- Cost savings: Cost savings could be a main driver for outsourcing security. With a provider, business continuity can be guaranteed for the most time of the year with minimal investments in resources and technology, which could result in big cost savings and revenue generation (Hulme 2001). Since, a provider offer same services to several other customers, it can offer those at a cheaper rate through economies of scale. A company can negotiate a decent service level agreement with a provider, which could ultimately result in big savings for the company.

- Staffing and accountability: “Outsourcing security offers economies of scale, but also economies of skill, since it would cost much to hire full-time security experts” (DeJesus 2001). It is hard to find security staff with expert knowledge. Shortage of security staff is rated as the number two reason companies are turning to provider (Hulme 2001). Also, it gets quite expensive to hire full-time employees to perform the security functions, especially for small and medium size businesses that cannot afford hefty salaries to the trained staff. There is one other benefit that could be achieved by using provider’s staff and that is accountability. Since a company does not have to maintain the staff records and other security related resources in their system, a MSS provider could help remove these resources off the balance sheet for flexibility.

- Expertise and experience: Provider are the people who deal with hundreds and thousands of potential threats more than a single organization does. Their job is to keep track of new and potential vulnerabilities for their clients. It is very much possible that a provider can respond to a threat better than in-house personnel will, as they might have already dealt with a similar issue for some other client. At the same time, the security technology is getting so complex that a trained security professional will most likely perform much better than inexperienced in-house personnel using trial and error method for implementation. A company can, thus, leverage the expertise and experience of a provider to respond to an incident in a timely manner.

- Facilities: Providers usually have a remote security operations center (SOC) to monitor and manage the security operation of the clients. The SOC are located in various parts in the country, and hence enable a provider to remotely monitor most of its client. SOCs are the physically hardened sites with a strong infrastructure (DeJesus 2001). A company can make use of a provider to utilize the facilities provided and increase their security level.

- Threat of new attacks: It is most likely that a security staff in a company might not be aware of new threats and vulnerabilities until they actually experience the attack. Security threats are rising and it is difficult to keep up with these new threats. (Hulme 2001).

- Round-the-clock support: An attractive benefit of hiring a provider is round-the-clock support. Depending upon the contract with the provider, the provider is responsible to provide support for the duration agreed upon in the contract. A provider can provide 24 by 7 for 365 days support through economies of scale. The main advantage of round-the-clock support is real-time results and no wait until an administrator identifies the incident that happened last night 6 hours ago.

1.4 Outsourcing Monitoring Risks

There are quite a few benefits of hiring a provider, which were discussed in previous section. However, there are some shortfalls of hiring a provider. The risks associated with hiring a provider are listed below:

- Trust: Trust plays a very vital role in the decision of outsourcing as the key security functions. It takes a while to build trust with the provider. (Hulme 2001) It is very true that a provider has access to sensitive client information and knows about vulnerabilities in the client's security infrastructure. Hence, some companies are hesitant and not comfortable with the fact that an outsider performs the security administration, a delicate and vital function of the organization. However, a confidentiality agreement between the two can help mitigate this risk (Allen, Gabbard et al. 2003).
- Ownership: Ownership and responsibility of security functions can, sometimes, become reasons for conflicts and finger pointing when an incident occurs. The client is usually the owner and the provider is responsible for the services that are agreed upon in the contract. There is a possibility of the client losing some control over security administration. Hence, the scope of services should be clearly discussed in the contract and SLA. To mitigate the risk the user security awareness and training should be conducted. Also more than one team should be made responsible for security tasks (Allen, Gabbard et al. 2003).

- Hidden costs and other effects: A MSS is a form of outsourcing, hence comes with risks such as hidden costs and other effects that a company cannot quantify at the time of negotiation with the provider. For example, answers to questions such as, would a provider provide the same level of service as in-house professionals would?, how does the provider prioritize the services while serving several other clients?, cannot be predicted at the time of contract signing [Allen et al., 2001]. To avoid such surprises, a company has to perform the due diligence and discuss these issues with the provider.

- Failure in partnership: Infrequent communication and lack of planning can cause the partnership to fail at any stage. Frequent communication and review meetings between the client and the provider can mitigate the risk. Like any other relationship, this relationship to needs a due care and attention.

1.5 Problem Statement

There are many problems concerning the outsourcing concept, these problems can be categorized into two categories, the first category is related to the client and the second category is related to the provider.

- The outsource software can be only needed in a specific department at an organization (client) so it is very important to give permission to that department to access that software without the other departments in order to reduce the cost of using the outsource software.

- One of the requirements of using outsourcing is that the outsourcing provider's staff should access the client's systems. Despite the goal of the outsourcing process, this means that the systems are subject to the risk of either outsourcing staff or others, such as hackers. So the provider's staff should access client systems only from specific parts. These parts should normally be subject to a risk review to determine their security status as part of any risk analysis procedure required by the client. The risk review should assess the premises against the client's physical security policy.

- Implementation and operation is the phase considered the most important phase, The time of taking actions or delivery of services into the client are very complex operation and risky one. So list of measures must be planned by the client to monitor the Provider's ability to take the right action in a timely manner.

- The most famous problems that may face the outsourcing provider are how to ensure the services deliverined to a client and ensure exposure to hackers, which could lead to increasing costs which may cause the loss, where the main aim of the outsourcing provider for all these operations is to achieve a certain profit.

1.6 Objectives

The aim of this thesis is to design a model for monitoring the LAN and WAN networks during the activities of outsourcing process in order to solve most of the problems and verifying the following goals:

- Monitoring all the activities in outsourcing process to ensure the success of the operations in this process.
- Reducing the cost of using services by applying some of permissions for that departments or users to access the services and not allowing the other departments.
- Identifying some of measures to monitor the Provider's ability to take the right action in real-time.
- Specifying the parts or areas of which that outsourcing provider’s staff should access client systems in order to avoid the risk of either outsourcing staff or others.

1.7 Thesis Structure

The remaining part of the thesis Consists of four chapters: Second chapter is literature review about outsourcing monitoring, services, relationship and models. The third chapter is research methodology which is applied in this thesis, that is port knocking, image processing. The forth chapter is the proposed model which is developed to monitor the outsourcing operations system. The fifth chapter is the conclusions and recommendation for future work.

Chapter Two: Literature Review

2.1 Related works

(Webb and Laborde 2005) identify a set of factors that make a relationship between both company (client) and its provider a successful relationship. And what a provider must do to ensure that the continuation of relationship with company (client). In addition, the authors discuss some of the factors which lead to successful relationship between the provider and the company such as approach, design and methodology. The authors describe the outsourcing relationship being an emotional decision in the first beginning time, so if the company (client) feels that the provider is taking care of outsourcing process or not, upon which the decision of relationship will be made to continue or not. The competition between outsourcing providers is fierce and leads to conflict in the coming years, this is because of the heavy presence of companies that provide outsourcing services.

Different phases of an outsourcing relationship come up with different challenges, and a relationship needs to be studied as a dynamic phenomenon. The outsourcing literature includes several models of outsourcing relationships in their development. In the extensive literature survey and analysis of the outsourcing literature, (Dibbern 2004) use a two-phases model(decision, implementation) comprising five stages (rationale for outsourcing, alternatives analysis, making the decision, initiating and managing an outsourcing relationship and assessment of outcomes). (Lacity and Willcocks 2001) model includes six outsourcing phases: scoping, evaluation, negotiation, transition and middle and mature phase. We found these models are difficult to apply to the provider's perspective, especially because we are mainly considering the social and cultural side of an outsourcing relationship and focus less on the legal and business aspects of it. Observing the temporal development of outsourcing arrangements from the provider's side, we noticed four main phases and a fifth additional one. These phases are:

1. **Initiation.** This phase mainly includes general marketing activities, active search for customers, answering RFPs (requests for proposals), and customer's acquisition.
2. **Establishment:** This phase is the real start of an outsourcing relationship; the provider and the client aim to reach a shared understanding of the product or service to be delivered in order to negotiate and sign the contract.
3. **Delivery**: This is the most important phase, when the actual product or service is developed and delivered. It involves the highest level of interaction between the provider and the client.
4. **Closing:** The product/service is signed-off and the relationship ends.
5. **Re-establishment:** Under some circumstances, especially if the customers were happy with the quality of the product/service, they might come back either for maintaining/altering the previously developed product, or for developing a different one.

(Ranganathan and Balaji 2007) identified common challenges in offshore outsourcing through interviews and case studies at 18 companies, with offshore services outsourcing projects in the United States. The common challenges include differences in language, culture and time zones that they have to contend with over and above differences in company cultures. More significant changes to the company services and business units are required for offshore services outsourcing than for domestic outsourcing, as the company and end-users have to work with an offshore team that is culturally different and multifaceted. Offshore outsourcing also includes risks such as loss of core knowledge and provider opportunism, which are compounded by the geographic distance between client and provider, as well as different laws and legal systems in the different countries. Concerns regarding data security and privacy, intellectual property protection and dispute resolution also accentuate challenges in services offshore outsourcing.

(Allen, Gabbard et al. 2003) The set of services offered by providers vary in ability to meet the companies (clients) security requirements which include the confidentiality, integrity, and availability information assets critical to the company's vision. So, it is important that the companies (clients) specify their security requirements and go to candidate providers to demonstrate their ability to meet them, although the companies are still at information security risk and business risk, but contracting with a provider allows it to share risk management and mitigation of approaches.

The process of outsourcing some of security services to a provider to manage these security services is often a good solution for information security responsibility and operations. The results from engaging a reputable and competent provider have the potential to be far superior to anything a company (client) can achieve on its own. Described in this section are reasons for contracting with a provider and some of the benefits that may be results from the relationship between the company and its providers. These factors can contribute in reducing the risks faced by the company (client) through a combination of risk mitigation and sharing between the client and providers.

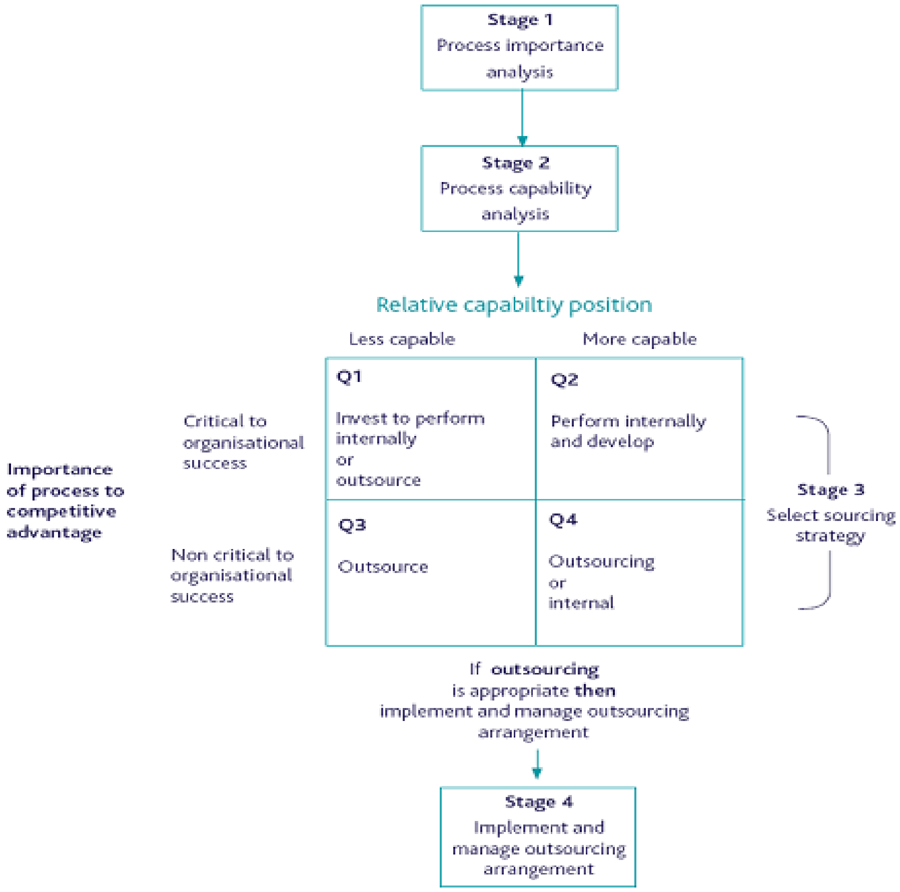
(McIvor, Humphreys et al. 2009) The successful process of outsourcing relationship requires some factors including the role of outsourcing process in addition to a significant improvement in the company. The outsourcing framework which shows in (Figure 2.1) illustrates the four stages in this process as follows:

Stage 1 Process importance analysis: This stage requires determining the level of importance of the processes that meet the customer needs. Identifying which processes are critical.

Stage 2 Assessing process capabilities: Determining whether a company can achieve good performance levels internally in critical processes on an ongoing basis is a very important area in outsourcing evaluation. This analysis is concerned with identifying the disparity between the sourcing company and the potential external sources.

Stage 3 - Selecting the sourcing strategy: The company must select the most appropriate sourcing strategy for all processes (critical and non-critical) in this stage there are four potential sourcing strategies for the process.

Stage 4 - Implementing and managing the outsourcing arrangement: In this stage, there are a set of issues to be considered in order to begin in implementing and managing the outsourcing relationship between the company (client) and its provider.



Stage 1
Process importance analysis
Stage 2
Process capability analysis
Relative capabiltiy position
Less capable
More capable
Q1
Invest to perform internally or outsource
Q2
Perform internally and develop
Q3
Outsource
Q4
Outsourcing or internal
Critical to organisational success
Non critical to organisational success
Importance of process to competitive advantage
Stage 3
Select sourcing strategy
If outsourcing is appropriate then implement and manage outsourcing arrangement
Stage 4
Implement and manage outsourcing arrangement

Figure 2.1: The outsourcing framework

2.2 The Importance of Computer Network Security

There are many reasons that the computer network security is important knowing that the biggest threats to network security over the past two years have been from viruses, worms, and Distributed Denial-of-Services (DDoS) attacks, which caused the most significant business disruptions and financial losses. Malware, spyware, and new multi-vector "turbo" worms are becoming increasingly sophisticated and their damage more divesting. The severity of these threats can be attributed to the dozens of vulnerabilities waiting to be exploited, the availability of worm source code online, recycled exploits, and the area of editing the existing worms. However, it is the secondary effect of worms and DDoS attacks that have wreaked the most havoc. Their propagation mechanism increase traffic loads and cause more processing on network devices (random scanning for vulnerable destinations, header variances, or unicast traffic sent to multicast addresses, for example). Many of the other types of attacks can also occur, such as brute force dictionary-based password cracking, unauthorized access or snooping of data from the wireless networks, and illicit use of telephony networks to gain access to free long-distance calling and pinpoint areas where security needs to be reinforced.

2.3 Challenges of Network Security

Security as it is traditionally defined in companies is one of the most pervasive problems that a company (client) must define. Rarely has there been a company issue, problem, or challenge that requires the mobilization of everyone in the company to solve. The sheer expansion of any problem that traverses the entire company poses many management challenges, particularly when the focus is on security. First, the most important areas of the company must be identified and targeted. This requires the company to take an inventory to determine what needs to be protected and why. In a large, complex company, this can result in the identification of hundreds of assets that are important to strategic drivers. Second, to secure this collection of company assets requires many skills and resources that are typically scattered throughout the company. Because security is a problem for the whole company, it simply is no longer effective or acceptable to manage it from the information technology department (Caralli and Wilson 2004).

2.4 Security Requirements

The specification of security requirements for systems has something in common with safety requirements. It is impractical to specify them quantitatively, and security requirements are often 'shall not' requirements that define unacceptable system behavior rather than required system functionality. However, there are important differences between these types of requirements(Sommerville 2007):

The notion of a safety life cycle that covers all aspects of safety management is well developed. The area of security specification and management is still immature and there is no accepted equivalent of a security life cycle.

Although some security threats are system specific, many are common to all types of the system. All systems must protect themselves against intrusion, denial of services, and so on.

Security technique and technologies such as encryption and authentication methods are fairly mature. However, using this technology effectively often requires a high level of technical sophistication. It can be difficult to install, configure and stay up to date. Consequently, system managers make mistakes leaving vulnerabilities in the system. Even though, these methods will be used in the side of provider in order to gain higher level of security.

The dominance of one software supplier in the world markets means that a huge number of systems may be affected if security in their programs is breached. There is insufficient diversity in the computing infrastructure and consequently it is more vulnerable to external threats. Safety-critical systems are usually specialized in custom systems, so this situation does not arise.

The conventional approach to security analysis is based on the assets to be protected and valued to an organization. Therefore, a bank will provide high security in an area where large amounts of money are stored compared to other public areas where the potential losses are limited. The same approach can be used for specifying security for computer-based systems with a possible security specification process.

2.5 Outsourcing Monitoring Services

The interesting part about companies providing MSS is that no two companies are similar in their backgrounds. Hence, they do not offer similar services. MSS providers are different types such as start-up companies, established companies, large telecommunication and computer companies, Internet and Application service providers and consulting firms (Amaladoss 2001). Therefore, the services offered by these companies can range from on-site consulting to remote security management. The services can be categorized as follows (Hunt 2001; Allen, Gabbard et al. 2003):

1. Perimeter Management and Network boundary protection: The service usually includes installation and maintenance of firewall, virtual private network, Intrusion Detection Systems (IDS).

   The provider is responsible for configuration and upgrading to the software and hardware protecting the network boundaries of the client.

2. Managed Security Monitoring (MSM): Managed Security Monitoring is more focused on the monitoring of the client's network. It deals with everyday monitoring of network and interprets the system events in order to identify any malicious activity on the network. Incident management and incident response process gets included under this category too (Hunt 2001).

3. Vulnerability assessment and penetration testing: This service includes periodic port scans, hacking attempts into the network in order to identify vulnerabilities that could be exploited by attackers.

4. On-site consulting: On-site consulting is a means of providing assistance to the client. It may include management activities such as risk assessment, identifying requirements of security, and development of security policy. It may also include technical support required to integrate and configure a security product. It may also sometimes include operational assistance such as executing incident response and recovery.

5. Compliance monitoring: The service includes monitoring of events to identify violations that may have occurred in a company. It also monitors any unauthorized changes to application server, web server and firewalls (Hunt 2001).

6. Anti-virus and content filtering services: Managed anti-virus services include scanning for virus, worms and malicious code on the desktop, scanning emails and network traffic. Spam filtering can also be added as an add-on to the contract with the MSSP. If a company wants to outsource its email services, it should also make sure that MSSP offers anti-spam functionality.

2.6 TCP, UDP and ICMP

TCP, UDP and ICMP are three of the most important networking protocols used regularly in modern networks. Transmission Control Protocol (TCP) is a stateful protocol that allows the two machines to create a connection between themselves and exchange information. A connection can be defined as two machines that have mutually 'agreed' to communicate. Such a connection is established by performing the 'Three-Way Handshake'. This can be compared to making a telephone call: the initiator dials the number, the receiver picks up and says "Hello?" at which point the initiator also says "Hello!" and the conversation can begin until it is ended by either end. Most applications, such as Email, Web Browsing, and File Transfers, use TCP connections to transfer information. The opposite of TCP is the User Datagram Protocol (UDP) which is stateless and so no formal connection is established between communicating hosts. This can be compared to a postal letter: the sender writes a letter and sends it off to its destination. The letter might arrive at its destination, or it might not, either way the sender will not receive any confirmation. A host sending UDP packets to another host will receive no acknowledgement as to whether or not the packets have been received, this makes UDP a lot faster than TCP, although far less reliable.

UDP is suitable for applications which require a rapid rate of transmission, and where reliability is not of up-most importance, such as Audio/Video Chat.

The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet protocol suite, and is used by networked computers to send error messages, for example when a specified port cannot be reached. In the case that a service is not available or a host cannot be reached, there is a number of ‘control messages’ that end hosts or intermediate routers can use in order to inform other devices of these errors. One example is the ICMP PORT UNREACHABLE (ICMP Type 3, Code 3) which informs a requesting host that the requested port cannot be reached for some reason. Applications do not tend to use the ICMP protocol directly (except for the ping command), but in certain cases ICMP can be used to transmit small amounts of information within the data field of the ICMP packet.

2.7 Methods for Protecting Networks

The usual method of limiting the sources of network connections is to use a Firewall. A Firewall works by selectively accepting or rejecting network packets based on their source addresses or other characteristics. Unfortunately, source addresses on packets tell little about the person who sent those packets; determined attackers are quite capable of disguising the source of packets that they send. Once a port on a Firewall is open to one host, any attacker could potentially use that opening. Also, not all authorized users have predictable IP addresses, so granting them access through a Firewall requires opening the Firewall to much or all of the Internet. Thus, while Firewalls are useful and effective defenses against many attacks, they are not complete solutions.

2.8 Threats against firewall authentication services

Authenticating users before allowing them through a firewall is beneficial in two situations, each of which assumes attackers with differing capabilities(Degraaf, Aycock et al. 2005):

1. As an extra layer of defense for critical services.
2. As a light-weight authentication service for insecure legacy services.

In the first case, such a service would be used to protect critical systems against attacks for which corrective patches or upgrades have not yet been applied or are not yet available. Assuming that patches and upgrades are supplied soon after the flaws are announced and deployed immediately, attackers must be assumed in this scenario to be dedicated and have access to significant resources, including novel (0-day) attacks. In particular, such attackers may be capable of subverting routers and inserting themselves between users and the authentication service.

The second case defends against a much less capable form of attacker. For various reasons, network administrators are occasionally required to allow remote access to legacy services over the Internet. Such services are frequently not securable by design, and may be proprietary. If privacy, integrity and authentication are required, then a system that supplies all three services is needed, like a VPN. However, if privacy and integrity are not required, then a simple authentication system would suffice, which would need to prevent attackers from masquerading as authorized users. Traffic interception or modification is not a threat in this case; since if attackers were capable of this, then they could attack the protected service directly by modifying authorized users' unprotected data streams. We take the conservative approach and assume in our threat model that an adversary has the more powerful capabilities relevant to the first model. In summary, we assume that an adversary can:

- Monitor and intercept all network traffic.
- Send packets with arbitrary source addresses.
- Replay captured network traffic.

Further, we are only interested in attacks that could cause the authentication system to incorrectly grant access to an attacker at an arbitrary address.

Chapter Three: The Methodology

3.1 Overview

The Computer networks rapidly grow in term of size and importance. If the security of the network is compromised, there could be serious consequences, such as loss data privacy, loss of information, and even legal liability. There are many types of potential threats to network security rapidly developing to make the situation even more challenging. When the network security is considered, the following three major factors should be considered:

1. The vulnerability: The vulnerability is the degree of network, device weakness such as routers, switches, desktops, servers and even security devices.

2. The threat: The threats are some people who find security weakness and gain advantage from this weakness, such individual can be expected to continually search for new exploits and weaknesses. The threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices.

3. The attack: The attacker's goal is to compromise a network target or an application running within a network. Many attackers use the following processes in order to get the valuable information for helping them accessing, using services, and retrieving the important data or information, these steps are:

   A. Perform footprint analysis (reconnaissance): A company webpage can lead to information, such as the IP addresses of servers. From there, an attacker can build a picture of the security profile or "footprint" of the company.

   B. Enumerate information. An attacker can expand on the footprint by monitoring network traffic with a packet, finding information such as version numbers of FTP servers and mail servers.

C. Manipulate users to gain access. Sometimes employees choose passwords that are easy to crack. In other instances, employees can be induced by talented attackers into giving up sensitive access-related information.

4. Escalate privileges. After attackers gain basic access, they use their skills to increase their network privileges.

5. Gather additional passwords and secrets. With improved access privileges, attackers use their talents to gain access to well-guarded, sensitive information.

6. Install backdoors. Backdoors provide the attacker with a way to enter the system without being detected. The most common backdoor is an open listening TCP or UDP port.

7. Leverage the compromised system. After a system is compromised, an attacker uses it to stage attacks on other hosts in the network.

3.2 Firewalls

Firewalls are an essential network component when it comes to controlling the flow of access in networked environments. In short, the goal of a firewall is to allow controlled connectivity between areas of differing trust levels, through the enforcement of a security policy and connectivity model, based on the principle of least privilege. Firewalls can be either hardware, which sits on a network between a trusted side and an un-trusted side; or software, which runs on the hosts themselves. In both cases the purpose of the firewall is to provide a logical barrier to prevent unauthorized or unwanted communications between different areas of a computer network.

The ‘Access Control’ mechanisms offered by a firewall rely on a set of administrator-defined rules, which are then applied to each and every packet flowing through the firewall. The default rule, which helps satisfy the principle of least privilege, is the ‘default deny’ rule where all traffic is rejected unless explicitly allowed. In this manner, one can be sure that no access is allowed except for the rules that specify an ‘allow’ condition. In most firewall packages there are two distinct ways that a firewall can deny traffic (Shinder 2003):

Way #1 Reject/Deny: Different firewalls refer to this rule as Reject or Deny although they both perform the same action. Using the REJECT/DENY rule will instruct the firewall to drop packets4 and send an ICMP PORT UNREACHABLE back to the initiator. The connection will be rejected, but the initiator will know that a host exists at that IP, and is denying access.

Way #2 Drop: Using the DROP rule instructs the firewall to be more silent in its denial. Packets that arrive are dropped without sending an ICMP PORT UNREACHABLE back to the initiator. The connection will be rejected, but the initiator will simply assume that no service is running on the target host (or that the target host does not exist).

As mentioned above, firewalls are purely access control mechanisms – with a fundamental lack of authentication. A firewall will simply compare an incoming packet to see whether or not its requested access is allowed by the firewall rules. There is no mechanism to allow or deny access based on some form of strong authentication of the user requesting access. Due to this, firewall configuration is either extremely restrictive (eg. access restricted to certain IP addresses), or unrestrictive (eg. anyone can access the FTP port). In such a way, it is difficult to configure a firewall to protect a host which must be accessible to clients whose IPs are not known prior to them connecting.

Established techniques to protect Internet-connected machines tend to rely either on filtering packets, or on application-level security. The first technique is implemented by firewalls, Internet-connected devices running software whose job is to filter or log unwanted network traffic. However, there are common attacks against which a firewall cannot protect. For example, firewalls do not protect against attempts to exploit bugs in application-level software. Such vulnerabilities occur because the Internet architecture assumes that services bound to a port should be accessible by any machine using the Internet protocols.

The second technique is to deploy high-strength application-level security mechanisms. However, authenticated services are built above the network layer [13, 6, and 16] and are often themselves subject to attack once discovered on a host. Reliance solely on application-level security exposes the problem of the computational expense of such security mechanisms. The high computational burden of commonly deployed cryptographic schemes leaves the server open to computational DOS attacks. Furthermore, complex schemes are error prone, as exemplified by the integer overflow bug in SSH which has been the target of recent attacks.

Alternative techniques, such as those used by next-generation Internet Protocols [1, 5, and 11] incorporate authentication headers at the network layer. However, these are still open to computational DOS, and their key exchange mechanisms also reveal the existence of the machine and the services it is running. Consequently, we argue that there is a need for computationally cheap and simple defense mechanisms that allow early rejection of the majority of attacks. In particular, we argue that there is significant benefit in having multiple, progressively stronger, layers of security, rather than attempting to have a single 'perfect' security layer. In more detail, when protecting a particular service:

1. The service should be hidden. This allows hosts to attempt to be invisible to other Internet-connected machines while still providing service to authorized parties.

2. Authorized source credentials should be easy to validate, yet difficult to forge. At the most basic level we can use identifiers from a sparse address space, but more generally we use a one-way authentication function based on some secret key. For the service to remain hidden, this stage should elicit no response if the credentials are invalid.

3. Full-strength application-specific security mechanisms are still used to provide true end-to-end authentication.

Although extremely lightweight, service hiding does deter attacks initiated by random port scanning, making it harder to exploit application-level vulnerabilities. This is not ‘security by obscurity’ rather; it is akin to authenticated signaling where application authentication information is included in the signaling message.

What is needed is a mechanism to open ports on a firewall to authenticated users, without allowing other traffic to pass. The obvious way to construct such a mechanism is to run an authentication service on firewalls, which validates the identity of remote users and modifies firewall rules according to per-user access policies. Such a service could be used for a number of purposes, including:

- Making services invisible to standard port scans.
- Providing an extra layer of security that attackers must penetrate before accessing or breaking anything important.
- Acting as a stop-gap security measure for services with known unpatched vulnerabilities.
- providing a wrapper for legacy or proprietary services with insufficient integrated security

There are a number of ways to create such an authentication service; one is to use “port knocking

3.3 The Port Knocking (PK) techniques

Port knocking is a clever new computer security trick. It's a way to configure a system so that only systems who know the "secret knock" can access a certain port. For example, you could build a port-knocking defensive system that would not accept any SSH connections (port 22) unless its detected connection attempts to close ports 1026, 1027, 1029, 1034, 1026, 1044, and 1035 in that sequence within five seconds, then listened on port 22 for a connection within ten seconds. Otherwise, the system would completely ignore port 22.

It's a clever idea, and one that could easily be built into VPN systems and the like. Network administrators could create unique knocks for their networks, and only give them to authorized users. It's no substitute for good access control, but it's a nice addition. And it's an addition that's invisible to those who don't know about it.

Those unaccustomed to host-based networking sometimes have trouble coming to terms with the notion of a 'port' on a computer. In the simplest of terms a port is a virtual door (represented by a 16-bit integer) which allows the computer to keep track of which pieces of data is destined for which application or service. A computer has 65535 of these ports (Stallings 2007). Networking (transport layer) protocols such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) both use the concept of a port when transmitting packets to and from networked hosts. Some other protocols such as ICMP, however, do not use ports when transmitting information.

The port number (when used) is included in networking packets and is interpreted not only by sending and receiving hosts, but also by intermediate routers and firewalls. A firewall can be configured to allow or deny certain packets based on their destination port.

When a service is listening for requests on a port, that port is said to be open, and clients can connect to the service. If no service is listening, then the port is considered closed. A client cannot connect to a closed port. Many ports, especially those within the 0-1023 range, are reserved for use with specific services. The vast majority of web servers, for example, run on port 80. There exist many services with their own port numbers such as File Transfer Protocol (port 21), SSH (port 22) and the Post Office Protocol (port 110). Although these port numbers are 'reserved' for those services, it is still possible to run a web server, for example, on port 22, if the administrator felt like doing so. The Internet Assigned Numbers Authority (IANA) is responsible for assigning TCP and UDP port numbers to specific services, and their list of officially assigned port numbers is regularly updated.

The name "Port Knocking" originated with Martin Krzywinski in 2003 (Krzywinski 2003), and refers to the concept of sending packets to predetermined network ports, essentially forming what can be compared to as a 'secret knock' on those ports.

In computer networking, PK is a method of externally opening ports on a firewall by generating a connection attempt on a set of prespecified closed ports. Once a correct sequence of connection attempts is received, the firewall rules are dynamically modified to allow the host which sent the connection attempts to connect over specific port(s). The following figures below illustrate the PK mechanism.

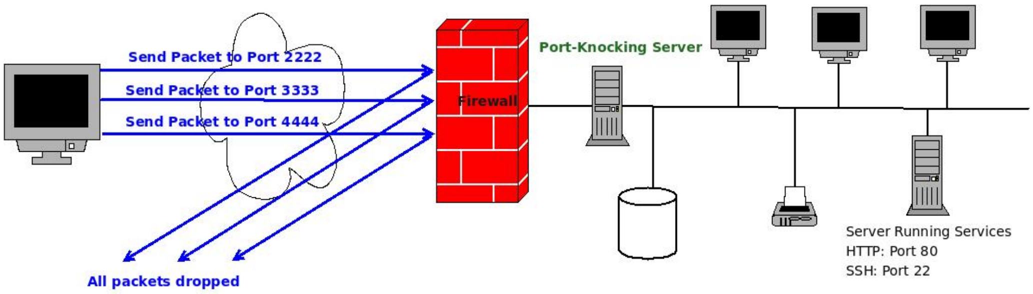


Figure 3.1: the firewall uses a default drop policy

In Figure 3.1, the firewall uses a default drop policy. It shows 3 knocks (packet) sent to predefined ports (2222, 3333, and 4444), and all 3 knocks are dropped.

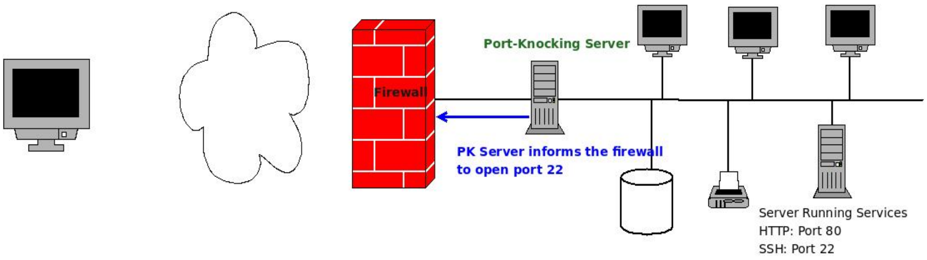


Figure 3.2: PK server informs firewall to open a predefined port number

In Figure 3.2, the PK server informs the firewall to open port 22 according to a predefined configuration between the PK server and the client requesting a service. Because all three knocks where received in the correct predefined sequence based on the configuration.

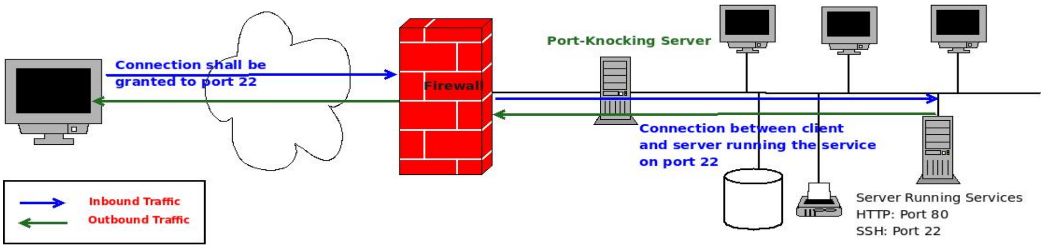


Figure 3.3: PK server runs a service to a predefined port number

In Figure 3.3, the client is able to communicate with the server running a service on port 22.

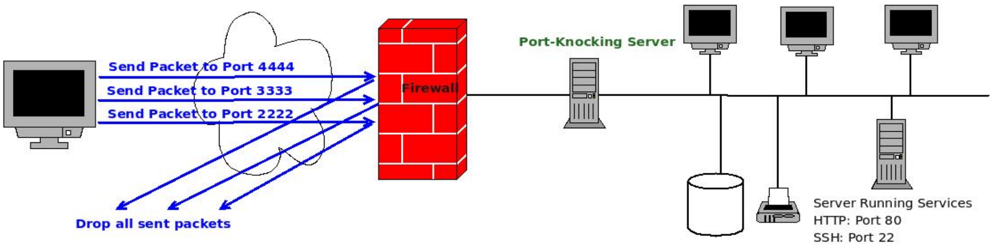


Figure 3.4: PK server informs the firewall to close an opened port.

Figure 3.4 shows 3 knocks sent to predefined ports (4444, 3333, and 2222), and all 3 knocks shall be dropped. These three knocks are needed to close the port, because the connection is no longer needed. Therefore the PK server shall close the open port 22, which means closes the connection.

3.4 Three-Way Handshake

The Three-Way Handshake is the protocol that computers use in order to establish a TCP connection with each other.

1. The initiating machine will send a ‘Hello’ (formally called a SYN) packet to a specified host on a specified port. For example, if you browse to http://www.foo.com, your computer will first send the server a SYN packet on port 80 (the default web server port) to the server at www.foo.com. If port 80 is

not open on the web server, then your client will not receive a reply (and the connection will fail).

2. However, if port 80 is open, then the web server is listening and will reply to the client with a SYN/ACK packet, acknowledging that it received the first (SYN) packet and requesting a confirmation to complete the connection.

3. Finally, the client will send back an ACK packet, signaling that it confirms the connection.

At this point, both computers keep track that they are connected to each other. It is also important to note that some machines will only log a connection1 once the full Three-Way Handshake has been performed. The connection is ended by one side or the other, by sending a FIN packet to the other end, who then replies with a FIN&ACK packet, and finally the initiating side sends back a final ACK packet.

3.5 Steganography

The word steganography is of Greek origin and means "covered, or hidden writing". Its ancient origins can be traced back to 440 BC. Steganography is the art and science of writing hidden messages in such a way that no-one apart from the sender and intended recipient even realizes there is a hidden message, a form of security through obscurity (Menezes, Van Oorschot et al. 1997). By contrast, cryptography obscures the meaning of a message, but it does not conceal the fact that there is a message. In digital world, the term steganography includes the concealment of digital information within computer files.

For example, the sender might start with an ordinary-looking image file, then adjust the color of every 100th pixel to correspond to a letter in the alphabet—a change so subtle that someone who isn't actively looking for it is unlikely to notice it.

3.6 Mutual Authentication or two-way authentication

Mutual authentication (or two-way authentication) refers to two communicating parties authenticating each other suitably. In technology terms, it refers to a client or user authenticating themselves to a server and that server authenticating itself to the user in such a way that both parties are assured of the others' identity.

3.7 Hybrid Port-knocking (HPK)

The PK techniques have been studied by many researchers and they developed their models trying to avoid all possible types of port attacks that may threat network security. PK techniques can be used for efficient, reliable, and cost-effective host authentication. The new PK technique for host authentication can be applied. The technique should avert all types of port attacks and meet all other network security requirements. It utilizes three well-known concepts, these are: PK, steganography, and mutual authentication, therefore, it is referred to as the hybrid port-knocking (HPK) technique (Al-Shamary 2010). Since the concealment technique shall be applied through the mixing of the above three concepts, therefore the following suctions are the description of the three concepts used together with the proposed technique. The hybrid port-knocking (HPK) technique consists of four main steps. In the following subsections are the descriptions of the four steps:

Step1: Traffic monitoring

In this step, a PK server is installed behind network firewall monitoring and checking traffic arrived to firewall (gateway), as shown in Figure 3.5.

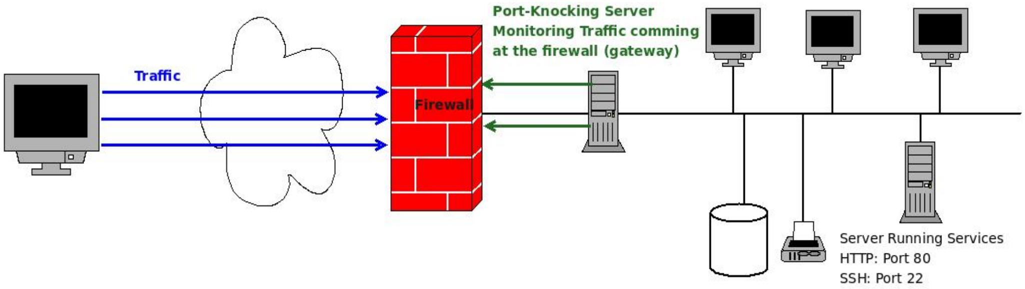


Figure 3.5: Traffic monitoring.

Step2: Traffic capturing

In this step, the PK server captures only traffic that contains images (pictures) for further processing, as shown in Figure 3.6. In this figure, for example, only Traffic #3 is captured for further processing because it contains images.

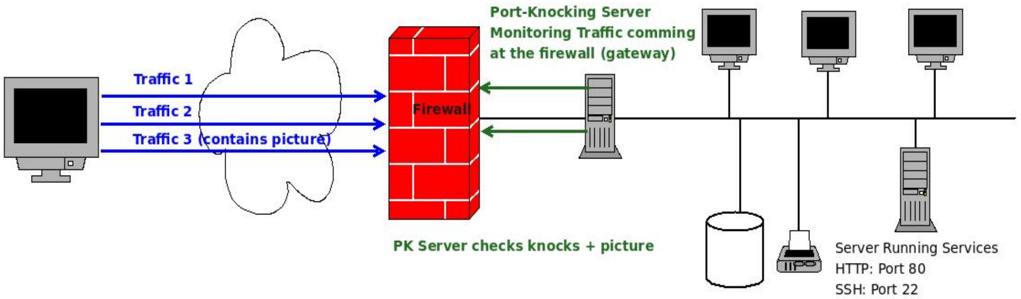

Port-Knocking Server
Monitoring Traffic comming
at the firewall (gateway)
Traffic 1
Traffic 2
Traffic 3 (contains picture)
Firewall
PK Server checks knocks + picture
Server Running Services
HTTP: Port 80
SSH: Port 22

Figure 3.6: Traffic capturing.

Step3: Image processing

In this step, the PK server processes the captured image, which supposes to hide some information that can be used to prove the knocker identity (steganography). If the image contains correct information then either demand the firewall to open a port for the client, or send the remote commands request to the appropriate server Figure 3.7. Otherwise, if the result of image processing fails to reveal valid authentication parameters, the PK server blocks the IP address of the source that sent the knocks and the image.

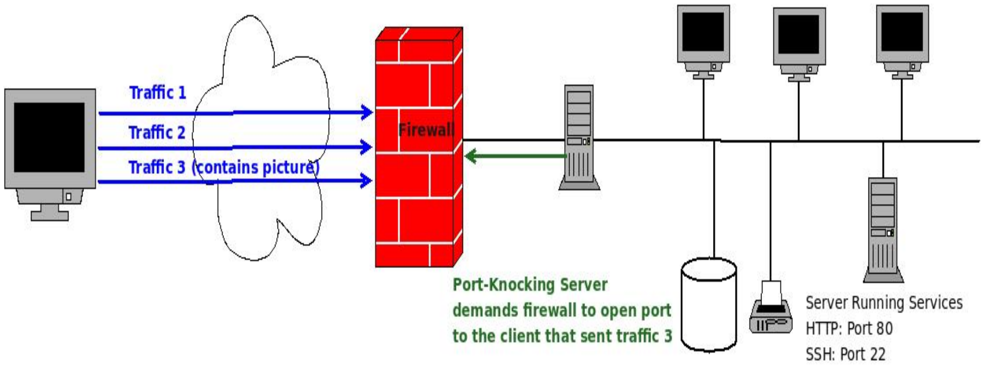


Figure 3.7: Traffic processing (request processing).

Step4: Port Closing

Finally, in Step #4, after task is completed, either the client informs the port-knocking server to close the port, or the PK server decides to close the opened port after specified silent period on that open port Figure 3.8. In any of these two cases, the PK server demands firewall to close the open port. In this case, if the client wants to access the system, it needs to initiate new access or authentication request, i.e., start from Step #1.

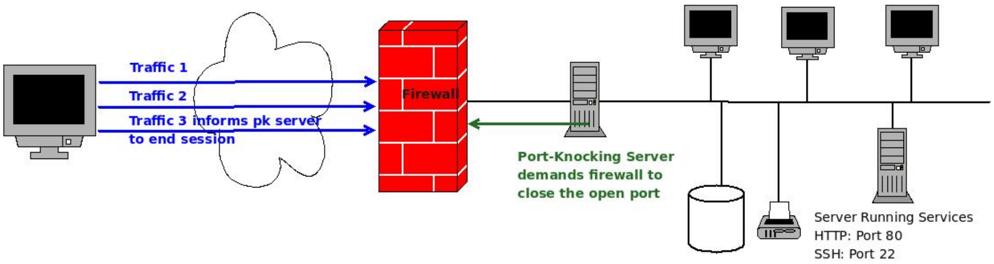

Traffic 1
Traffic 2
Traffic 3 informs pk server to end session
Firewall
Port-Knocking Server demands firewall to close the open port
Server Running Services
HTTP: Port 80
SSH: Port 22

Figure 3.8: Port closing.

Chapter Four: Proposed Model for Outsourcing Monitoring System

4.1 Overview

This chapter presents a new model for Outsourcing Monitoring System (OMS) for both the owner of resources (provider), and the user of the resources (client), and the relationship between the client and the provider. Usually the monitoring system for the outsourcing operations have many relationships between the client and the provider, these relationships have been considered in order to solve the set of outsourcing system problems, especially those problems mentioned in the problem statement in chapter one. The model consists of three sub-models: the Client sub-model, the Provider sub-model and Provider-Client relationships sub-model, as shown in figure 4.1.

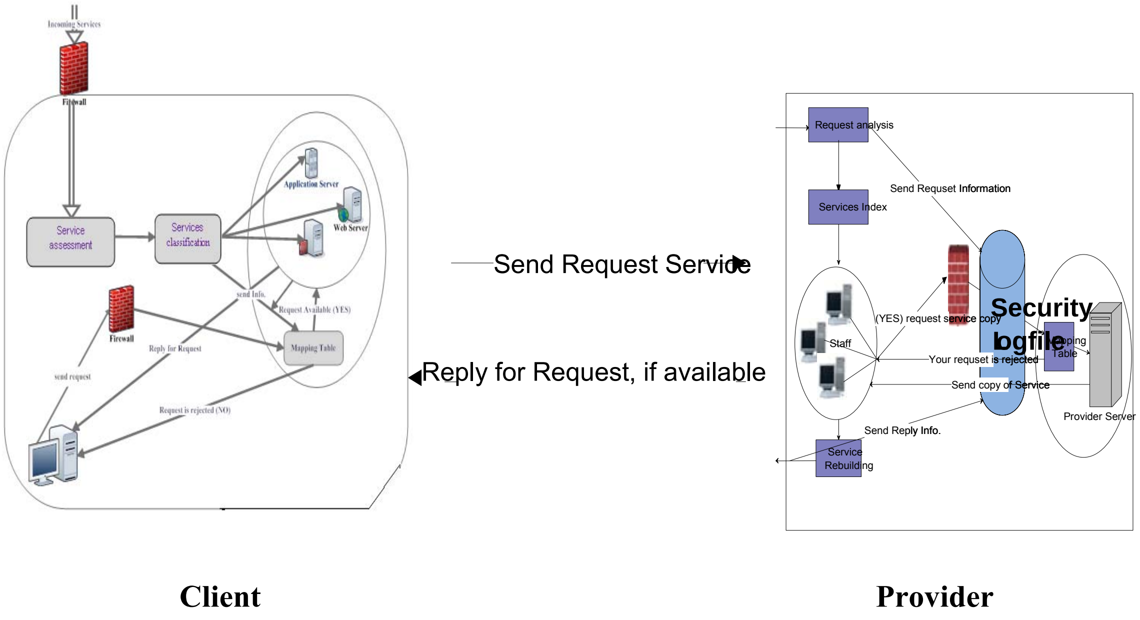


Figure 4.1: Outsourcing Monitoring System

4.2 Client sub-model

Figure 4.2 presents Client sub-model which consists of three modules, these are service assessment module, services classification module, and mapping table module. This model is design in order to deal with the distributing of the outsources (services) to the specified departments by set of rules, in order to ensure the quality of services, protecting services, and reducing the cost of outsourcing services that results from using the services by departments or users who are not in real need to it. Detailed description of these modules is in the following sechons.

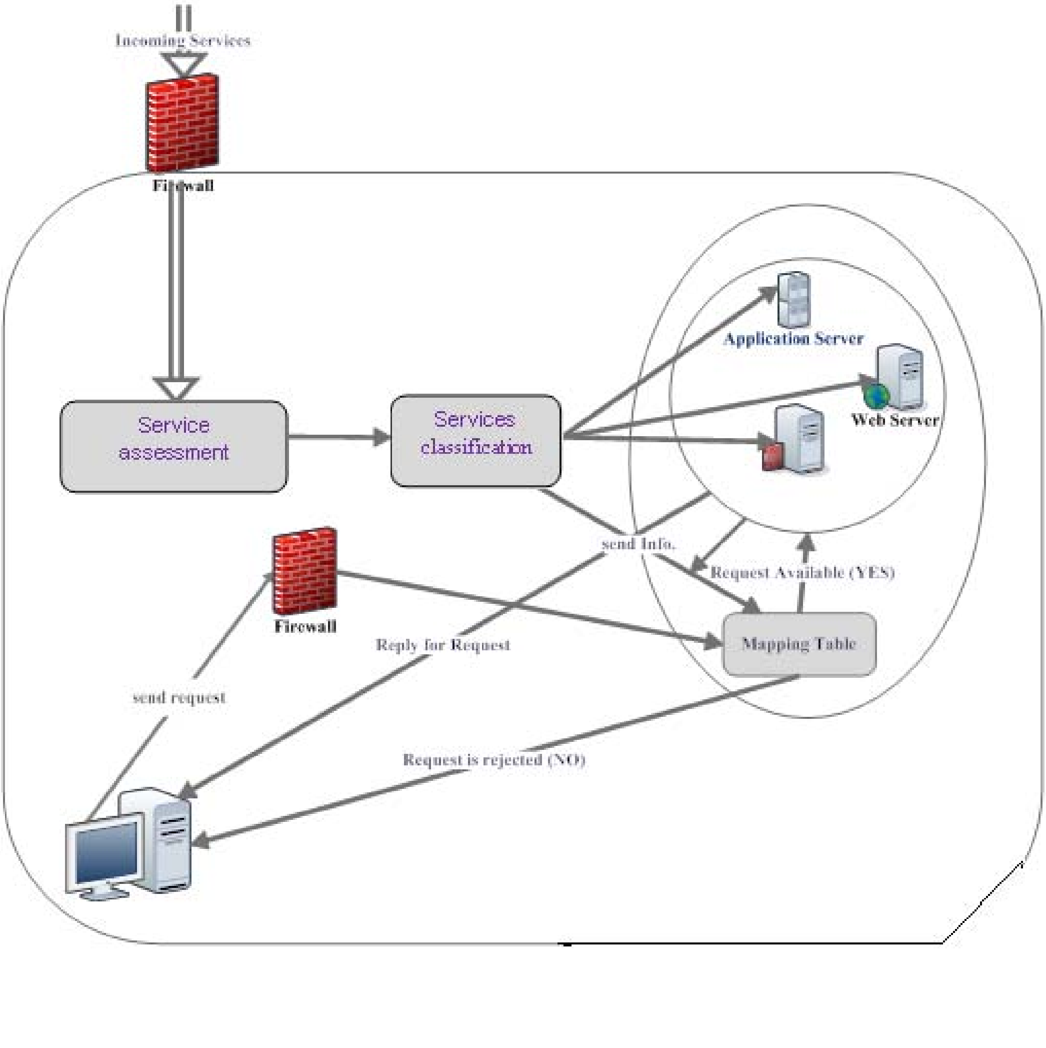


Figure 4.2: **Client Sub-model.**

4.2.1 Service Assessment Module

The process of sending the services by provider to company (client) is considered as the first tangible response. So the client must take some procedures to assess these services such as readiness services, the compatibility of these services with the nature of the company structure and work, and source of services. The expected result from this process is one of the following options:

1. Accept the services
2. Reject the services
3. Record some of observations
4. Provider assessment.

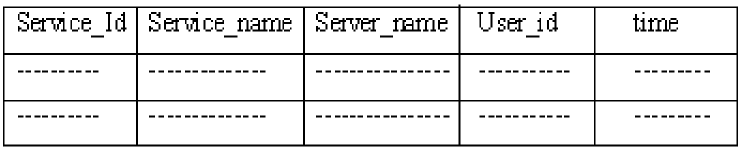
4.2.2 Services Classification Module

The accepted services included in the classification process, which involve classifying the services according to the nature of those service are: tools, software, technologies and policies, and distributing these services to the company (client) servers. The process of classifying each service involves giving this service an identifier to distinct it, and sending some information (including the given identifier) about this service into the mapping table in servers to ensure the accessibility and some of the constraints.

In addition, the service identifier must reflect the providers identifier (suppose that there are many providers), services category number and a sequence of this service. This identifier combined with service name and name of server where the service is stored to send them into a mapping table to update the client database.

4.2.3 Client-Mapping Table module

Mapping table is a table to store some information about the services in servers to ensure the accessibility and constraints. This table as mentioned earlier receives some information resulted from the services classification process. The structure of the mapping table is a number of fields that consist of the received information from classification process and some information inserted by IT staff in company (client) such as the user identifier authorized(it may be the IP address), time of using. Figure 4.3 shows the full structure for mapping table.



Service_Id	Service_name	Server_name	User_id	time
---------	-------------	---------------	----------	---------
---------	-------------	---------------	----------	---------

Figure 4.3 Mapping Table Structure

Following are the seven steps representing summary of the process of this module.

Step1: The service sent by the provider to the company (client).

Step2: The received service including services assessment, which may be accepted or rejected.

Step3: The accepted services including the process of services classification that classify the services provided in the mapping table with the necessary information.

Step4: The IT staff company (client) updates the mapping table by inserting some information as shown in the previous Figure 4.3.

Step5: If any user requests a service from the server, this request (if accepted by firewall) passed through the mapping table in the server to check if this user is among those authorized to use this service or not.

Step6: if the checking result is "NO", the server will send a message for the user telling him "SORRY: YOU DO NOT HAVE ACCESS ON THIS SERVICE".

Step7: if the checking result is "YES", the server will give access to this service for this user.

4.3 Provider Model

Figure 4.4 presents the provider model which is the set of processes or operations that must be monitored by the provider company network in order to achieve the set of provider company objectives. There are multiple operations and processes inside the provider company that reply to the requests of outsourced companies (clients). These processes will be called as modules and in the following subsections are detailed descriptions of them.

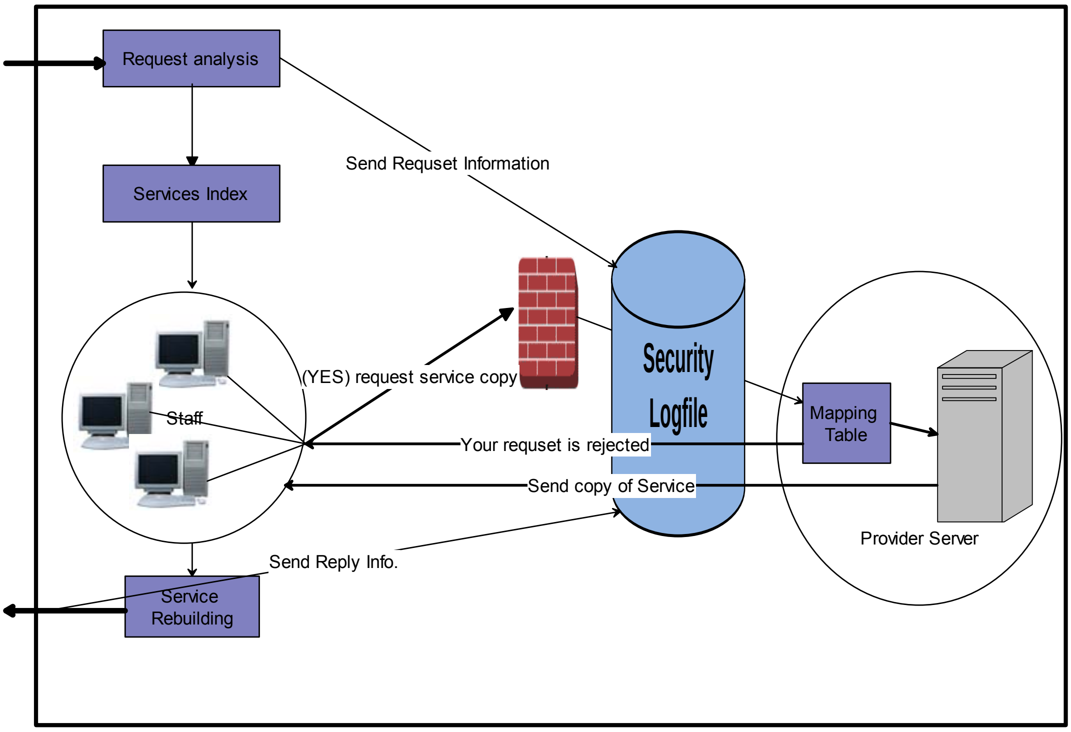


Figure 4.4 Provider Model

4.3.1 Request Analysis Module

When the provider staff receives the companies (clients) requests, they will analyze the requests in order to be able to reply to these requests. This analysis involves distinction of the request type (service, type, security status). Also the analysis involves the request information analyzing. The request information format must be observed in relationship agreement which must be identifying the list of services types that are included in the agreement, each service must be identified by be the service identifier, description, type and so on. The result of this process is either request accepting or request rejecting according to the relationship agreement.

4.3.2 Services Index Module

One of the advantages of outsourcing relationship is that the provider can keep track of services in provider server which is developed to solve some problems in many companies (clients). These services must be indexed in order to back them when needed. Therefore the staff must go back to the services index to see if this request type was replied to last time. If the result is positive, the staff can send request for the server to get a copy of this service. Otherwise the provider staff must develop this service according to the relationship agreement.

4.3.3 Request Copy of Service Module

The provider staff send request for server to get a copy of the service through the firewalls which enroll some of the steps to ensure the right connection, such as port knocking (PK) server and technique which use drop policy to reject the connection or open the connection so the staff can request a service.

4.3.4 Provider-Mapping Table Module

The accepted service request will include in the table mapping a spare procedure to ensure that no one from the staff can get in the services from server except the authorized staff. The mapping table in the provider server consists of services that available to serve the clients (outsourced companies) requests indicated in the service index. Each service is identified by service identifier, service name, description, and users or staffs who are authorized to read it. The structure of the mapping table shows this in figure 4.3. So the result will be either accepting the request and sending back a copy of the service for the company staff or rejecting the request and sending back a message to tell them so.

4.3.5 Security Log files Module

The transaction in the company must be recorded in a security logfile, following are some of the translation types that must be recorded in security logfile:

1. Outsourced company (client) request information: such as company name, company identifier, request time, request type.
2. Staff requests: each staff request information (request time, staff ID, request result (accept, reject), IP address).
3. Staff request reply: reply time, receiving IP address, port number.
4. Replies for outsourced company (client): time, receiving IP address, port number, type of service (reply).

4.3.6 Service Rebuilding Module

Set of services which are available in the provider server may be needed to updated or rebuild according to the service description of the outsourced company (client). On other side, if the requested services are not available in the provider server, then the staff must build these services in order to meet the outsourced company (client) requests according to the relationship agreements. In all cease all of building or rebuilding services must be stored in the provider server and indexed in service indexing to back them when needed. Following is the summery of the processes of the provider model.

- The provider side receives the request from the outsourced company (client) if the connection is accepted by firewalls and set of used techniques.
- The received requests are analyzed to extract the requests information then take the right decision.
- The requested services are scanned by the services index to check if these services are available in the provider server or if these services are developed in earlier time.
- Provider staff send request to the server to get a copy of the available in the server according to scan the results in services index process.
- The staff request is checked by passing it to the mapping table to ensure the staff authentication of these services.
- If the staff requests are accepted, the provider will send services copy to the staff.
- The received services are rebuild, if needed, and sent to outsourced company (client).
- The staff sends copy of new built services or rebuilt services to the provider server to be stored and indexed in services indexing.
- All the transactions in provider LAN are recorded in the security logfile.

4.4 Provider-Client Relationships Model

This sub-model demonstrates the processes of managing the relationship between the client and the provider. In addition, this sub-model represents the series of operations or processes which happen when both company (client) and provider are connected. Figure 4.5 presents the first step when the outsourced company (client) request from the provider company to open connection in order to send services requests.

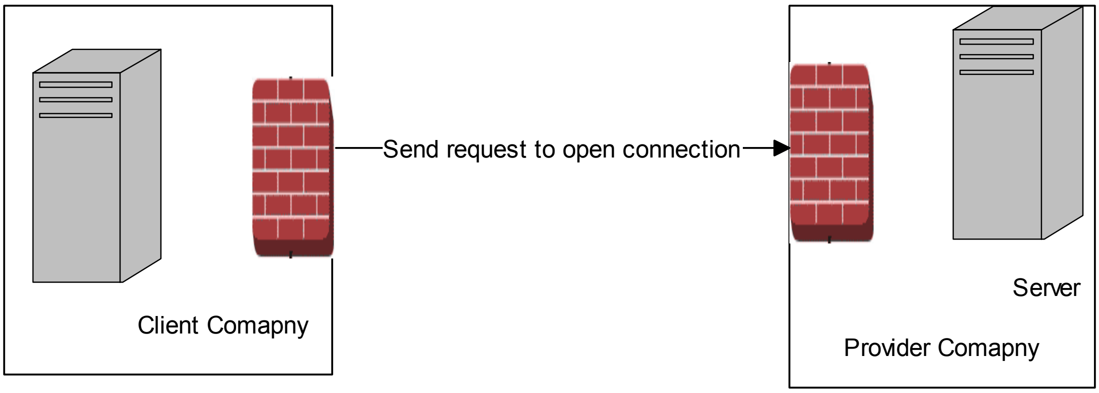


Figure 4.5: Client request to open a connection with provider

In the provider side, if the connection is illegal, the firewall drops the request and tells the client side as shown in Figure 4.6.

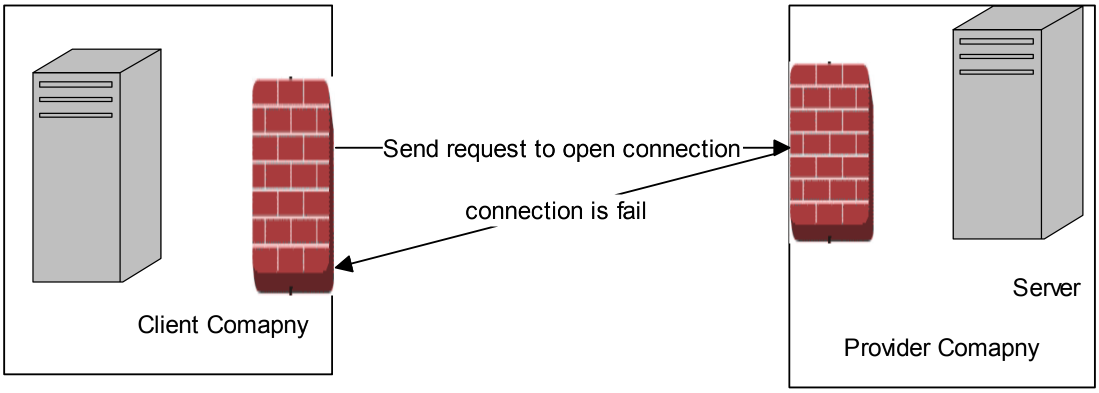


Figure 4.6: Client request is canceled.

The client side must use some functions to send the connection request such as capturing image and image processing or hash function, all of these in order to ensure that the authentication of connection and no attacks will happen. In other case, if all the connection parameters are correct, then the PK server will give approval to open the connection process on port #x. also all connections requests and replies are recorded in both company and provide logfiles. See figure 4.7

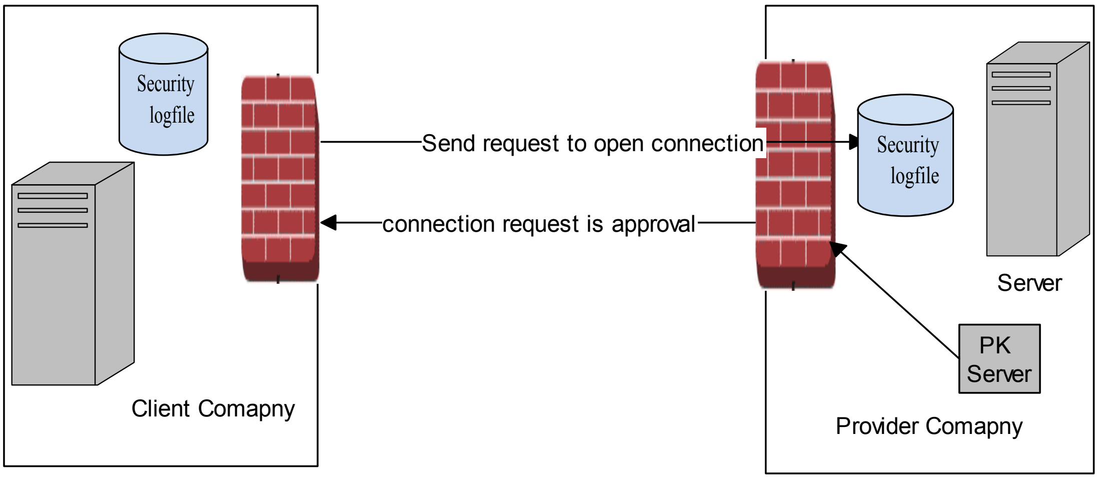


Figure 4.7: Client request is Approved.

When the outsourced company (client) receives the approval of the communication process, it begin to send services requests to provider company as shown in figure 4.8:

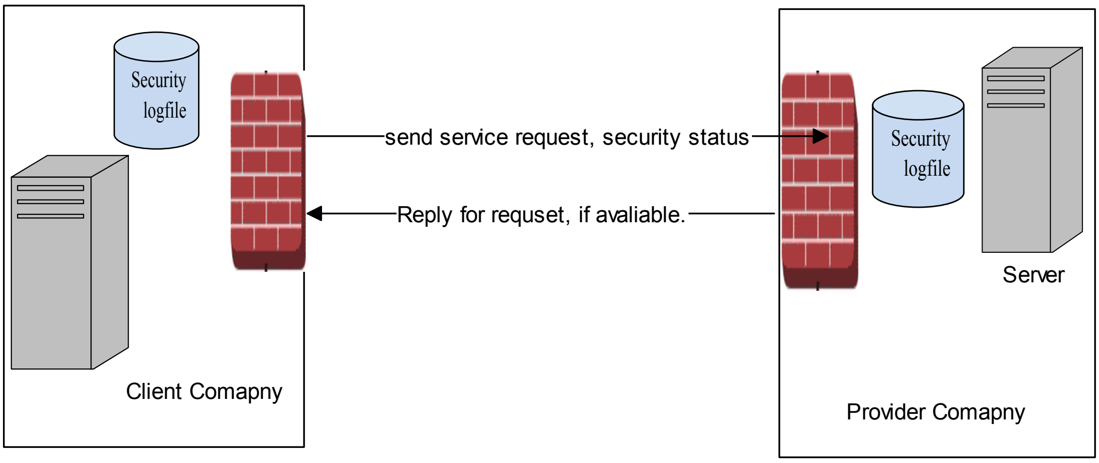

Security logfile
send service request, security status
Reply for requset, if avaliable.
Security logfile
Server
Client Comapny
Provider Comapny

Figure 4.8: Services Requests.

Many events may occur when the companies connect to Internet. These events may damage or corrupt in customers, partner's data or operations. All these events must be recorded in the security logfile in the company (client) network. In outsourcing operations process the company (client) IT staff must remove the sensitive data from these logfiles before sending it to the provider such as identification of communication partners, or authorization information in order to ensure of the privacy data. The operation of sending those logfiles is done periodically or in real-time, the provider (as MSSP) analyzes those logfiles and sends back security status for the company (client), with some warning alerts or services with reference to the identities of these attacks to take the appropriate action against them.

Managing the outsourcing relationship is similar to the operation of database log transaction. In log transaction each modification process is recorded in this logfile. Also in outsourcing operation a logfile must be created to record information related to events in network security outsourcing monitoring operations. Logfile must be evolved to contain information, so many logfiles may be created in the same outsourced company to save information related to network security such as authentication logfiles, device logfiles and security logfiles to track possible threats.

Number and forms of network security logfiles have increased because of increasing the network devices, computers and attacks. This is leading to logfiles management for the process of the logfiles creation, logfile storage, logfiles analysis and logfiles deleting.

Logfiles are created to track large amount of information related to network devices or systems, so the logfiles are classified either to security software logfiles to track information related to security information or OS system logfiles, and application logfiles.

The relationship between both the company (client) and the provider is confined in two operations: 1. sending requests (services) or security data to be analyzed. 2. Receiving of services or security status.

Also, all the sent and received data between the client and the provider must be recorded in security logfiles to return to them when both need it. So there are some directions that must be defined in agreement to help both the provider and the client:

1. Logfile formats and types: logfiles type and formats must identified before the beginning of outsourcing relationship to facilitate reading these logfiles by both client and provide, to facilitate analysis of logfiles by the provider, and to facilitate choosing the appropriates techniques for analysis logfiles.

2. Logfile Protection: Outsourcing logfiles contain information and records about network components: devices, applications, web, e-mail and operating systems. So these logfiles must be protected from attacks. On the other side, the clients must protect their sensitive information from others or from outsourcing monitoring provider because these logfiles may contain special entries or information for example: e-mail information, or user's login authentications. The client must control the access to logfiles or update records, and entries, especially from the provider. Also the provider and the client must keep the logfiles from overwriting old data when the size limit is touched. So the outsourcing provider and clients must keep copies of old logfiles required to create archives.

3. The separation of multiple logfiles: How the provider can deal with multiple logfiles and multiple formats?

4. Provider Privacy: The provider is responsible for building an integrated security system to protect its network as discussed in the methodology chapter, there are some approaches that can be used by any network administrators in order to ensure that data privacy of: port knocking (PK), image processing, Traffic capturing, cryptography ,.., etc.

The above full model in Figure 4.1, which represents the relationship between outsourcing security provider and client or multi-clients, is leads us to a new process or a new life cycle, which illustrates the processes or operations that must be done in each time period or in a few minutes. These operations summarize the outsourcing monitoring security model into a new life-cycle as shown in the handling process, Figure 4.9 as follows:

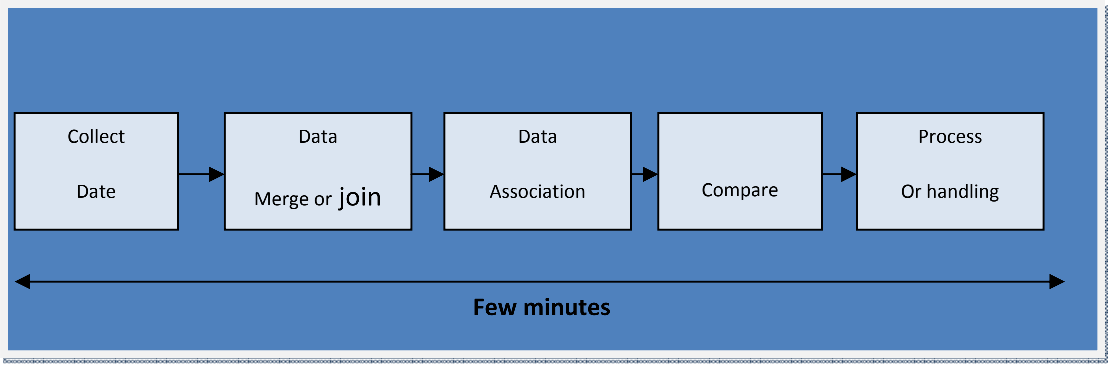


Figure 4.9: **Handling Process**

1. **Collect Data:** as it is visible in the outsourcing monitoring security model the data is collected from all devices in the client network and saved in multiple logfiles in the client network. These logfiles must have the same format in the same network.
2. **Data merge or join**: the data collected is combined in a single logfile and stored in network management point such as servers and others in the same format as in the provider logfiles.
3. **Data Association:** The consolidation data is processed and reduced to be analyzed to know the nature of attacks, if there is any, and the kind of threats. Note that there may be thousands of questions and analysis on these data to image or define the attacks or problems.
4. **Compare:** The attack which may be known in the previous stage is compared by the outsourcing provider with the attacks and threats or vulnerabilities that the provider suggests or knows that the client has had before.
5. **Process or handling:** The provider processes these vulnerabilities and uses this point to avoid it in other network clients, or by the same client in next-times

Chapter Five: Conclusions & Discussion

1.1 Conclusions

The outsourcing system is a sensitive relationship between an outsourced company (client) and a provider company. So it is necessary for both the client and its provider to build a system to monitor the operations in this relationship, because both sides of this relationship are responsible for the success of all operations, and achieving all the goals. In this research, a new model has been developed for monitoring the outsourcing system in order to solve some problems in outsourcing system. The first part of this model, the client sub-model, is designed to ensure dealing with the distribution of the (services) to the specified departments by set of rules, in order to ensure the quality of services, protecting of services, and reducing the cost of outsourcing services. The second part of the model is the provider model that designed to achieve the set of the provider company objectives, such as access authorization on services and requests reply. The third part of the model is designed to focus on the connection procedure between outsourced company (client) and its provider, open connection, request of services, reply on service and close connection. Finally, a full model has been designed to integrate three parties to form a single model for monitoring the outsourcing system.

1.2 Discussion

As has been discussed in the previous sections, the outsourcing system holds many activities in both provider network and customer (client) network, and the relationship between them. In order to monitor the set of activities in the outsourcing system, a new model has been built of three sub-models: the first sub-model is concerned with monitor activities within the client network. The second sub-model is concerned with monitor activities within the provider network and the third sub-model is concerned with monitor activities in the relationship between the client and provider.

In this section, the aim is to evaluate the proposed model by comparing it with some models or outsourcing processes in order to show the strengths and weaknesses of the model. (Bendor-Samuel 2000) states that few users take the time to adequately define what it is they are buying. What usually happens is that the procurement process focuses on obtaining what is perceived as a good price, leaving the definition of the scope of the services for the provider to establish after the user has trained the provider. In these cases the provider determines, during the course of the agreement, what its scope of work is. A more prudent approach is for the user to establish the scope of the services before approaching a provider. This process should be started by defining what contributions are required of the provider. When assessing value, the user must understand what is valuable to them, for example low costs; however beyond that companies vary widely when defining value. Scope thus describes the boundaries of the process so that both parties can see clearly where one's responsibility ends and the other begins. A more thorough specification of the outsourcing needs of the company should be defined in order to ensure optimal benefit relationship and alignment with the initial intent of the outsourcing arrangement. In order to address this, a multi-sourcing approach or gradual bases outsource starting with non-essential parts can be considered and strategic components kept in-house.

The proposed model asserts that the necessary time and effort must also be spent on negotiating and establishing the outsourcing process, with respect to management structures and systems for monitoring and evaluating the relationship. The model state that regardless of how the activity is handled in-house outsourcing must be managed differently, often requiring new management. As has already been outlined, the outsourcing company must identify the required services level in order to measure the service provider accordingly, and management must monitor and evaluate adherence to the outsourcing agreement.

The outsourcing company (client) must also establish whether the provider has a good track record of service commitment, and this should be examined from multiple perspectives. The user should also ascertain how their account will be managed. Account management is an effective service in action and is a critical dimension of the outsourcing system. It is also useful to identify the provider's existing customers and their levels of satisfaction with service provided. Finally, the user must establish the quality of the provider's infrastructure and human resources.

Mapping table is a table to store some information about the services in servers to ensure the accessibility and constraints. This table as mentioned earlier receives some information which resulted from services classification process. The structure of mapping table is a number of fields consist of the received information from classification process and some information inserted by IT staff in the company (client) such as the authorized user identity (it may by the IP address) or time of using.

To ensure of the implantation of this model, the provider must also establish a server for port knocking (PK), in order to open the connection with the client; the PK server plays an important role in the process of authorization to open the communication process, as well as the provider needs to establish a new server to manage the indexing table that is concerned with the list of services that have been processed, sent, or develop.

1.3 Future work

In this thesis, there are some of areas that need to be studied in order to apply the proposed model in the real outsourcing relationship environment, such as mapping table which needs to observe its structure and management. Also logfiles, services classification process needs to be studied in details in the future.

References

- Allen, J., D. Gabbard, et al. (2003). Outsourcing managed security services, CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

- Al-Shamary, D. A. H. (2010). "A Hybrid Port Knocking System." PHD Thesis, Arab Academy for Banking and Financial Sciences.

- Amaladoss, B. (2001). "Managed Security Services–An Evolving Security Solution!" Sans Institute (sezione Reading Room) **8**.

- Caralli, R. and W. Wilson (2004). "The Challenges of Security Management." Networked Systems Survivability Program, SEI.[cited 2007 12th March].

- Degraaf, R., J. Aycock, et al. (2005). Improved port knocking with strong authentication.

- DeJesus, E. X. (2001). "Managing managed security." Information Security Magazine, gennaio.

- Deshpande, D. (2005). Managed security services: an emerging solution to security, ACM.

- Eom, J. H., S. H. Park, et al. (2007). "Risk assessment method based on business process-oriented asset evaluation for information system security." Computational Science–ICCS 2007: 1024-1031.

- Firesmith, D. (2004). "Specifying reusable security requirements." Journal of Object Technology **3**(1): 61-75.

- Gao, H. S., X. D. Yu, et al. (2008). Availability Models for Protection Techniques of Transport Network Based on ASON Technology.

- Gold, J. I. and M. N. Shadlen (2007). "The neural basis of decision making."

- Hulme, G. V. (2001). "Security's best friend." InformationWeek July **16**: 2001.

- Hunt, S. (2001). "Market overview: Managed security services." Giga Information Group.
- Krzywinski, M. (2003). "Port knocking: Network authentication across closed ports." SysAdmin Magazine **12**(6): 12-17.
- McIvor, R., P. K. Humphreys, et al. (2009). "A study of performance measurement in the outsourcing decision."
- Menezes, A. J., P. C. Van Oorschot, et al. (1997). Handbook of applied cryptography, CRC.
- Rivest, R. (1992). "RFC1321: The MD5 message-digest algorithm." RFC Editor United States.
- Schneier, B. Applied Cryptography: protocols, algorithms and source code in C, 1996, John Wiley & Sons, Inc.
- Schneier, B. (2003). "Non-Security Considerations in Security Decisions." Workshop on Economics and Information Security.
- Shinder, T. W. (2003). Best damn firewall book period, Syngress Media Inc.
- Sommerville, I. (2007). Software Engineering. Eight Edition, Addison Wesley, Harlow, England.
- Stallings, W. (2003). Cryptography and network security, Prentice Hall New Jersey;.
- Stallings, W. (2007). Network security essentials: applications and standards, Prentice Hall.
- Standard, N. S. H. (1995). "Federal information processing standards publication 180-1." US Department of Commerce, National Institute of Standards and Technology **131**.
- Vincent, J. L. (2009). "Definition, Monitoring, and Management of Shock States." Intensive and Critical Care Medicine: 143-150.

- Webb, L. and J. Laborde (2005). "Crafting a successful outsourcing provider/client relationship." Business Process Management Journal **11**(5): 437-443.

Appendices

Appendix A1: Curriculum Vita

Full Name: Anas Ali Al-Kasasbeh

Date of Birth: 15/12/1981

Place of Birth: Al-Karak

Marital Status: Single

Nationality: Jordanian

Phone #: Home: 0096232365423 - Cell: 00962799253399

E-mail: anas_kasasbeh2002@yahoo.com

Ana4897@mutah.edu.jo

Mu'tah, Al-karak, Jordan, P.O. BOX (7).