"MULTI-LAYER SECURITY MECHANISM FOR ISPSC NETWORK"

MEADDEN TRIXI R. CARTA
LESTER IAN B. TAJORES
PAUL JOHN G. ALMAZAN
WELLA M. BAHINGAWAN
GENARO V. RABARA Jr.

A CAPSTONE PROJECT PROPOSAL PRESENTED TO THE FACULTY
OF THE ILOCOS SUR POLYTECHNIC STATE COLLEGE
INSTITUTE OF COMPUTING STUDIES
STA. MARIA CAMPUS

BACHELOR OF SCIENCE IN INFORMATION TECHNOLOGY

APRIL 2015

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

APPENDICES

Chapter I

INTRODUCTION

Project Context

The world is becoming more interconnected with the advent of the Internet and new networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. There are currently two fundamentally different networks, data networks and synchronous network comprised of switches. The internet is considered a data network. Since the current data network consists of computer-based routers, information can be obtained by special programs, such as "Trojan horses," planted in the routers. The synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers. That is why security is emphasized in data networks, such as the internet, and other networks that link to the internet.

System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented. There exists a "communication gap" between the developers of security technology and developers of networks. Network design is a well-developed process that

several advantages when designing networks. It offers modularity, flexibility, ease-of-use, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. The implementation of individual layers can be changed later without making other adjustments, allowing flexibility in development. In contrast to network design, secure network design is not a well- developed process. There isn't a methodology to manage the complexity of security requirements. Secure network design does not contain the same advantages as network design. When considering network security, it must be emphasized that the whole network is secure. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, and decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message.

An effective network security plan is developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack. The steps involved in understanding the composition of a secure network, internet or otherwise, is followed throughout this research endeavor. To lessen the vulnerability of the computer to the network there are many products available. These tools are encryption, authentication mechanisms, intrusion-detection, security management and firewalls. Businesses throughout the world are using a

combination of some of these tools. "Intranets" are both connected to the internet and reasonably protected from it. The internet architecture itself leads to vulnerabilities in the network. Understanding the security issues of the internet greatly assists in developing new security technologies and approaches for networks with internet access and internet security itself.

Networking enables employees within corporations to work with each together and with people in various locations and businesses elsewhere. It enables contact in entirely new ways and entirely new levels, across the office and right around the world. When the business is properly networked, no one is ever very far away.

The complexity of information networks has been growing very rapidly as virtually every employee is connected to corporate information networks and to the Internet. The extent of this, of course, depends on the type of business. Information networks carry a growing amount of data traffic and, as more services run through networks, the data is becoming more versatile and thus the demand for network management is growing. This has put a great amount of new requirements to enterprise IT departments, including data network administrators and managers. One popular approach has been to outsource network services, but the IT buyer still has to know the requirements and manage them to be fulfilled. These are key elements that have to be in order for outsourcing to be successful. Marcia Robinson states in her book Offshore Outsourcing that additional management needed for offshore outsourcing can dilute initial outsourcing savings by 20 30%. Regardless of the network services being outsourced or made in-house, they

have to be managed efficiently.

A study by Thomas Mende (2004) states that, on average, the information network causes 15% of all problems resulting in downtime at $1 billion-plus companies. However, only 2% are caused by actual networking hardware failures: The other 13% are due to different issues like human errors, unmanaged changes, misconfigurations, routing failures, and problems with networking software.

Few companies build their network infrastructure without a need for extension or replacement investments in the future. Although network equipment is nowadays usually fairly long-lived the network infrastructure might need replacement investment for other reasons for example, to improve functionality, data rates or response times. This also adds up the needs of effective Network Infrastructure Management, which means the process of building and maintaining the infrastructure of the network.

Information and Communication Technology (ICT), which is the merger of telecommunication and computing, is the major enabling factor. However, rich communication is unlimited to human interaction. Technology is increasingly used to automate many tasks. In addition, Stansberry (2009) stated that most data centers today are interested in automation which helps them automate menial processes.

But with the advancement of technology particularly on network, there are lying threats like data theft, eavesdropping, DoS attacks etc. Secured and proper network infrastructure is a must for enterprise networks. Securing your servers and workstations with end point protections are not enough.

Especially if your network is exposed to the internet. According to Curtin (1997), network security is a complicated subject, historically only tackled by well-trained and experienced experts. However as more and more people become "wired", an increasing number of people need to understand the basics of security in a networked world. Today, layer 3 network security, Unified Treat Management (UTM), Network Address Translation (NAT) etc must be observed for a proper and secure network.

Purpose and Description

Network Administrators. The output of this study would provide a better security to the Internet connection in ISPSC.

Students. This research helps the student to know the network security in ISPSC. It aims to secure the computer network in ISPSC

Researchers. This study would help the researchers to enhance their knowledge about the security.

Future Researchers. This study would help the future researchers to develop this study in the future. This study serve as their basis for future.

General Objective

To develop an efficient security in computer network of Ilocos Sur Polytechnic State College.

Specific Objectives

1. To identify the ICT Profile of Ilocos Sur Polytechnic State College;
2. To identify the network security issues along hardware software security and data archiving of Ilocos Sur Polytechnic State College;
3. To establish a network security firewall and evaluate the firewall such as: a.) ISPSC existing firewall b.) Untangle c.) Pfsense for Ilocos Sur Polytechnic State College;

Scope and Limitation

The scope of the study focused on the use of an open-source technology which could enforce or trigger network policy control on the application and network layer security in a simplified environment with the use of untangle gateway-firewall.

The security mechanism that was built shall not only be limited on the implementation action on Microsoft environment but may also work with other operating systems such as Linux, Android Mobile OS and Mac OS.

Chapter II

REVIEW OF LITERATURE

This section contains literature and studies, from foreign and local sources, reviewed by the researchers, which have been found relevant to this paper. The topics are discussed according to:

Multilayer Security Mechanism in Computer Networks

Rajeshwari (2011) mentioned that in multilayered security infrastructure, the layers are projected in a way that vulnerability of one layer could not compromise the other layers and thus the whole system is not vulnerable. The paper evaluates security mechanism on application, transport and network layers of ISO/OSI reference model and gives examples of today's most popular security protocols applied in each of mentioned layers. A secure computer network systems is recommended that consists of combined security mechanisms on three different ISO/OSI reference model layers: application layer security based on strong user authentication, digital signature, confidentiality protection, digital certificates and hardware tokens, transport layer security based on establishment of a cryptographic tunnel between network nodes and strong node authentication procedure and network IP layer security providing bulk security mechanisms on network level between network nodes. Strong authentication procedures used for user based on digital certificates and PKI systems are especially emphasized.

Firewalls

A study by Kenneth Ingham (2014) mentioned in his study that firewalls are network devices which enforce an organization's security policy. Since their development, various methods have been used to implement firewalls. These methods filter network traffic at one or more of the seven layers of the ISO network model, most commonly at the application, transport, and network, and data-link levels. In addition, researchers have developed some newer methods, such as protocol normalization and distributed firewalls, which have not yet been widely adopted. Firewalls involve more than the technology to implement them. Specifying a set of filtering rules, known as a policy, is typically complicated and error-prone. High-level languages have been developed to simplify the task of correctly defining a firewall's policy. Once a policy has been specified, the firewall needs to be tested to determine if it actually implements the policy correctly.

Little work exists in the area of firewall theory; however, this article summarizes what exists. Because some data must be able to pass in and out of a firewall, in order for the protected network to be useful, not all attacks can be stopped by firewalls. Some emerging technologies, such as Virtual Private Networks (VPN) and peer-to-peer networking pose new challenges for firewalls.

An article about firewall from www.tech-faq.com (2014) states that firewall is a software component that restricts unauthorized inward network

access. It allows outward information flow. It is set up to control traffic flow between two networks by configured permissions like Allow, Deny, Block, Encrypt, etc. It is normally employed to avoid illegal access to personal computers or corporate networks from external unsafe entities like the Internet. The firewall scrutinizes all the information flowing in and out of the network. If some data do not meet the necessary criterion, it is denied access into the network. A firewall's key function is to legalize the stream of traffic among computer networks of different trust levels. Similar to the physical firewalls installed in buildings that help limit the spread of fire, the software firewalls also help control network intrusions. A poorly configured firewall is useless. By default, the "deny" rule-set should be applied and allow only those applications to communicate for which the permissions have been explicitly set to "Allow." However, such configurations require expertise understanding. Due to the lack of such expertise understanding, many corporate networks keep "Allow" as their default rule-set.

Untangle Gateway-Firewall Security

Untangle delivers an integrated family of applications that simplify and consolidate the network and security products that businesses need at the network gateway. The Untangle Server and 12 of the applications that run on it are open source and free under the GNU General Public License v2 (GPLv2). Untangle's platform provides the GUI, logging, reporting and "virtual-pipelining" technology to make all of the apps run together smoothly.

Signatures updates and software upgrades, which install automatically, are also included.

ClearOS

ClearOS (formerly named ClarkConnect) is a Linux distribution, based on CentOS and Red Hat Enterprise Linux, designed for use in small and medium enterprises as a network gateway and network server with a web-based administration interface. It is designed to be an alternative to Windows Small Business Server. ClearOS succeeds ClarkConnect. The software is built by ClearFoundation, and support services can be purchased from ClearCenter. ClearOS 5.1 removes previous limitations to mail, DMZ, and MultiWAN functions.

Pfsense

pfSense is an open source firewall/router computer software distribution based on FreeBSD. It is installed on a computer to make a dedicated firewall/router for a network and is noted for its reliability and offering features often only found in expensive commercial firewalls. It can be configured and upgraded through a web-based interface, and requires no knowledge of the underlying FreeBSD system to manage. pfSense is commonly deployed as a perimeter firewall, router, wireless access point, DHCP server, DNSserver, and as a VPN endpoint.

BIBLIOGRAPHY

Books

C. Huitema, IPV6: The New Internet Protocol. Englewood Cliffs, NJ: Prentice-Hall, Nov. 1999.

W.Ford, M.S.Baum, Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption, Second Edition, Prentice Hall PTR, Upper Saddle River, NJ 07458, 2001.

M.Markovi_, "Cryptographic Techniques and Security Protocols in Modern TCP/IP Computer Networks," Short- Tutorial, in Proc. of ICEST 2002, Oct. 1-4, 2002.

B.Schneier, Applied Cryptography, Second Edition, Protocols, Algorithms and Source Code in C, John Wiley & Sons, Inc., New York, Chichester, Brisbane, Toronto, Singapore, 1996.

RSA Laboratories: PKCS standards. [6] T.Unkaševi, M.Markovi, G.Djorevi, "Optimization of RSA algorithm implementation on TI TMS320C54x signal processors," in Proc. of TELSIKS'2001, September.

G.Djorevi, T.Unkaševi, M.Markovi, "Optimization of modular reduction procedure in RSA algorithm implementation on assembler of TMS320C54x signal processors," DSP 2002, July, Santorini, Greece, 2002.

M.Markovi, T.Unkaševi, G.Djorevi, "RSA algorithm optimization on assembler of TI TMS320C54x signal processors," in Proc. of EUSIPCO 2002, Toulouse, France, Sept. 3-6, 2002.

M.Markovi, G.orevi, T.Unkaševi, "On Optimizing RSA Algorithm Implementation on Signal Processor Regarding Asymmetric Private Key Length," in Proc. Of WISP 2003, Budapest, Sept. 2003.

(RajeshwariGoudar and PournimaMore. Multilayer Security Mechanism in Computer Networks. IRACST – International Journalof Computer Networks and Wireless Communications (IJCNWC), Vol. 1, No. 1, December 2011)

(Kenneth Ingham Consulting and Stephanie Forrest. "A History and Survey of Network Firewalls". University of New Mexico)

Internet Resources

(Firewalls. http://www.tech-faq.com/firewall.html. Last accessed December 21, 2014)

(Untangle. http://en.wikipedia.org/wiki/Untangle. Last accessed December 22, 2014)

(Wireless Security. http://en.wikipedia.org/wiki/Wireless_security Last accessed December 22, 2014)

(http://www.valleytalk.org/wp-content/uploads/2013/01/ top-down-network-design-3rd-edition.pdf

http://www4.ncsu.edu/~kksivara/sfwr4c03/projects/4c03projects/RPanchal-Project.pdf

http://www08.abb.com/global/scot/scot296.nsf/veritydisplay/039b702fdf091a4ec12569e7005e1fae/$file/WBPEEUD210017A0_-_en_AltaVista_Firewall_Data_Sheet.pdf