DETECTING PLAINTEXT RECOVERY ATTACK IN SECURE SHELL (SSH)

ZAID MUJAIYID PUTRA BIN AHMAD BAIDOWI

UNIVERSITI TEKNOLOGI MALAYSIA

DETECTING PLAINTEXT RECOVERY ATTACK IN SECURE SHELL (SSH)

ZAID MUJAIYID PUTRA BIN AHMAD BAIDOWI

A thesis submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

APRIL 2010

To my beloved wife, mother, late father, brothers and sisters

ACKNOWLEDGEMENT

I am heartily thankful to my supervisor, Dr Shukor Abdul Razak, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the subject.

In preparing this thesis, I was in contact with many people, researchers, academicians, and practitioners. They have contributed towards my understanding and thoughts. In particular, I wish to express my sincere appreciation to the project coordinator, Dr Rabiah Ahmad for her guidance, advices and motivation. Without her continued support and interest, this thesis would not have been the same as presented here.

I extend my appreciation to my entire family members, especially my beloved wife, colleagues and others who have provided assistance and support. My fellow classmates should also be recognized for their support. My sincere appreciation also extends to all my colleagues and others who have provided assistance at various occasions. Their views and tips are useful indeed.

Lastly, I offer my regards and blessings to all of those who supported me in any respect during the completion of the project.

ABSTRACT

Plaintext Recovery Attack is a new attack in security system world. It was discovered lately in the year of 2008. It is known that Secure Shell (SSH) connection is secure enough but this new discovered attack proved that there is vulnerability exist in SSH. Therefore, people need to aware of the attack since it could harm computer systems and connection could be dropped. In this thesis, we proposed a new mechanism to detect the attack and alert the system user that the computer is being attacked. The methodology used is System Development Life Cycle (SDLC) by applying waterfall model. Study and analysis have been done to make sure that the all necessary information is gathered. A simple tool was developed and tested successfully to prove that the mechanism can be implemented. Input parameter is needed to simulate the attack since the attack is new. Block-by-block input parameter is sent through the SSH connection from source host to destination host. The destination host detects the attack by checking the end of block size. If the block is attacked, then the block size would be recognized as the first block. This tool helps computer users and administrators are aware of this kind of attack. The weaknesses of this new mechanism shows that it needs further research to tighten up the mechanism.

ABSTRAK

Plaintext Recovery Attack merupakan serangan terbaru dalam era sistem keselamatan. Ia telah dijumpai baru-baru ini dalam tahun 2008. Semua sedia maklum bahawa sambungan *Secure Shell* (SHH) adalah cukup selamat namun serangan terbaru yang dijumpai membuktikan bahawa wujudnya kelemahan di dalam SSH. Oleh sebab itu, semua pihak perlulah sentiasa berwaspada terhadap serangan tersebut kerana ia boleh membahayakan sistem komputer dan sambungan tersebut boleh terputus. Dalam tesis ini, kami mencadangkan satu mekanisma baru dalam mengesan serangan tersebut sekaligus memaklumkan kepada pengguna sistem bahawa komputer tersebut telah diserang. Metodologi yang digunakan ialah Kitaran Hayat Pembangunan Sistem (SDLC) dengan mengaplikasikan model *waterfall*. Kajian dan analisa telah dijalankan bagi memastikan bahawa semua maklumat berkaitan telah dikumpulkan. Sistem ringkas telah dibangunkan dan diuji dengan jayanya bagi membuktikan bahawa mekanisma baru tersebut boleh dilaksanakan. Kemasukan parameter digunakan bagi menggantikan serangan sebenar dan dihantar blok demi blok melalui sambungan SSH dari komputer sumber ke komputer destinasi. Komputer destinasi mengesan serangan tersebut dengan menyemak saiz blok terakhir. Jika blok tersebut diserang, maka saiz blok tersebut dikenali sebagai blok pertama. Sistem ringkas ini membantu pengguna-pengguna komputer dan pentadbir sistem supaya lebih berwaspada terhadap serangan tersebut. Kelemahan mekanisma baru ini menunjukkan bahawa kajian lanjut perlu dilaksanakan bagi memastikan mekanisma ini lebih selamat.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

ICT	-	Information Communication and Technology
SSH	-	Secure Shell
CTR	-	Counter Encryption
CBC	-	Cipher Block Chaining
IV	-	Initialization Vector
EIDS	-	Extended Intrusion Detection System
NIC	-	Network Card Interface
JDK	-	Java Development Kit
JPCAP	-	Java Packet Capture

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Introduction

This chapter discusses the background of the problem, problem statement, project objective and project scope. Finally, we summarize the chapter as a whole.

1.2 Background of the Problem

Nowadays, businesses are growing rapidly regardless of geographical restrictions. Many organizations use Information and Communication Technology (ICT) as a tool to double their income. Confidential data and information are kept in ICT equipments such as servers that can be accessible anytime and everywhere all over the world.

System administrators are the one who can access the equipments by using secure protocol such as Secure Shell (SSH). According to Amit, Ajay and Surbhi (2007), the main purpose of SSH is to securely transmit data over network connections by using strong encryption and authentication methods such as AES or triple DES. SSH was initially designed to replace the insecure remote login procedure such as rlogin and telnet. In other words, SSH is used as a secure communication channel by many organizations.

It is widely known that SSH protects from any types of attacks while communicating over the internet. It protects data during the process of transition against attacks like eavesdropping, DNS and IP spoofing, connection hijacking, man-in-the-middle attacks and insertion attacks before reaching the destination (Attachmate Corporation, 2008). SSH uses strong cryptography integrity checks such as SHA-1 and MD5. Hence, SSH is unlikely to be attacked. However, once an attacker is accessible to the root of a machine, SSH has no defense. Attacks such as password cracking, IP and TCP attacks, traffic analysis, and covert channels can undermine the network security.

There are various attacks against SSH have been discovered, for example, keystrokes and timing attacks (Dawn Xiaodong, 2001), password guessing (Seifert, 2006), brute-force attack (Owens & Matthews, 2008) and the latest is plaintext recovery attack (Martin, Kenneth & Gaven, 2009).

Keystrokes and timing attacks occur while we are connecting to SSH by typing or hitting our keyboards. The timing leaks between the two buttons enable an attacker to sniff and analyze the typing patterns. This leads to the disclosure of information on the keys typed. Meanwhile, brute-force attack and password guessing are found to be a common attack in SSH (SANS Institute, 2007). Plaintext Recovery Attack can recover bits in the packet transferred and cause SSH connection drop.

Suggestions and recommendations to protect these kinds of attacks have been identified. For brute-force and password guessing protection, it is advised to turn off the services that allow external host to come in, to move listening port from 22 to some other ports, to use strong password, using tools such as IPTABLES / SSHD / TCPWRAPPER / PORT KNOCKING to block the attacks and many other things have been suggested. As for plaintext recovery attack, as at this thesis written, there is only one straightforward suggestion to protect the attack: use Counter Encryption (CTR) instead of Cipher Block Chaining (CBC) encryption in the protocol design.

One the other hand, we have discovered that in order to detect attacks in encrypted environment is to detect intrusions based on transferred data size and timing without using decryption algorithm (Foroushani, Adibnia & Hojati, 2008). Currently, there are fewer studies addressing the attack detection within encrypted environment. This is supported by Kabila (2008) in his article in which he described that Network-based Intrusion Detection is unable to detect attacks within encrypted network traffic.

1.3 Problem Statement

In November 2008, researchers from University of Royal Holloway discovered a highly dangerous SSH flaw. According to the experts, this flaw could allow hackers access to sensitive data. As we know, SSH is widely used by system administrators for securely access remote system from apart over the internet communication. Therefore, SSH is no more secure than what we expect because it may harm the organization communication system.

This flaw has led to Plaintext Recovery Attack where it could cause the connection to be dropped down. It means that the connection needs to be re-established in some other time. Besides, this attack could exploit the encrypted length field and makes the field useless for the packet. The Message Authentication Code (MAC) would return error and reveal the amount of data expected in the packet including the length field. As a result, the encrypted information could be exposed to the attackers and it could help them to gain access to the network.

It is therefore, more research on Plaintext Recovery is needed in order to ensure SSH secure against this attack. At time of this report was written, less research was done in capturing this attack as it was newly found (Martin, Kenneth & Gaven, 2009). Although the possibility of this attack is small, it is found to be highly dangerous once it is attacked. This attack could also reveal critical and sensitive information of an organization to the attackers. By doing this research, we hope it will help to reduce the risk of this attack.

In a nutshell, this problem situation drives us to do research in this topic and at least to contribute knowledge and research in area of detecting attacks.

1.4 Project Objectives

In order to ensure this project is feasible to complete within the stipulated time, we have identified three objectives of this project. The objectives are:

i. To study existing mechanism to secure SSH.
ii. To develop new mechanism to detect Plaintext Recovery Attack.
iii. To evaluate the proposed mechanism.

1.5 Project Scope

In this project, it is considered that the attack has been launched. Therefore, the tool that we have developed requires a few parameters to be keyed in and assuming that the data has been revealed during the attack. This project focuses on:

i. Plaintext Recovery Attack exists in OpenSSH version 4.7.
ii. Virtual environment for the purpose of testing and development.

1.6 Rationale of Study

In November 2009, the new attack, Plaintext Recovery Attacks against SSH has been discovered by Information Security Group Royal Holloway, University of London.

A research including testing on virtual environment has been performed. The rationalities of the studies are as follows:

i. Several attacks against SSH have been identified but these attacks are new to the security area.
ii. Even though there are several papers have been done in this area, none of the works addressed such attacks.
iii. There is one pattern publication created in capturing attack in encrypted environment however the pattern is to capture by decrypting the encrypted packet. On the contrary, our research is not akin to such pattern.

1.7 Summary

We have discussed the background of the problem, the problem statement and the objectives of the project. On the other hand, we have narrowed down the scope to ensure it meets the objectives at the end of this project. Finally, we have justified the reason why we propose to do research in this area.

The next chapter, we discuss the relevant studies done by previous researchers in relation to this project.