Remote Scan Using Secure Automated Client Server Model

Venkateshwarlu Gogikaru and Mahendra Pratap Singh

Department of Computer Science and Engineering
National Institute of Technology Karnataka, Surathkal, India
{gvenkateshwarlu7,mahoo15}@gmail.com

Abstract. In recent years, attackers gain entry into computer systems frequently with the help of Rootkit's. Detection of these Rootkits is not a simple task in early days. To detect Rootkits we need to run many scanning tools manually. This is not feasible many times and it is time consuming process for each client. We propose a secure automated client/server model to scan remote clients present in local area network. This model allows us to run the scanning tools automatically and periodically, to know the Rootkits present in the client system. For our experiment purpose we automated *RootkitRevealer* tool.

Keywords: Client Server Model, Rootkits, Remote Scan.

1 Introduction

Attackers wish to attack the systems with the help of malwares like viruses, Trojans horses, spywares, rootkits and etc.. Among these rootkit is the one sophisticated method of attack. Important feature of the rootkit is hiding their presence in a system. This makes detection of these malware much difficult. Recently, a number of attacks have surfaced all related to the rootkits with more sophisticated technology. One among them is Stuxnet [1], which targeted on industrial systems.

The term rootkit has been around for more than 15 years. Rootkit is a program that provides the means to create an undetectable presence on a computer [2]. Rootkits are not inherently "bad," and they are not always used by the "bad guys." It is important to understand that a rootkit is just a technology. But now a day's many bad guys using this technology to gain access into computer systems in an organization to access the important information.

Most of the attackers wish to gain entry into computer systems frequently by injecting illicit functionality to maintain control, gather information, or neutralize the defenses of the target system, among other objectives. While past attacks often focused on modifications to userlevel libraries or system binaries, the operating system kernel is an increasingly popular target from many days. Attackers typically modify the kernel using these rootkits either to implement their illicit functionality directly or indirectly.

K.R. Venugopal and L.M. Patnaik (Eds.): ICIP 2011, CCIS 157, pp. 476–481, 2011.

To detect these rootkits many companies developed different rootkit detection tools (RDTs) [3]. But we have to run all these tools manually. When there is large number of systems in an Organization, this is not possible many times. To achieve this we need an automated scanning mechanism.

To achieve this we proposed and implemented secure automated client server model with the help of RootKitRevealer (RKR) tool. RKR is one of the very first advanced rootkit detection tool. RKR successfully detects many persistent rootkits including AFX, Vanquish and HackerDefender [4]. This tool is very pretty simple to use, no installation required, so we use this tool in our experiment. In this experiment secure communication is maintained with the help of SSL in client server communication.

The rest of the paper is structured as follows. In section 2, tells the motivation of work, In Section 3, we give overview of SSL/TLS between client and server. In Section 4, we present the proposed model. In Section 4, the detailed implementation issues are discussed, and Section 5 concludes.

2 Motivation

Now days many company people developing different products and tools to detect the malwares. But these tools are not supporting the needs of an organization. For a person (say administrator) to detect malwares in an organization which consists of many systems is not a simple task. To do so, administrator has to install different tools in every system manually and scan them which is not feasible many times. This motivated us to make an automated model, to perform scan, updating the software and other things, in all the systems present in an Organization from a single system.

3 Overview of SSL/TLS

This section describes the SSL/TLS handshake protocol [5],[6]. In the remainder of the paper, the term "SSL" is used to refer to both SSL and TLS standards. SSL is the most widely used protocol to ensure secure communication in a network. It is typically employed by web servers to protect electronic transactions. SSL uses the RSA cryptosystem during an initial client/server handshake to establish a shared symmetric key for use during an SSL session

3.1 SSL Handshake Protocol Description

The simplest version of the SSL handshake (key-establishment) protocol [5],[6] consists of two communication rounds that contain the following messages and computations:

1. Client sends a "client hello" message to server. This indicates that client wants to initialize a SSL/TLS session and the message includes the cipher suites client supports and a random nonce r_c.