Thomas J. Watson School of Engineering & Applied Science

Department of Electrical & Computer Engineering

Hardware-Based Security

(EECE658)

Intranet Security Management

(OS Type & Version Detection via Packet Analysis)

Submitted By

Alem Haddush Fitwi
afitwi1@binghamton.edu
Ph.D. Student

Submitted To

***Prof.** Yu Chen*
ychen@binghamton.edu

05 March 2018

Binghamton, New York

Summary

At present, the Internet has amazingly revolutionized the way we do and manage things. The revolution of the Internet can be traced back to the development of the Advanced Research Projects Agency Network (ARPANET) in the early 1970s by the Department of Defense of the USA along which the rapid development of the Internet, the TCP/IP protocol has become the most widely used network interconnection protocol; insufficient security concerns at the beginning of the design has left a lot of weakness, though. These vulnerabilities of the Internet Technologies are widely exploited by both internal and external users and attackers/hackers. Traditionally, border security devices like firewalls and software's like antivirus are deployed in enterprise networks; however, these security defense mechanisms have never been sufficient to protect the enterprise sensitive resources from attacks perpetrated from terminals of internal users. Hence, there has been a tremendously pressing quest for the design, development, and deployment of less-resource hungry, effective intranet or terminal security solutions that ensure secure, authentic, and authorized access to enterprise resources as per the business access rights of users defined in enterprises' security policies.

The prime goal of this project is to implement a part of an intranet security solution. It focuses on the implementation of an algorithm that will function in a way similar to network mapping to detect the type and version of operating systems running on terminal devices where the Raspberry Pi will be used to run the python script which will be responsible for the detection via packet analysis, port scanning, port filtering, and based on predefined peculiar attributes of operating systems. For the sake of simplicity the implementation test, all the terminals and the Raspberry will be placed in the same subnet.

Keywords: *Internet, ARPANET, TCP/IP, Intranet security, Raspberry PI, security policies*

Contents

1. Background Information

The Internet has alarmingly revolutionized the way we communicate, the way we do business, and the way we live. The start of the revolution of the Internet can be traced back to the development of the Advanced Research Projects Agency Network (**ARPANET**) in the early 1970s by the Department of Defense of the USA. The ARPANET was an early packet switching network and the first network to implement the protocol suite TCP/IP, which later both technologies became the technical foundations of the Internet. In other words, along with the rapid development of the Internet, the TCP/IP protocol has become the most widely used network interconnection protocol [1].

However, due to insufficient security concerns right at the beginning of the design, the protocol has a lot of security risks. It is to be recalled that the Internet was first applied in a research environment for a few trusted user groups. Therefore, network security problems were not the major concerns at that time which has left big security holes in the TCP/IP protocol stacks. The vast majority protocols do not provide the necessary security mechanisms [2]. Various studies show that many of the vulnerabilities of any network, be it Intranet, Extranet or Internet are compromised or affected by intentional or unintentional attacks directed from Terminals or terminal users where the edge security devices like firewalls and antivirus alone can't solve [3, 4, 5, 6, 7].

Malware accounts for a large percentage of all the security threats that have occurred, and gray ware is becoming more influential. Security threats relevant to crimes have become serious concerns that threat network security. Today, users are no longer threatened by traditional viruses rather by network threats that integrate viruses, hacker attacks, Trojan horses, botnets, and spyware. The network threats are difficult to defend using previous antivirus or anti-hacker technologies [6].

2. Problem statement

As indicated in many literatures, traditional enterprise border protection measures become meaningless unless coupled with a robust mechanism to counter the increasing internal security risks. That is, even though antivirus and security equipment like firewall are deployed on enterprise networks, the enterprise still faces such problem as Terminal anomalies, misuse

of resources and policy breaches at terminals, system damage, unstoppable information leaks, viruses, worms, and malwares that cause the enterprise network or device to respond slowly.

Hence, against this serious problem, Security Experts or researchers are expected to give huge due attention to efficient intranet and terminal security protection systems development and deployment. One way is to keep track of the status of operating systems installed in terminals or end user computers and enforce security authentication whenever the terminals attempt to access resources in the enterprise core zones.

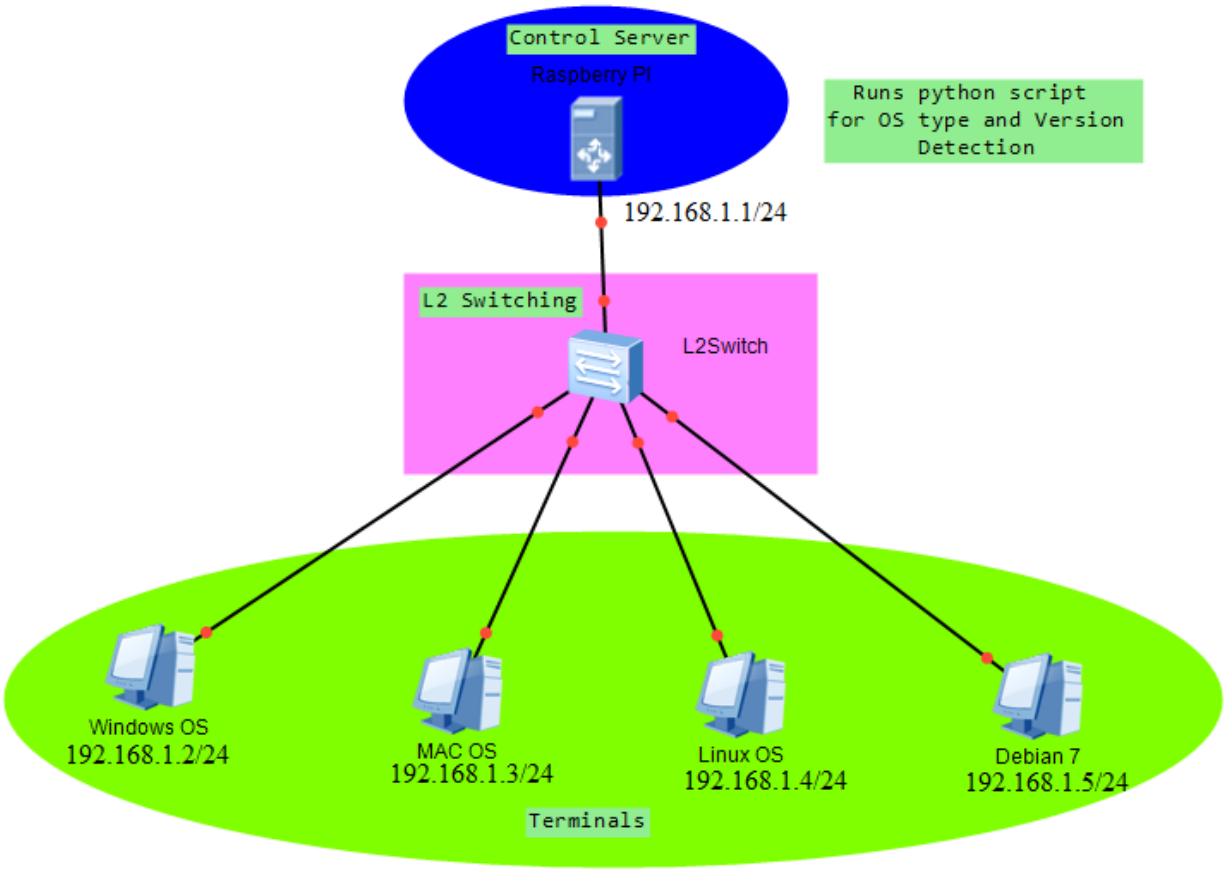

Figure 3.1: Detection OS installed on terminals

3. Objective

3.1 General Objective

The main objective of this project is to implement a part of the intranet security system. That is to say, the types and versions of operating systems installed in terminals will be detected

and identified by running python script on the Raspberry PI which will be assumed as an access control server as depicted in figure 3.1.

3.1 Specific Objectives

The detailed and specific objectives of this project proposal are tersely outlined as ensues:

- ⇒ Define peculiar attributes of different operating systems
- ⇒ Build a kind of mapping algorithm and implement it in python
- ⇒ Analyze packet tuples
- ⇒ Emulate open ports
- ⇒ Perform port filtering
- ⇒ Grab MAC addresses of target hosts portrayed in figure 3.1
- ⇒ Detect the OS type and version running on the target hosts, depicted in figure 3.1.

4. Time Frame

Table 4.1: Project Implementation Schedule

S/N	Activities	**Spring 2018**							
		March				**April**			
		W-1	W-2	W-3	W-4	W-5	W-6	W-7	W-8
1	Literature Survey								
2	Implementation								
3	Functional Tests								
4	Reporting								
5	Presentation								

5. References

[1] Abbate, Janet Ellen. "From ARPANET to Internet: A history of ARPA-sponsored computer networks, 1966--1988." (1994): 8-13

[2] Bellovin, Steven M. "A look back at" security problems in the TCP/IP protocol suite." *Computer Security Applications Conference, 2004. 20th Annual*. IEEE, 2004: 1-2

[3] Richardson, Robert. "2011 CSI computer crime and security survey," 2011." (2010): 19-21

[4] Singh, Utkarsh, Sumit Jaiswal, and R. S. Singh. "Cloud banking." *CSI Transactions on ICT* (2016): 1-6.

[5] CeRT, MAJOR AUSTRALIAN BUSINESS. "2015 CYBER SECURITY SURVEY." (2015): 19-23

[6] White, G. K. *Simple Institutional and User Best Practices for Cybersecurity in Research Reactors*. No. LLNL-CONF-679241. Lawrence Livermore National Laboratory (LLNL), Livermore, CA, 2015: 3-7

[7] Ivanovs, Ivo, and Sintija Deruma. "Revising Cybersecurity Skills for Enterprises."