EMBEDDED INTRUSION PREVENTION SYSTEM(eIPS) ON LINUX-BASED SINGLE BOARD COMPUTER IN E-COMMERCE SECURITY

Suhizaz Sudin
Zahereel Abdul Khatib, Salina Asi, R.Badlishah Ahmad,
Ahmad Nasir Che Rosli
School of Computer and Communication Engineering
Kolej Universiti Kejuruteraan Utara Malaysia
01000 Kangar, Perlis, Malaysia
suhizaz/zahereel/salina/badli/ahmadnasir@kukum.edu.my

ABSTRACT

Intrusion Prevention Systems(IPS) is a new type of security element that pervades the network and automatically protects organizations from a broad variety of attack types and from all potential points of attack inside out. This embedded system plays an important role in recent technology development. This IPS application will be develop and embed on the linux-based single board computer (SBC).SBC can handle several functions depend to their features even they has limitation in term of memory, capacity, control system and security. This paper will explain the concept of Embedded Intrusion Prevention System(eIPS) on a Linux-based Single Board Computer. The eIPS also is giving an idea described how network management software and extensible hardware can work together in order to protect the e-commerce applications.

KEYWORDS
Intrusion Prevention Systems, embedded system

1. INTRODUCTION

The tremendous increase in cyber attacks linked with the dependence of modern organization on the reliability and functionality of their IT structure has led to a change in mindset. As “IT downtime” is rising, the priorities are shifting. As recent surveys show, cyber attacks – especially targeted to the networks – are real, and no longer an unlikely incident that only occur to few exposed networks of organizations in the limelight.

In the struggle to both maintain and implement any given IT security policy, professional IT security management is no longer able to ignore these issues, as attacks on networks become not only more frequent but also more devastating; in many organizations commercial success is directly related to the safe and reliable operation of their networks.

The term Intrusion Prevention Systems (IPS) is relatively new, often pushed by the marketing departments to move the Intrusion Detection Systems (IDS) manufactures away from the negative image of IDS. They are essentially a combination of access control (firewall/router) and IDS, this alliance coming naturally as both technologies often use shared technologies.

Nearly all modern commercial firewalls use “stateful” inspection and commercial IDS use signature recognition. Both technologies need to “look deep into the packet” before making an access decision in the case of a firewall or raise an alarm in the case of an IDS. To make this possible in an efficient manner, sufficient processing power is necessary, which has become more easily available in recent years. An IPS works like an in-line network IDS allowing for instant access control policy modifications.

With the arrival of DDoS attacks such as the recent “W32.Blaster.Worm” the market trend is clearly focussing on IPS rather than IDS. Predominantly an IPS is not only found on security appliances, such as

certain firewalls, but also on stand alone appliances delivered. The idea to implement IPS here is driven by commercial as well as technical aspects. To-date IPS has had the most success with "flood" (i.e. DoS) type attacks.

With the progress of technical sophistication in the hacker methods, especially modern DoS or DDoS attacks, attack signatures are not easily detected. Generically one may assume that an attack signature is derived from a stream of packets with a malicious content in both the packet header and the packet payload.

2. INTRUSION PREVENTION SYSTEM(IPS)

2.1 Definition of IPS

An IPS can be defined as an in-line product that focuses on identifying and blocking malicious network activity in real time. In general, there are two categories:

- rate-based products; and
- content-based (also referred to as signature- and anomaly-based).

The devices often look like firewalls and often have some basic firewall functionality. But firewalls block all traffic except that for which they have a reason to pass, whereas IPS pass all traffic except that for which they have a reason to block.

2.2 Rate-based IPS

Rate-based Intrusion Prevention Systems block traffic based on network load, for example, too many packets, or too many connects, or too many errors. In the presence of too much of anything, a rate-based IPS kicks in and blocks, throttles or otherwise mediates the traffic. Most useful rate-based IPS include a combination of powerful configuration options with range of response technologies. For example, limit queries to the Domain Name Server (DNS) server to 1000 per second and/or offer other simple rules covering bandwidth and connection limiting.

A rate-based Intrusion Prevention System can set a threshold of maximum amount of traffic to be directed at a given port or service. If the threshold is exceeded, the IPS will block all further traffic of the source IP only, still allowing other users (source Internet Protocol (IP)s) to use that service.

2.2.1 Disadvantages of rate-based IPS

The biggest problem with deploying rate-based IPS products is deciding what constitutes an overload. For any rate-based IPS to work properly, the network owner needs to know not only what "normal" traffic levels are (on a host-by-host and port-by-port basis) but also other network details, such as how many connections their web servers can handle. However, most commercial products do not yet provide any help in establishing this base-line behaviour, but require the services of a "trained" product specific systems engineer who often spend hours on site setting-up the IPS. Because rate-based IPS require frequent tuning and adjustment, they will be most useful in very high-volume Web, application and mail server environments.

2.3 Content-based products

Content-base Intrusion Prevention Systems block traffic based on attack signatures and protocol anomalies; they are the natural evolution of the Intrusion Detection Systems and firewalls. They block the following:

- Worms – (e.g. Blaster and MyDoom) that match a signature can be blocked.
- Packets that do not comply with TCP/IP RFCs can be dropped.
- Suspicious behaviour such as port scanning triggers the IPS to block future traffic from a single host.

The best content-based IPS offer a range of techniques for identifying malicious content and many options for how to handle the attacks, such as simply dropping bad packets to dropping future packets from the same attacker, and advanced reporting and alerting strategies.

As content-based IPS offer IDS-like technology for identifying threats and blocking them, they can be used deep inside the network to complement firewalls and provide security policy enforcement as they often require less manual maintenance and fine-tuning to perform a useful function than their rate-based cousin.

3. EMBEDDED SYSTEM

An embedded system has become a tremendous technology development in recent decade. It application is needed and become more dependent in our environment such as in communication and network, signal processing, control systems, consumer electronics and biomedical systems. The examples of embedded systems application are air conditioner, microwave oven, LCD projector, digital camera, DVD player, play station, MP3 player, PDA and web-enabled TV sets.

Primarily an embedded system is a combination of hardware and software. Different with general computer that is multitasking, the main characteristic to define embedded systems is it performs a specific task. An embedded system are very powerful and complicated, low power consumption, limited memory capacity and use a very small operating systems. Single Board Computer (SBC) is one kind of embedded system technology widely used. SBC can performs specific tasks like computer as it has a processor, RAM, hard disk and OS or languages.

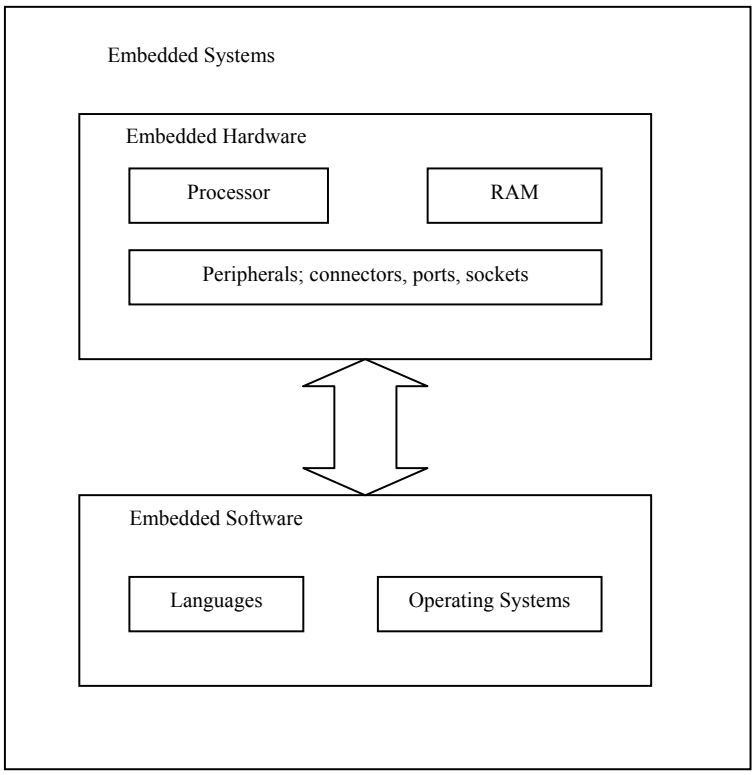

Figure 1 : An embedded system structure

3.1 Embedded Hardware - TS5400 Model Single Board Computer

The TS5400 PC/104 single board computer is a Technologic Systems (TS) product with 133 MHz AMD 586 processor. It is included with 16-64 MB SDRAM, Dual 10/100 Ethernet, 2 USB ports, PCMCIA socket, compact flash socket, 3 COM ports, 38 DIO, PC/104 expansion bus, 2 MB flash drive and optional A/D converter. Appendix outlines the TS5400 model hardware features and specifications [7].

The compatibility of an embedded system referred to the element of the processor, memory, I/O maps and BIOS. Memory for this model is depends to the capacity of compact flash used in the range from 32 MB – 1GB. SBC model from Technologic Systems is boot from IDE compact flash, DiskOnChip or On-

board flash drive. TS5400 are compatible with several embedded OS with x86-based operating system. They are TS-Linux, DOS, Windows CE, Net BSD, MicroCommander, SMX, QNX, Phar Lap, MicroC/OS II and eRTOS. The most popular OS that used with this x86 models are DOS and TS-Linux.

This model has three COM ports and COM 2 is used to be a monitor for SBC using null modem. A serial port is conneceted from board at COM 2 to serial port at computer localhost. To enable the console at localhost functions well, a minicom should installed fisrt. Linux has provides package that contain minicom. A default baud rate should be change from 9600 to 115200. At the same time, the correct serial port that has been connected from localhost must be set at minicom configuration.

In this research, the operating systems used is TS-Linux 3.07a that has been pre-installed by TS company before shipping. TS-Linux is one type of embedded OS that is created by TS and has many similarity like normal Linux features especially in filesystem but in small size. It support apache web server with PHP, and also support telent and file transfer protocol (FTP) between server and client. In addition to that, the basic utilities are BASH, ASH, minicom, vi, busybox and tinylogin.

Network support is one of the important feature for latest single board computer technology. TS5400 has one RJ45 port and support standard network as stated earlier. It support Secure Shell (SSH) function but can only issuing by remote host to access the board. Furthermore, the Secure CoPy (SCP) is allowed by this model by activating the dropbear function provide by TS-Linux. In other hand, PCMCIA is also reliable which using 802.11 standard for wireless network.

Figure 2 : The TS5400 Model

4. EMBEDDED INTRUSION PREVENTION PREVENTION SYSTEM(eIPS)

eIPS will be developed and installed on the TS5400 model Single Board Computer(SBC). eIPS is a structured program written in C in Linux Platform. TS-Linux is used as operating system and it has been installed with kernel version 2.4.23 and using minicom medium as TS5400 terminal. TS provides three kernel versions which are kernel 2.4.18, 2.4.22 and 2.4.23. Of course there are limitations within those kernel because they are a small and simple kernels. It including important and familiar packages and drivers.

TS5400 has default network setting including IP, Netmask, Broadcast, Network and Gateway. By using Ethernet cable, the TS5400 support network after configure it to available LAN at */etc/sysconfig/ifcfg-eth0* and */etc/sysconfig/network_cfg*. As stated earlier, this model support SCP function but this method only available by issuing command from localhost. This function allow to upload file(s) from localhost (computer) to remote host (SBC) and download file(s) from remote host to localhost.

To enable the board as a server, simple edit the /etc/proftpd.conf. The default setting only allow anonymous user to ftp to it. Telnet function can be actived by removing the comment mark '#' at telnet line at /etc/inetd.conf. In other hand, TS-Linux hasn't provided gcc function. It mean that TS500 cannot compile file except just execute the executed file that has been transferred to it. It also cannot use make command or in other word it cannot install any programs or softwares. So the development will be done in a desktop then transferred the executable file to TS5400.

5. eIPS AND E-COMMERCE SECURITY

Any business that is still in business, conducts "commerce". Commerce is the exchange of money for goods or services between companies (B2B) or end consumers (B2C). "E-commerce" is doing commerce using electronic technology such as intranets, extranets and the Internet, which provides with a new means of obtaining useful information and purchasing products and services between companies and end consumers. Although this form of e-commerce has undergone rapid growth, particularly through the use of the Internet, business and consumer fears and concerns about the risks, both have inhibited its growth real and perceived, of doing business electronically (Kamthan, 1999).

From the time a business installs a web server or hires space on a commercial web server from an ISP, there is a potential for business systems in the organisation to be exposed to breaches of security and confidentiality across the entire Internet (Lawrence and Corbett, 2000).

Any link to the Internet exposes the business to tampering, or Internet graffiti, where data can be exposed with meaningless scribble, pictures or electronic junk in the same way that graffiti artist scrawls on walls. Link to the Internet also exposes the business to the theft of data. Database can be very easily captured wholly and transferred for other uses such as industrial espionage (Sielgel, 1996). The TCP/IP protocol developed to run the Internet was not designed with security in mind. This protocol, the basic system running Internet communications, is vulnerable to interceptions (Hunt, 1998). Any movement of data from a browser to a server or back is vulnerable to eavesdropping (Chaffy, 2000). Website security is about keeping strangers out, but at the same time allowing controlled access to the network (Lawrence and Corbett, 2000).

eIPS offers a range of security measures for e-commerce applications. Data transmission is controlled based on parameters configured in the eIPS script resulting the effectiveness of e-commerce.

6. CONCLUSION

The spread of worms and viruses throughout the Internet has had a devastating impact on end users who suffer when their computers become infected with malware and on system administrators who deal with the burden of protecting entire networks of hosts. Active and extensible networks can be used to implement a distributed intrusion prevention system that decreases the rate at which worms and viruses spread. By stopping or slowing a worm outbreak, data can be saved and machines can be patched before they would otherwise become infected. Passive systems for intrusion detection have been used in the past to alert when a machine is compromised or a network is under attack. Active systems can be used to stop an attack and prevent a worm from spreading. By using extensible hardware, this type of protection can be provided with minimal impact on overall network performance.

Embedded intrusion prevention systems can be used to protect large numbers of system globally and e-commerce application specifically. eIPS give an idea described how network management software and extensible hardware can work together in order to protect high speed networks from fast outbreaks of new Internet worms and viruses.

REFERENCES

Rafeeq Ur Rehman and Christopher Paul, 2003. *The Linux Development Platform*. Prentice Hall PTR.

Lawrence Wiencke,2006. *TS5400 Single Board Computer with Linux and lots of serial ports.* http://www.physics.utah.edu/~wiencke/pc104html/5500.html

K. V. K. K. Prasad et. all , 2002. *Programming for Embedded Systems: Cracking the Code*. Wiley Publishing Inc.

Stephen A. Edwards ,2003. *Design Languages for Embedded Systems*. Computer Science Technical Report CUCS-009-03.

http://www.embeddedarm.com

Raj Kamal, 2004. *Embedded Systems: Architecture, Programming and Design*. McGraw Hill.

V. Ahuja ,1997. *E-commerce on Internet*, Academic Press Ltd, London.

Craig Hunt , 1998. *TCP/IP for Unix administrators (2nd ed.)*, O'Reilly (1998) ISBN 1-56592-322-7.

Elaine Lawrence and Briam Corbett ,2000. *E-commerce and Internet digital models for business (2nd ed.)*, John Wiley & Sons, Australia.

C. Sielgel ,1996. *Internet security for business*, John Wiley & Sons, Inc, New York.

Pankaj Kamthan,1999. *A matter of trust*, Journal of E-Commerce on the WWW.

D. Chaffy, 2000. *Business information systems; technology, development and management in the e-business*.