Towards the Design of Hardware Based Security Device and Communication Implementation

Dennis Arturo Ludeña Romaña[1] Kazuya Takemori[1] Shinichiro Kubota[2] Kenichi Sugitani[2] Yasuo Musashi[2]

Graduate School of Science and Technology
Kumamoto University
2-39-1 Kurokami, Kumamoto 860-8555, Japan
dennis, takemori@st.cs.kumamoto-u.ac.jp

Center for Multimedia and Information Technologies
Kumamoto University
2-39-1 Kurokami, Kumamoto 860-8555, Japan
s-kubota, sugitani, musashi@cc.kumamoto-u.ac.jp

Abstract— **Currently, the network security appliance is one of the most important research topics in IT security. The use of log files for further security analysis was proven their importance in the development of a three DNS query traffic based detection model system for a proactive detection of security threat in the university campus network. In the current detection strategy we can detect some suspicious infected candidates that need further analysis to prove their infection level. In order to perform this detailed analysis we need to collect the traffic from the suspicious candidate. We decide to use a hardware based system which is going to collect the traffic directly from the suspicious candidate. The traffic collected will be useful as a proof of the infection of the system. This information will provide us the possibility to create a personalized and portable device, which can be located in any network to analyze the same traffic without decreasing the network efficiency.**

Keywords: Computer network security, security hardware device, computer threats, threat detection.

I. INTRODUCTION

During the past few years, Information Security became an important concern from home users to corporate users. All of them wants to ensure that the information they provide in different online transactions are safe. Security gives the system the confidence to be safe about the transaction online. There are a lot of different threats that we might possibly face everyday in the Internet or in the institutional intranets if necessary steps are not taken into account by users. As a general policy, we will defend our private information from a wider point of view.

Nowadays, IDS (Intrusion Detection System) updates are based on "signatures". These "signatures" contain the complete definition and behavior characteristics of a threat. Based on this "signature", the IDS system can detect the attack of a threat and its payload. Unfortunately, these signatures are released for update after the attack has been widely executed and hundreds of users were already infected. The payloads could be from a DDoS attack to information leaking or network hijacking.

If we can provide a better network management and ensure a high security level in our institutions, the network will have better performance. In other words, we will increase the integrity, reliability, availability, efficiency, and better management [1, 2].

II. BACKGROUND WORK

For the past several years, the DNS query packet-based analysis is being performed in order to detect the early stages of worm attacks, from statistical analysis until the last three-model method in [3]. The program BIND 9.2.6 has been used as a server daemon. Using the query logging option, the DNS query packet and their query information has been captured [3].

Using this statistical detection method, we were successful in detecting several threat attacks (mostly worms), and other related network behavior issues. In our last paper publication, several successful detection results can be observed and analyzed in detail [3].

The results of these detections gave us the possibility to identify different suspicious infected PCs. Unfortunately, a further analysis of these systems present some difficulties because of:

- The remote location of the suspicious infected PC. In some cases the system is located in another building, where the security team is unable to get inside to perform more detailed analysis of the system.
- The temporal behavior of the worm. Because worms or other malware has a temporal based traffic generation (related to the spread procedure or infection activity).
- The temporal behavior of the worm, but in this case based on the fact that in some cases the worm is located in storage devices, like USB memory devices, or external hard disk drive. When such devices are connected to the suspicious infected PC, it begins to generate traffic that makes the system to be considered as infected.

III. MICROCONTROLLER-BASED SECURITY SYSTEM

In this study, we decided to integrate all our related background studies into a new hardware-based device. The following are some of the reasons behind the development of the hardware-based security device:

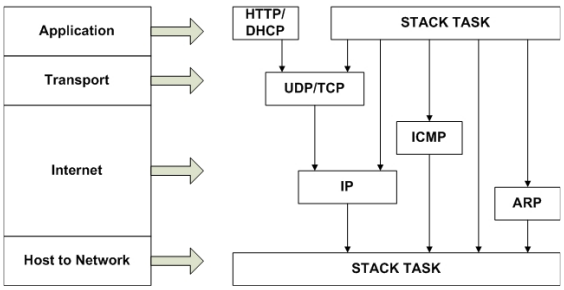

Figure 1. Comparison between the TCP/IP Stack Reference Model and the Microchip's TCP stack

- The device generates no additional traffic to the network.
- The device can be remotely controlled because it has server functions.
- Remote configuration or modification is available.
- The device can send the collected data to a log collecting server.

We decided to use the development board Microchip PICDEM.net2 based on the microcontroller Microchip PIC18F97J60, some of the characteristics of this board are:

- RJ-45 Modular Connectors. Two installed devices plus an option to add another Ethernet controller.
- LCD Display
- User defined LED and push buttons
- RJ-11 Modula Connector
- Serial Port

The major advantages of the system are:

- Compared to the software-based device, like small Linux boxes, they have no overhead.
- The system performs in a faster cyclic process, because of the dedicated characteristics of the hardware.
- Packet capturing capability is high.
- Compared to FPGAs, the PIC Microchip can be remotely updated, using the different services installed on it, like FTP.

Although they were another hardware-based detection system, we believe this is the first one in their class that the implementation will not put any additional load to the network and the system itself is resilient to any know attack which can stop their normal performance [4].

IV. DESIGN FRAME

The communications between the microcontroller and the network must be based on the standard OSI L7 protocol which is the common protocol use in the Ethernet-based communications.

Some of the TCP/IP layers are always active in the sense that they are always working, not only when they are required to, but when another event not related to their function occurs. Standard systems in the user- and server-side are capable to handle this. Also, the multitasking characteristics of the system allow the modularity of these processes. But since we are talking of a device like a microcontroller, we must put into consideration how much memory and resources can be used at a time. Special attention must be focused in the main application independency. A comparison between the TCP/IP OSI L7 and the Microchip's TCP stack is shown in Figure 1.

Also, in the moment of the implementation of a new module under the main program, we must design the code to accomplish "cooperative multitasking." This property indicates to the division of a long application into smaller machine states, returning control to the main application whenever the logic must wait for a certain event [5].

The location of the system will be in the same network segment including the suspicious infected PC; the connection will be done using a network device tap. This device gives us the possibility to check individually the *Inbound* and *Outbound* traffic. Figure 2 shows the location of the system.

Using this configuration, the system can analyze the same traffic generated/received by the PC terminal. The data collection resultant can be based on the traffic generated by the following specific protocols:

- SMTP
- POP
- SSL
- DNS
- HTTP
- HTTPS

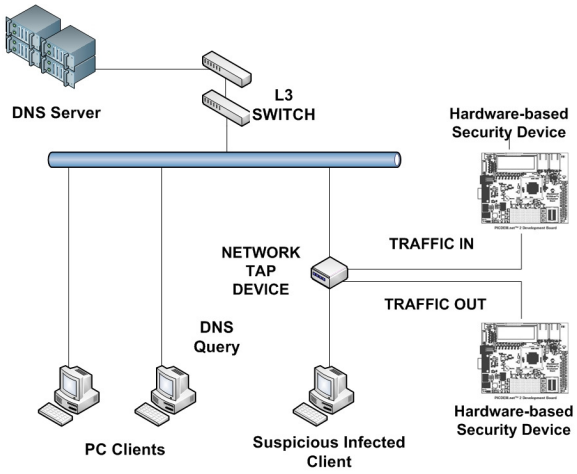

Figure 2. Location of the system

The detection strategy of the system is based on a filter design. The filter will be based on the three models based detection strategy presented previously by Musashi et al [1, 6 – 8].

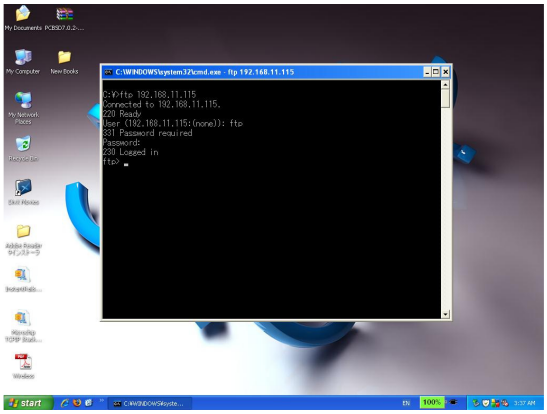

Figure 3. FTP Service working on the Client Side

This configuration allows us to have several data to design the filters that can be installed into the IDS.

The characteristics of the above mentioned filter will vary from the analysis that is going to be daily performed. After this analysis the new characteristics should be update to the system. The update process of the system must not interfere with the performance of the system.

V. Implementation Of FTP Server

Initially, we must define a communication system between the user and the Hardware-based Security System. Although in the device, the DHCP and HTTP server are already installed, we must implement an additional FTP server into the device shown in Figures 3 and 4.

Additional application to the main source code will be added using the FTP server. Also, in the near future filter rules will be upgraded using the FTP server.

In the case, the code must be compiled before using the pre-defined Microchip tool MPFS (Microchip File System).

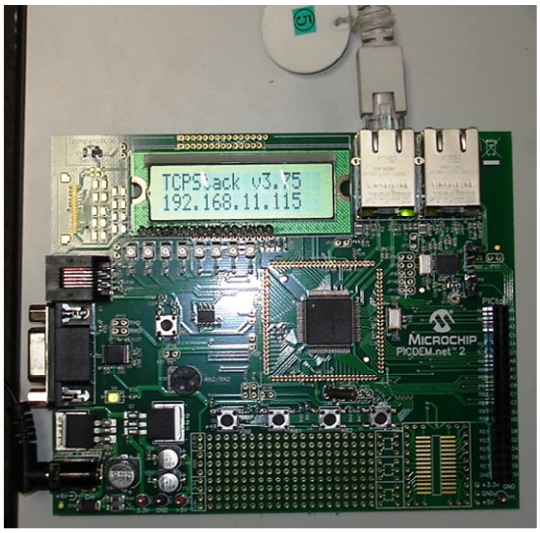

Figure 4. System working with a DHCP service

VI. Conclusions And Future Work

We decided to implement our DNS query packet based threat detection system inside a microcontroller device, in order to make a Hardware-based Threat Detection System. The development board selected for this purposes was the PICDem.net 2 from Microchip based on the microcontroller Microchip PIC18F97J60. We selected this microcontroller because its proven capabilities as an industrial class system. We established the necessary parameters for the development of the strategy. The fundamentals of the strategy to be implemented in the microcontroller will be based on the successful experiences in the early threat detection using DNS query packets. We successfully implemented the FTP server inside the microcontroller as an additional module to the main application. The FTP service will provide us an essential communication tool between the device and the client. The different up to date files will be sent using this service. The filtering results will be sent using the HTTP server pre-installed in the TCP/IP stack.

We continue further study in the development of the necessary additional applications for the filter implementation using the "Cooperative multitasking" in order to minimize the load for the processor and make the system more robust to handle all the necessary additional processes.

References

[1] Aissi S., Dabbus N. and Passad A. R., Security for mobile networks and platforms, Artech House, Norwood MA, USA, 2006.

[2] Harrington A. L., Network Security: A Practical Approach, Elsevier, San Francisco CA, USA, 2005.

[3] K. Takemori, W. J. Kong, D. A. Ludeña Romaña, S. Kubota, K. Sugitani and Y. Musashi, "Entropy Study on A Resource Record Query Traffic from the Campus Network", IPSJ SIG Technical Reports, Internet Operation and Technology 4th (IOT04), Vol. 2009, No. 21, pp.101-106.

[4] K. Bartoš, M. Grill1, V. Krmícek, M. Rehák and P. Celeda, "Flow Based Network Intrusion Detection System using Hardware-Accelerated NetFlow Probes", CESNET Conference 2008, Prague, Czech Republic, Proceedings, pp. 49–56.

[5] J. Axelson, Embedded Ethernet and Internet Complete, Lakeview Research LLC, Madison WI, USA, 2003.

[6] D. A. Ludeña Romaña, S. Kubota, K. Sugitani, and Y. Musashi. "Entropy Study on A and PTR Resource Records-Based DNS Query Traffic", IPSJ Symposium Series (IOTS2008), Vol. 2008, No. 13, pp.55-61.

[7] D. A. Ludeña Romaña, Y. Musashi, H. Nagatomi, and K. Sugitani, "Statistical Study of Unusual DNS Query Traffic", ECTI Transactions on Computer and Information Technology (ECTI-CIT) Special Issue in Information Technology, Vol. 6, No. 2, 2008, pp.106-109.

[8] D. A. Ludeña Romaña, S. Kubota, K. Sugitani and Y. Musashi, "DNS Based Spam Bots Detection in a University", Proceedings for the First International Conference on Intelligent Networks and Intelligent Systems (ICINIS 2008), Wuhan, China, 2008, pp. 205-208.