Visual Anomaly Detection of Network Connections in a Personal Computer

Hayate Goto*
The Univ. of Electro-Communications

Tetsuji Takada†
The Univ. of Electro-Communications

ABSTRACT

In this paper, we propose a visual anomaly detection system using network connections to/from a personal computer. End users have been exposed to security threats and they are still vulnerable to unknown attacks because current tools such as anti-virus software and firewall can only handle known threats. The system aims to become a supplementary security tool for the end users by visualizing network connections in the end user's computer. Our proposed system splits the data by time span and visualizes each block of data into one visual image. The system also provides the visual images as a temporal sequence. These ideas help users to capture a trend in normal situations and detect anomalous activities in network connections.

Index Terms: H.5.2 [Information Interfaces and Presentation]: User Interfaces—Screen design K.6.5 [Management of Computing and Information Systems]: Security and Protection—Unauthorized access

1 INTRODUCTION

Security threats such as malware are still one of the major issues within the field of ICT and end users are continually suffering from issues related to these threats. On the other hand, countermeasures against such threats have not changed compared to those from the past. Easily available major countermeasures for end users are Anti-Virus(AV) and Firewall software. These measures are able to protect the end user's computer from limited threats. The reason is that these two schemes only have protective functionality against already known threats. This means that they can not protect computers from unknown threats. In Japan, there have been cases where men are mistakenly arrested on charges of submitting illegal content to Internet bulletin boards in 2012. Further forensic investigations revealed the truth of the incident. It was that his computer was infected with malware and the computer was controlled remotely by a third person. Though the confiscated computer was scanned with AV software, since the malware was not widely known at that time, it was not detected during the initial investigation.

We consider that end users need to have an alternative countermeasure that can handle unknown security threats. In an intrusion detection system(IDS), there are two detection schemes: One is misuse detection that can correctly detect already known threats. The other is anomaly detection that can detect unknown threats. However, since installation and configuration of IDSs need technical skill and domain knowledge, IDSs are not suitable for end users. So, we try to realize a visualization system that helps end users to recognize an anomalous situation of network connections in a personal computer. The reason why we focus on network connections is that malware and other security threats generally make use of network communication. The network connection data in a personal computer is a good source of information for detecting undesirable activities. Our goal is to realize a system that assists such detection by using visual patterns.

There are already some visualization systems that have similar purposes. Snortview[1] is a visualization system of the logs generated from a network-based IDS. DAEDALUS[2] is a visual alert system that detects attacks to unused IP addresses. The target user of these systems is an expert user or an administrator of a network. Sesame[3] is a novel security user interface for non-expert users. This system provides users visuals for security-related system information. However we argue that the system still requires the users to have some domain knowledge because the visual representations are based on an actual computer model.

We have two ideas to achieve above purpose: 1) A system visualizes a block of data to one visual representation. 2) A system provides users a temporal sequence of the data visually. We assert that, through visual representation, if end users can recognize a normal situation of network connections, they can easily recognize anomalous situations. We therefore implement a prototype system based on the above ideas. The system has the potential to build trend models of normal activity of a user computer visually and detect anomalous situations.

2 NETWORK CONNECTIONS AS A VISUAL PATTERN FOR DETECTING SECURITY THREATS

Our prototype system has two modules: a network sensor module and a visualization module. Both modules are running in a target computer. We use the free software "Packet Police for Windows"[4] as a network sensor module. This software captures all network connection on a running computer and records them into the log file. This log file will be the data source for the visualization module.

Figure 1 is a screen snapshot of the visualization module. We implemented it in Java using a framework called Processing. This screen has three visual panes that gives visual representations about the network connections from a brief overview to a detailed view. The left half pane is a time slots view. This pane gives an overview of the network connections in a personal computer within a specific time period. As you can see in Figure 1, there are 20 similar visual blocks in the pane. Each pane represents the network connection status for period of three minutes. It means that the left pane visualizes the network connection data for one hour (3 mins. $\times$ 20 blocks). When starting up the system, the user can look at the data for the past one hour. The user can then travel to past data by using the user interface. The center pane is a connection status view. This view provides an enlarged representation of one of the visual blocks in the time slots view. A user can select a specific visual block from the time slots view and investigate in more detail using an enlarged representation. The rightmost pane is a text view that gives users detailed textual information. When a user investigates the data through the connection status view, she/he is able to access detailed information of selected lines. In such case, the user can select a plotted point on the axes using a mouse in order to view the information in this pane.

Here we will explain how we visualize the network connections. The network sensor module records a network connection as a tu-

*e-mail: hayate.goto@uec.ac.jp
†e-mail: zetaka @ computer.org

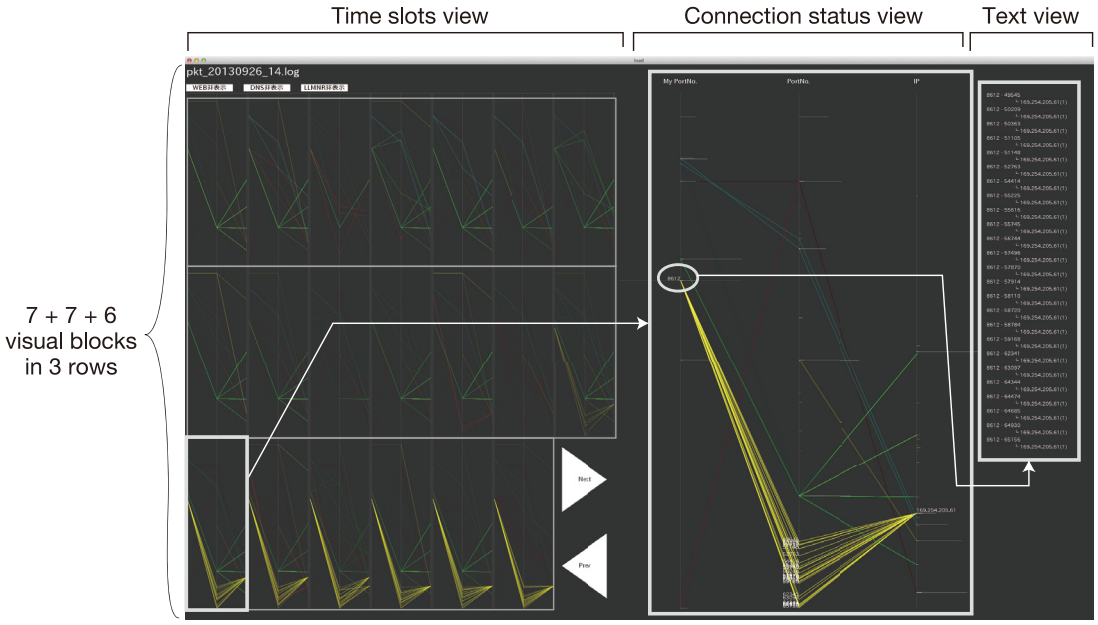

Figure 1: Screen Snapshot of the Prototype System.

ple: (IP address of my computer:Port number of my computer, Destination IP address:Destination Port number, Layer 4 Protocol(TCP or UDP)). We visualize one network connection as one line in parallel coordinates. There are three vertical lines in the pane. Moving left to right, these lines are the axes that represent each value for: the port number of the host computer, the destination port number and the IP address. We assign a port number value "0" to the top of the axis and port number value "65535" to the bottom of the axis. We also assign an IP address value "0.0.0.0" to the top of the axis and "255.255.255.255" to the bottom of the axis. We did not represent the IP address of the host computer in the visual pane because we consider that the information makes no contribution to find anomalies in the network connections. From these value assignments, one tuple of network connection information is plotted to three points over three axes. We then connect their points using a line. The color of the line indicates the communication status of the network connection: sending and/or receiving data.

We specified that the visual block can represent the network connection data over a specific time span. The reason is that a user can capture a trend of network connections in her/his computer by visualizing a block of data into one visual representation. The system could have visualized single connections into single visual representations, however, this would not be able to assist in the discovery of anomalies within a group of network connections viewed as a whole unless looked at by a security expert.

3 A Use Case Scenario

We explain a use case in the prototype system using the figure 1. The time slots view in the figure has three rows. The user can clearly recognize the visual difference between the two upper rows and the bottom row. The visual blocks in the bottom row have some bright lines that are not drawn in the upper visual blocks. The line brightness represents the frequency of network usage. Light network usage is represented with a bright line as major anomalous network connections tend to have small network usage to avoid detection by system administrators.

The connection status view shows a zoomed view about the bottom left block in the time slots view. The bright lines are drawn from a fixed point in the left axis to a fixed point in the right axis through some points in the middle axis. This means that user's computer communicated with a specific destination machine through some port numbers. If an expert knows this situation, he would suspect that there may be malware attempting to attack a specific service on a host computer. Because the line color of their connections means that they are all UDP connections and the data flow of them is only one way from a destiantion computer to a host computer. After an additional survey, these communications are caused by a legitimate utility software for a network printer.

In this case, it was not visual example caused by a security incident. It does however show that visual patterns of the network connection over a time span has the potential to detect anomalies in network connections. Even if a user does not have knowledge in the network domain, the user can still independently observe visual patterns of normal network connection activity on their computer through this system and use this information to compare to anomalous situations once/if they occur.

4 Conclusion

In this paper, we proposed a visualization system of network connections in a personal computer. A visual representation of network connections with temporal sequencing has the potential to enable users to build a normal model to which they can use to detect anomalous situations. A user evaluation study and providing of use case scenario using an actual security threat can be considered future works. We hope that this system could be a supplement to security tools for end users.

References

[1] H.Koike and K.Ohno, "SnortView: Visualization System of Snort Logs", In proc. of VizSec/DMSEC'04, pp.143-147, 2004.

[2] D.Inoue, M.Eto, K.Suzuki, M.Suzuki and K.Nakao, "DAEDALUS-VIZ: Novel Real-time 3D Visualization for Darknet Monitoring-based Alert System", In proc. of VizSec'12, pp.72-79, 2012.

[3] J. Stoll, C.S.Tashman, W.K.Edwards and K.Spafford, "Sesame: Informing User Security Decisions with System Visualization", In proc. of CHI'08, pp.1045-1054, 2008.

[4] SoftEther Corp., "Packet Police for Windows: A software for logging network connections and starting processes in a personal computer", http://www2.softether.jp/en/packetpolice/, Oct., 2012.