Cooperative Security Monitoring System

Jong-Hyun Kim
Electronics and Telecommunications Research Institute
Daejeon, Korea
jhk@etri.re.kr

Young-Soo Kim
Electronics and Telecommunications Research Institute
Daejeon, Korea
blitzkrieg@etri.re.kr

Ik-Kyun Kim
Electronics and Telecommunications Research Institute
Daejeon, Korea
ikkim21@etri.re.kr

ABSTRACT

Recently, security visualization plays a major role in interpreting and understanding security data and requirements. When dealing with large amounts of network security data, visualizing a manageable subset of that data for further investigation is an important consideration. The purpose of this paper is to review some of the current methods and present our visual solution to defend cyber threats.

Categories and Subject Descriptors

H5.2 [Information interfaces and presentation]: User Interfaces-Graphical user interfaces; K.6.5 [Management of Computing and Information Systems]: Security and Protection

General Terms

Security, Human Factors,

Keywords

Security visualization, Cyber threat, Network security monitoring, IP Traceback.

1. INTRODUCTION

Recently, cyber attacks against public communications networks are getting more sophisticated intelligent and varied. Moreover, in some cases, one country could make systematic attacks at a national level against another country to steal its confidential information and intellectual property. Therefore, the issue of cyber attacks is now regarded as a new major threat to national security. The conventional way of operating individual information security systems such as IDS and IPS may not be sufficient to cope with those attacks committed by highly-motivated attackers with significant resources. For real-time response cyber threats, not only individual security system, but also global cooperative security management system should be provided since there are global problems which cannot be solved by any single entity as well as single domain or single country. Now, many countries already recognized these issues and established many focus groups to develop technologies and guidelines to facilitate international cooperation and collaboration against cyber threats. For a systematic response to the cyber threat, the level of threats, the level of risk assessment, and a step-by-step alarm are required. it is possible to block threats at an early stage minimize the spread of the attack occurred by effectively visualizing cyber threats based on risk level, alarm reporting, and attack amount estimation.

2. RELATED WORK

Visualization may provide a means to improve the correlation process since security event data is massive and spans several devices requiring collaboration from each device administrator. A lot of research in visualization is currently in progress. Arcsight's Interactive Discovery provides the capability of out-of-the box visual perspectives. It includes visual charts such as parabox, time slice, histogram, and scatter plot [5]. NetIQ provides a distributed log warehouse, rule based correlation, and agent based change detection at the host/system level [10]. SecureScope is a three-dimensional visualization tool specializing in network security event data [21]. Each of these tools shows some relationship between in the security data that they represent. These relationships help security managers to explore and discover new information. Therefore, understanding how data relates and how to take advantage of visual perception with color, symbols, shape, etc. help users to make affective visualizations.

3. Cooperative security monitoring system

We developed the global cooperative security monitoring system called COSMOS, based on the automatically cooperative response framework for predicting and blocking the cyber threats such as DDoS attack. This system mainly performs the analysis of global intrusion event and 3D visualization of network security.

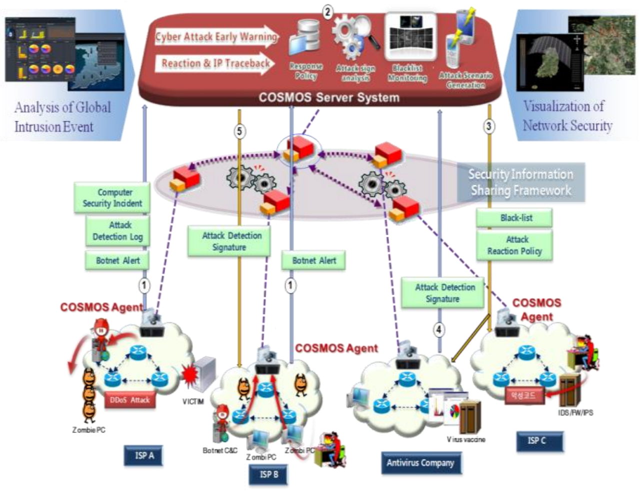

Figure 1. Framework of cooperative security monitoring system

Figure 1 shows the framework of COSMOS system. COSMOS has three components such as a server, an agent and an information sharing framework between the server and the agent. The agent can be located in major ISPs, Antivirus Company and so on. The server system may be located in national CERT or security monitoring center. The process of sharing security information in this framework can be explained as follows; First of all, we assume that cyber attack maybe be occurred in ISP A and ISP B, then the agent sends security information such as incident, attack detection log, and botnet alert to the server. And then the server analyzes those data and produces the accurate response policy. According to the security manager's decision, the server sends the corresponding policy to the agent. Finally, each ISP enforces the policy into their own security equipment for defending cyber attacks. Additionally, COSMOS system performs the analysis of global intrusion event and visualization of network security.

3.1 3D visualization of network security status

Figure 2 shows 3D visualization technique that is for intuitive diagnosis of network security status and fast response against malicious attacks by collecting security event logs from nation-wide networks in real time. It also visualizes the attack status, the distribution of zombies and C&C servers exploiting 3 Dimensional visualizing engines with geographic digital map technology. Additionally, it classifies the intrusion events by attack types and location,

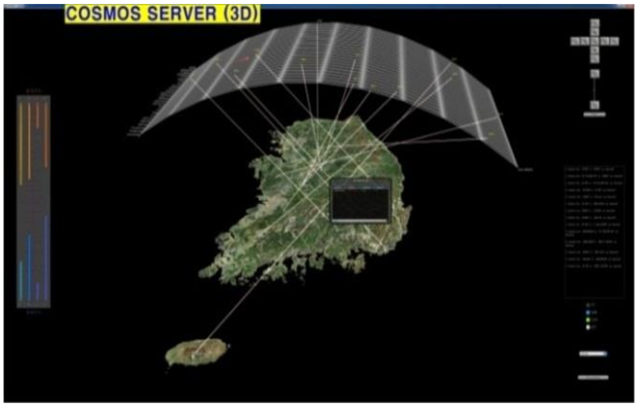

Figure 2. Visualizing global network security status

3.2 Network threat analysis & quantification

The technology uses a prediction model that can estimate the degree of cyber threats by monitoring botnet's size, activity, and propagation in a country, unlike the prediction model of existing research based on time series analysis.

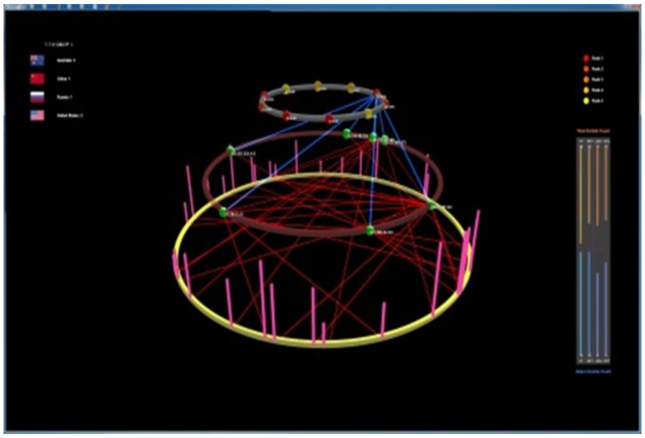

Figure 3. Visualizing network threat and quantification

Fig.3 shows visualization for detecting C&C servers and zombie PCs using following functions, 1) Estimation of the size of Zombies using DNS analysis and traffic monitoring, 2) Zombie PC's activity monitoring 3) Intuitive diagnosis of network security status and fast response through a threat quantification algorithm.

3.3 Web-based IP traceback

Web-based file sharing site has a strong point that the user can be provided with the information whatever and whenever he or she wants, however, the analysis of the uploaded file is needed since it is used as an attack spread site of network invasion attack

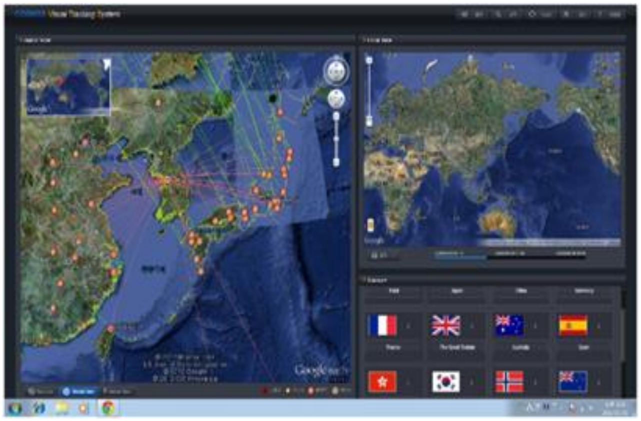

Figure 4. Visualizing Web-based IP traceback

Fig.4 shows a real-time tracing application by monitoring file uploading/downloading behavior in the Web-based file sharing site and by creating and managing tracing logs for suspicious files.

4. CONCLUSION

This paper introduces visual solutions that deal with three major outputs such as global cooperative response framework, network analysis on cyber threats, and Web-based tracing source of attack. In terms of future work, we are interested in visualizing the prediction model of cyber threats based on APT (Advanced Persistent Threat). We are also interested in some visual solutions for more sophisticated statistical and data mining capabilities in dealing with the cyber threats occurred by botnets.

5. ACKNOWLEDGMENTS

This research was funded by the MSIP(Ministry of Science, ICT & Future Planning), Korea in the ICT R&D Program 2013[Cyber targeted attack recognition and trace-back technology based-on long-term historic analysis of multi-source data].

6. REFERENCES

[1] HP Arcsight Home Page <http://www8.hp.com/us/en /software-solutions/software.html>.

[2] NetIQ Home Page <http://www.netiq.com/products/sm /default.asp>.

[3] Secure Decisions <http://www.securedecisions.com>.