Visualizing Intrusion Detection

Sjur Ringheim Lid

2005/05/13

1 Introduction

Computer networks are getting increasingly complex and hard to keep safe against attacks. The tools used to defend these systems generate enormous amounts of data every day, and because of this are getting harder to use and administrate. With the ever increasing amount of new attacks in today's world the amount of data will keep increasing, and because of the base-rate fallacy [1] the amount of false alarms will also increase. Another problem with detection of attacks is that they usually isn't detected until after the attack has taken place, this makes defending against attacks hard and can easily lead to disclosure of sensitive information. The fact that most businesses don't perform much forensic examinations after a successful attack, and almost never report these crimes makes detecting and stopping attacks even more important. These problems leads to the need for systems that makes detecting attacks easier and faster and is easy to use for security professionals.

What is proposed in this extended abstract is to make a system for early detection of attacks against a computer network. The system will use as little information as possible in the process to make it have the smallest amount of impact on the performance of the network its protecting. This system will work by visualizing changes in network traffic so that an administrator will have the ability to detect unusual patterns and use this as an indicator of an attack. Other systems, like Intrusion detection systems(IDS), that saves and detects more specific attack information will have to be used to confirm that there really is an attack.

The reason behind choosing to use visualization for this system is as noted in [2] that (1)

> human vision is especially tuned for discriminating tiny but high contrast visual effects (referred to in psychology as the just-noticeable-difference)

and (2)

> humans perform well at recognizing visual patterns especially when intuition can be used (ecological design)

Another reason why visualization is used is the old fact that humans have a short time memory of seven plus minus two elements [3]. This makes our capability of seeing patterns in the textual representation of attack patterns fairly small, while when seeing it visual the operator will be able to detect changes between multiple pictures. The use of color in the pictures will also make it easier for the operator to see areas where unusual traffic is occurring.

1.1 Research questions

The research questions that will be answered through the work with this thesis is:

1. How much of the IP-header data going through the network is needed to give a visualization that can be used for intrusion detection.
2. How often will these data have to be updated to the visualization module.
3. What is the best method of visualization for this type of use.

2 Previous work

Visualization of computer networks have been used in many contexts, [4] is one type of systems that has been developed to aid computer network designers in their work. [5] is another type of system that will give people working on the network an overview of load balancing and changes in the network.

When it comes to visualization and computer security there have been done multiple works, the most note full works of later date are [6] who developed a system to enhance a system administrators ability to detect anomalous traffic between internal and external domain. Their approach to visualizing the flow of data was to display links between two machines or domains. [2] [7] developed a tool that visualizes network flow information in a grid network of at most 65K unique nodes (a class B network). Another method that has been developed is [8], their approach is to use stacking of histograms that represent nodes and ports in the network to visualize changes in the network. All of the above systems have used some form of drill-down method that will give a user multiple levels of details about the flow of traffic in the supervised systems.

There has also been other types of visualization systems developed, like [9] that uses visualization to categorize different types of scan patterns, and [10] which uses visualization to visually confirm that data sent from one server is received by a temporary server and read/used by the users who asked for the information within a given time limit.

3 Claimed contributions

It is easy in large networks to mirror all traffic going through the network to a IDS, the problem behind this is that it creates so much traffic that you will have to decide which parts of the network you want the IDS to examine. The system proposed developed here will be a prototype for a system that will try to use IP-header data to guide the operator into knowing which parts of the network the IDS should examine at any given time.

For this thesis we will be using a hypothesis that states that visualization of IP-header information is enough information for an operator of a network to be able to guide their IDS's to look at the right spots of the network at any given time to detect and prevent attacks. There will be used as little of the header information as possible, so as not to increase the load on the network. Since there isn't any indicators on what is enough information in any literature we have found this will have to be researched. Another question that has arisen is whether the system needs to capture information about all packages or if a given percentage of packages is enough to give a good enough picture about the state of the network for this task.

There will also be researched how often the sensors placed in the network will need to update their information to the visualization module to make the image of the network relevant enough

for the operator to detect attacks. This will be done by using different time windows for the update, and there will also be tried with a smart module at the sensors end that will update when it believes that an attack is taking place.

How the correlation of information from the various sources used shall be done will also be a part of the thesis.

When it comes to the visualization part of the thesis there have been done some work earlier as stated in the previous work section of this extended abstract. These methods will be researched and other methods will also be taken into account before it is chosen which method to use.

Bibliography

[1] Axelsson, S. 1999. The Base-Rate Fallacy and Its Implications for the Difficulty of Intrusion Detection. In *ACM Conference on Computer and Communications Security*, 1–7.

[2] Yurcik, W., Lakkaraju, K., Barlow, J., & Rosendale, J. 2003. A Prototype Tool for Visual Data Mining of Network Traffic for Intrusion Detection.

[3] Miller, G. A. 1956. The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information. In *The Psychological Review*, volume 63, 81–97.

[4] Estrin, D., Handley, M., Heidemann, J., McCanne, S., Xu, Y., & Yu, H. November 2000. Network Visualization with the Nam, VINT Network Animator. *IEEE Computer*, 33(11), 63–68.

[5] Becker, R. A., Eick, S. G., & Wilks, A. R. 1995. Visualizing Network Data. *IEEE Transactions on Visualization and Computer Graphics*, 1(1), 16–28.

[6] Yin, X., Yurcik, W., Treaster, M., Li, Y., & Lakkaraju, K. 2004. VisFlowConnect: netflow visualizations of link relationships for security situational awareness. In *VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security*, 26–34, Washington DC, USA. ACM Press.

[7] Bearavolu, R., Lakkaraju, K., Yurcik, W., & Raje, H. A Visualization Tool For Situational Awareness Of Tactical And Strategic Security Events On Large and Complex Computer Networks.

[8] Abdullah, K., C. Lee, G. C., & Copeland, J. 2005. Visualizing Network Data for Intrusion Detection. In *2005 IEEE Workshop on Information Assurance and Security*.

[9] Muelder, C., Ma, K., & Bartoletti, T. October 2005. A Visualization Methodology for Characterization of Network Scans. In *Workshop on Visualization for Computer Security (VizSEC 2005)*.

[10] Swing, E. 1998. Flodar : Flow visualization of network traffic. In *IEEE Computer Graphics and Applications*, 6–8.