Repeat State Inputs in Echo State Networking Environment Through Bash Script Kernel Scanning

M.ASAN NAINAR[1], V. SANTHANA MARICHAMY[2], PRASANNA P[3]
[1, 2] *Department of General Engineering, SRM Valliammai Engineering College, India*
[3] *PG Student, Department of Computer Applications , SRM Valliammai Engineering College, India*

Abstract- ***Network level Security visualization is considered to be one of the foremost areas where most of the exploration is going on in visualizing the network nature for the systems. Due to vulnerability attacks and projection matrix manipulation, many investigators are directed towards security monitoring measures and preventive techniques against intrusions. There are many major procedures and technological jargons dominating the security related stuffs in the it industry. Many companies are focusing towards projecting their monitoring products in this evolving field. User accessed information such as number packet read and write, Input output response time and delay time were not tracked down. Visualizes all server status and activity and security events with client interaction. Ibm tivoli, spiceworks, xymon, intermapper are some of the major tools available in the market. Most of the tools picturize by monitoring certain items in the network/server. Network Trace and system activity can be Visualization and security events from the server and the interaction with the client were visualized in the module and also User contexts information were visualized. In this paper, the focused areas include host/server monitoring, internal and external monitoring, port activity and attack patterns. Network tomography is an important area of network measurement, which deals with monitoring the health of various links in a network using end-to-end probes sent by agents located at vantage points in the network/internet.***

Index Terms- ***Network tomography, Vulnerability attacks, Server monitoring, Visualization and end-to-end probes.***

I. INTRODUCTION

The visualization of network security events is the subject of this survey, this paper does not focus on designing and developing a specific visualization system. Instead, we consider network security with respect to information visualization and introduce a collection of use case classes. In this study, we provide an overview of the increasing relevance of security visualization. We explore a novel classification approach and review the artifacts most commonly associated with security visualization systems. Here provides a historical context for this emerging practice and outline its surrounding concerns while providing design guidelines for future developments.

Visual data analysis helps to perceive patterns, trends, structures, and exceptions in even the most complex data sources. As the quantity of network audit traces produced each day grows exponentially, communicating with visuals allows for comprehension of these large quantities of data. Visualization allows the audience to identify concepts and relationships that they had not previously realized. Thereby, explicitly revealing properties and relationships inherent and implicit in the underlying data. Identifying patterns and anomalies enlightens the user, provides new knowledge and insight, and provokes further explorations. It is these fascinating capabilities that influence the use of information visualization for network security. Visualization is not only efficient but also very effective at communicating information. A single graph or picture can potentially summarize a month's worth of intrusion alerts (depending on the type of network), possibly showing trends and exceptions, as opposed to scrolling through multiple pages of raw audit data with little sense of the underlying events. Security Visualization is a very young term. It expresses the idea that common visualization techniques have been designed for usecases that are not supportive of security-related data, demanding novel techniques fine-tuned for the purpose of thorough analysis. It may not always be possible to fully predict how an end user will perceive and interpret a design due to the varying nature of the audience's cognitive characteristics. Yet careful

consideration of the user's needs, cognitive skills, and abilities can determine the appropriate content and design. Often associated with human-computer interaction, the philosophy of user-centered design places the end user at the center of the design process. Network security is a highly specialized and technical discipline and operation.

It deals with packets and flows, intrusion detection and prevention systems, vulnerabilities, exploits, malware, honeypots, and risk management and threat mitigation. The complex, dynamic, and interdependent nature of network security demands extensive research during the development process. Without an in-depth understanding of security operations and extensive hands on experience, developing a security visualization system will not be possible. A design process centered on the needs, behaviors, and expectations of security analysts can greatly influence and impact the usability and practicality of such systems. For best results, security experts and visual designers must thereby collaborate to complement each other's skills and expertise to innovate informative, interactive, and exploratory systems that are technically accurate and aesthetically pleasing. In this survey, we begin by looking into different categories of data sources incorporated in the design of security visualizations and provide an informative list of sources accessible to the research community. By expressing the main contribution in the classification of network security visualization systems. We provide a detailed description of the proposed taxonomy together with an analysis of the derived use-case classes. We follow by giving a thorough description of each system as we outline its strengths and weaknesses. An overall assessment of systems in each use-case class in addition to guidelines and directions for future systems is also provided.

Security visualization is one of the major area where most of the researches going on in visualizing the network nature for the systems. Due to vulnerability attacks and projection matrix manipulation. Many researchers are directed towards security monitoring measures and preventive techniques against intrusions. There are many major techniques and technological jargons dominating the security related stuffs in the IT industry. Many companies are focusing towards projecting their monitoring products in this evolving field. ibmtivoli, spiceworks, xymon, intermapper are some of the major tools available in the market.

Most of the tools picture by monitoring certain items in the network/server. In this system, the focused areas include host/server monitoring in an network environment with specific features like internal and external monitoring, port activity and attack patterns. Network tomography is an important area of network measurement, which deals with monitoring the health of various links in a network using end-to-end probes sent by agents located at vantage points in the network/Internet.

The objective of the system incorporates all the above said information's. In addition, here try to focus on the basic stuffs like possible errors, User access, network related data transmission, Server reads/writes, Services and all other IO related information's in an optimistic way using Spinning Cube of Potential Doom Algorithm.

The system provides the way to manage the virtual machines by using the concept called visualization. This visualization helps to easily identify the state of the server in order to increase the security and other network flaws. It periodically updates itself and inform it to the admin by means of the graphical representation, because graphical representation provides much attention and it was easy to understand that how far the server was affected.

II. LITERATURE REVIEW

In the paper [1], the author is emphasizing insider threat detection in network monitoring domain and identify the threat is the main nature of this paper. Doesn't have any practical information and the paper fully focuses on theoretical part. Implication on performance is not explained in the paper.

And the paper [2], Distribution of the data entries to be published and the statistical distribution of the data stream is the core idea of the system and it's not handled ever before in this perception. Here didn't clearly explain once the data is mined for getting multidimensional data.

In the paper [3], A Document Model Management Framework based on Core Components. Usage of appropriate tools for implementing specific functionalities is an added advantage to simplify the problem. Currently, this tool doesn't support various modeling and transformation tasks as is necessary for model management. This paper doesn't support model versioning.

In the paper [4], The system uses a new attribute-based encryption protocol to control access to such identifying attributes. It supports threshold access rights and provides a heuristic instantiation of revocation. This paper didn't explain about the about the type of hacking and the relationship between the attributes and the prevention technique.

III. TECHNOLOGY IMPACTS ON ANALYSIS

In the existing system, focusing of the major technical perceptions for this network visualization areas.

- Endpoint Connectivity (Host / Server Monitoring)
  - Connectivity with the host and server will be monitoring for any down fall time
  - Utilization of the system – details about the host vs server utilization.
  - Number of accessible users - Calculating the individual and concurrent users on the system.
- Logging
  - Packet Traces –tracing the packets traversing between in the systems.
  - Server logs – monitoring the security, application logs in the server.
- Port Activity
  - Server shots interactions – monitor the port and protocol used in communication.
  - Level of activity through the port
- Intrusion detection
  - Intrusion alerts-alerts create by the developers on anonymous activities.
  - DNS traces – recording anonymous entries in the domain.

The existing system couldn't identify or specify the implication of the major disaster or network flaw in a system.

They didn't specify the exact pinpoint of issue and precautionary measures.

In the existing system, they've proposed various techniques in visualizing the network data. But unfortunately, they couldn't identify or specify the implication of the major disaster or network flaw in a system. In the proposed approach provides the detailed visualize of the network information as mentioned below,

- Number of TOTAL PACKETREADS
- Latest packets read in a specific interval
- Number of TOTAL WRITES ON THE PACKETS
- Latest packets write in a specific interval
- Complete Input/output busy time
- Complete CPU busy schedule
- Complete Input/output Reads
- Latest number of seconds Input / Output reads
- Number of process info reported errors
- Number of spid's reported error in the server
- Authentication information's
- Disabled services in the server

IV. System Description

The network security is the core component of this system, here the development of the monitoring system to enhance the performance and the security-based issues in the network environment. The visualization was the concept used in this system, where it helps to understand the amount of threats and other issues affected the system. Visualization provides an easy way of plotting the issues in the form of graph. So this system will boycott the old way of analyzing the physical values by giving an affected values in the form of diagrammatic representation so that it will give more attention than the old ways.

The Figure 1 depicts the architectural diagram of the system and the Figure 2 shows the visualization to client-server data flow model. The Initial Virtual Machine Information process defines the network and traces the initial; machine information using the algorithm Data Stream Model and the k-ary Sketch Algorithm which is generable from a network and produces a network N such that is generable from N and not from any other network.

Figure 1 System Architecture

The Server level information process tends to define:

1.The Number of packets Received/Send Status will be notified.
2.Along with that the Graphical Representation of the server level status information will be notified and shown in the graphical illustration.
3.The network packets info will also be defined in this module by indicating the packer revived status, Packets sent status & the Error packets status

Security events from the server and the interaction with the client were visualized in the Read/Write Status module.

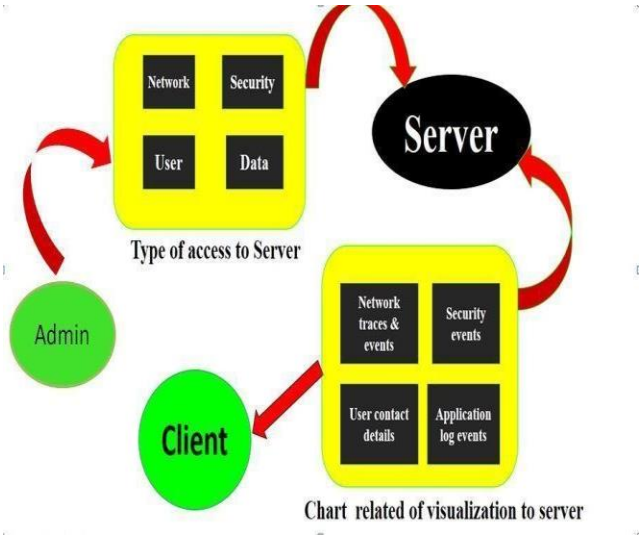

Figure 2 Client-Server Data Model

Technologies, services, and terms related to Identity management include Active Directory, Service Providers, Identity Providers, Web Services, Access control, Digital Identities, Password Managers, Single Sign-on, Security Tokens, Security Token Services.

V. CONCLUSION

As the number of security related events generated in modern networks is on the rise, the need for network security visualization systems is felt more than ever. In this paper, the recent works in network security visualization from a use-case perspective are examined. Five use-case classes, each representing a different application area, were defined and several recent works in each category were thoroughly described.

The underlying data sources of network security visualization and gave a few examples of each category are detailed. Analysis of these systems motivated us to examine several issues and concerns surrounding this emerging field. Also the advantages and shortcomings of all use-case classes and shed light on paths that researchers should focus toward are elaborated. The findings of the work into an informative table for future references. While the field of visualization is as wide as imagination allows, the analysis and taxonomy presented here will motivate better future work in this area.

REFERENCES

[1] Justin Myers, Michael. Grimaila, Robert F. Mills, Towards Insider Threatr Detection using Web Server Logs, Journal of Cyber Security and Information Intelligence Challenges and strategies.

[2] Bin Zhou, Yi Han, Jian Pei, Bin Jiang, Yufei Tao, Continuous Privacy Preserving Publishing of Data Streams, International Conference on Extending Database Technology, 2009, pp 648-659.

[3] Michael Strommer, Christian Pichler, Philipp Liegl, A Document Model Management framework based on core components, IEEE Conference on Commerce and Enterprise Computing, 2010, .

[4] Jessica Staddon, Philippe Golle, Martin Gagne, Paul Rasmussen, A Content Driven Access Control System, Symposium on Identity and rust on the Internet, 2008.

[5] Xinheng Wang, Chuan Xu, Guofeng Zhao, Kun Xie, Shui Yu Efficient Performance Monitoring For Ubiquitous Virtual Networks Based on Matrix Completion, IEEE,2018.

[6] C. Ware, Information Visualization: Perception for Design. Morgan Kaufmann Publishers, Inc., 2004.

[7] G. Conti, Security Data Visualization. No Starch Press, 2007.

[8] R. Marty, Applied Security Visualization. Addison-WesleProfessional, 2008.

[9] R. Erbacher, K. Walker, and D. Frincke, “Intrusion and Misuse Detection in Large-Scale Systems,” IEEE Computer Graphics and Applications, vol. 22, no. 1, pp. 38-48, Jan./Feb. 2002.

[10] R. Erbacher, “Intrusion Behavior Detection through Visualization,” Proc. IEEE Int’l Conf. Systems, Man and Cybernetics, pp. 2507-2513, 2003.

[11] T. Takada and H. Koike, “Tudumi: Information Visualization System for Monitoring and Auditing Computer Logs,” Proc. Sixth Int’l Conf. Information Visualisation, pp. 570-576, 2002.

[12] K. Lakkaraju, W. Yurcik, and A. Lee, “NVisionIP: Netflow Visualizations of System State for Security Situational Awareness,” Proc. ACM Workshop Visualization and Data Mining forComputer Security, vol. 29, pp. 65-72, 2004.