isrjournals

International Journal of Advanced Research in Computer Networking,Wireless and Mobile Communications

Volume: 5 Issue: 3 Mar,2022,ISSN_NO: 2320-7248

PULL STRATEGIZED KERNAL MONITORING WITH SHELL TECHINQUE

Manoj Kumar.R[1]

Student, Dept of MSC Cyber Forensic Information and Security(CFIS),
Dr. MGR Educational and Research Institute, Maduravoyal, Chennai-600095, India[1].

ABSTRACT— *Network monitoring enables the administrators to monitor a computer network for slow or failing components. In case of outages or other troubles the administrator can pinpoint where the exact issue is the system enables us to find out*

- *List of services in the target machine*
- *Read Memory / Time / Usage*
- *Write Memory / Time / Usage*
- *Performance/Speed of the system in writing / reading data*
- *Access specifications, like => Login Details*

  => Access to each login

  => Database lists

  => Access to the databases

  => Server Role / Members Group

  => Database Roles

Keywords— **network monitoring, computer network**.

INTRODUCTION:

Although 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, consider network security with respect to information visualization and introduce a collection of use case classes. In this study, provide an overview of the increasing relevance of security visualization. And explore a novel classification approach and review the artifacts most commonly associated with security visualization systems. Provide a historical context for this emerging practice and outline its surrounding concerns while providing design guidelines for future developments. Visual data analysis help 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 use cases 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, 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 our main contribution in the classification of network security visualization systems. Provide a detailed description of the proposed taxonomy together with an analysis of the derived use-case classes. Follow by giving a thorough description of each system as 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. Summarize the multiple attributes of recent network security visualization systems in a table for better future references. By outlining issues and concerns surrounding security visualization by elaborating on seven potential pitfalls. By summarizing our findings. Papers studied in this survey were selected based on the following metrics:

1. Relevance to network security: As the title of the paper indicates, this study focuses specifically on network security visualization systems. Visualizations of code security, binary files, or visual cryptanalysis are subjects that could span another volume of similar size and are thereby not considered in this study.

2. Contribution of system and visual techniques: Due to the chronological study of papers, systems that have utilized a specific visualization technique or method with highly similar characteristics to those of previous systems have not been selected for this survey. Similarly,

visualization systems that lack contextual, perceptive, and cognitive considerations are also not considered.

3. Satisfactoriness of evaluation: Although most systems surveyed in this paper lack formal evaluation yet many have been validated through ad hoc use case attack scenarios. Systems that lack even this basic validation strategy are also not considered in this survey. Believe these three metrics impact the quantity and quality of papers surveyed in this work to resemble systems that are focused explicitly on network security, are novel in their incorporated visual techniques, and are validated on at least a use-case scenario. Systems that do not adhere to these metrics are thereby not considered in this study.

OBJECTIVE:

- The Objective of the project incorporates all the above said information's.
- In addition, 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.

SCOPE:

Scope/Aim of the project is focused on providing an insight view of the Virtual machines by considering the following factors like, Normalized throughput, Server throughput, Aggregated throughput, reply time, Transfer time, CPU time per execution, Net I/O per second, CPU utilization, Execution per second.

SYSTEM STUDY:

EXISTING SYSTEM:

- In the existing system, focusing on the major technical perceptions for our network visualization areas.
- Endpoint Connectivity (Host / Server Monitoring)

  Connectivity with the host and server will be monitoring for any downfall 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 the systems.

  Server logs – monitoring the security, application logs in the server.

- Port Activity

  Server vs host 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.

DISADVANTAGES:

- Couldn't identify or specify the implication of the major disaster or network flaw in a system.
- They didn't specify the exact pin point of issue and precautionary measures.

PROPOSED SYSTEM:

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 our proposed approach, provide the detailed visualize of the network information as mentioned below,

- Number of TOTAL PACKET READS
- Latest packets read in a specific interval
- Number of TOTAL WRITES ON THE PACKETS

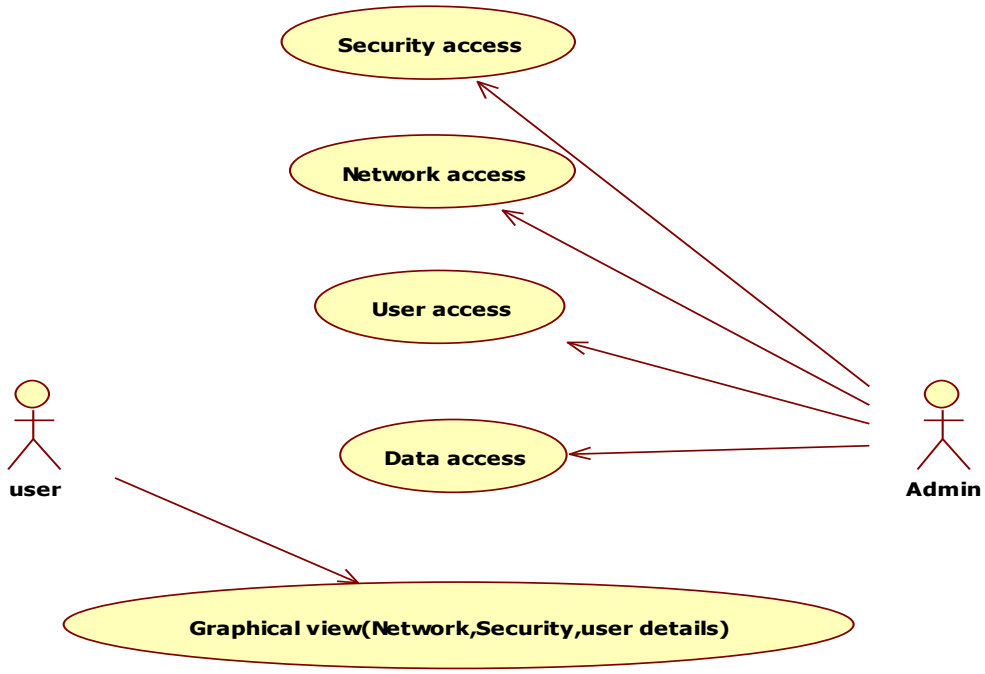
- Latest packets write in a specific interval
- Complete Input/output busy time
- Complete CPU busy schedule
- Complete Input/output Reads
- Latest number of seconds Input / Output reads
- Number of process info reported errors
- Number of spid's reported error in the server
- Authentication information's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

In our system, trying to project the detailed view of how the problem occurred and possible solution for the servers. Intrusion related information's were considered and precautionary measures towards intrusions will be addressed in our future work.

ADVANTAGES:

- Security events from the server and the interaction with the client were visualized.
- Visualized all the system process of server and also User contexts information were visualized.
- Traces of the data navigation happening in the network seeing data's in visualization manner.

Use case diagram



CONCLUSION:

SUMMARY

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, I have examined recent works in network security visualization from a use-case perspective. Five use-case classes, each representing a different application area, were defined and several recent works in each category were thoroughly described. And detailed the underlying data sources of network security visualization and gave a few examples of each category. Analysis of these systems motivated us to examine several issues and concerns surrounding this emerging field. I have elaborated on the advantages and shortcomings of all use-case classes and shed light on paths that researchers should focus toward. And aggregated the findings of our work into an informative table for future references. While the field of visualization is as wide as imagination allows, I hope that the analysis and taxonomy presented here will motivate better future work in this area.

FUTURE ENHANCEMENTS:

In future work, field. I have elaborated on the advantages and shortcomings of all use-case classes and shed light on paths that researchers should focus toward. And aggregated the findings of our work into an informative table for future references. While the field of visualization is as wide as imagination allows, I hope that the analysis and taxonomy presented here will motivate better future work in this area.

REFERENCES:

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

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

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

[4] 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.

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

[6] 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.

[7] 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.