International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

3 JUNCTURE BASED ISSUER DRIVEN PULL OUT SYSTEM USING DISTRIBUTED SERVERS

M.V.S.L TEJASRI[1], Mr. R. KANNAN [2]

[1]Student, Department of Computer science and Engineering, Gojan School of Business and Technology, Redhills, Chennai
[2]Assistant professor, Department of Computer science and Engineering, Gojan School of Business and Technology, Redhills, Chennai

---

Abstract - *Network level Security visualization is considered to be one of the foremost area 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 security events with client interaction. Ibmtivoli, 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 our project, our 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.*

***KeyWords*: Visualization, host/server monitoring, internal and external monitoring, port activity and attack pattern**

1. 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, 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. We provide 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 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 risk0 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 our 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 23systems is also provided. We 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

1.1 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.

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.

1.2 Satisfactoriness of evaluation

Although most systems surveyed in this paper lack formal evaluation yet many have been validated through ad hoc usecase attack scenarios. Systems that lack even this basic validation strategy are also not considered in this survey. We 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.

2. EXISTING SYSTEM

In the existing system, we are focusing on the major technical perceptions for our network visualization areas. 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*servervs host interactions – monitor the port and protocol used in communication level of activity through the portIntrusion detectionintrusion alerts – alerts create by the developers on anonymous activities.dns traces – recording anonymous entries in the domain.

3. RELATED WORKS

Towards Insider Threat Detection using Web Server Logs. Malicious insiders represent one of the most difficult categories of threats an organization must consider when mitigating operational risk. Insiders by definition possess elevated privileges; have knowledge about control measures; and may be able to bypass security measures designed to prevent, detect, or react to unauthorized access. In this paper, we discuss our initial research efforts focused on the detection of malicious insiders who exploit internal organizational web servers. The objective of the research is to apply lessons learned in network monitoring domains and enterprise log management to investigate various approaches for detecting insider threat activities using standardized tools and a common event expression framework[1]

Continuous Privacy Preserving Publishing of Data Streams. Recently, privacy preserving data publishing has received a lot of attention in both research and applications. Most of the previous studies, however, focus on static data sets. In this paper, we study an emerging problem of continuous privacy preserving publishing of data streams which cannot be solved by any straightforward extensions of the existing privacy preserving publishing methods on static data. To tackle the problem, we develop a novel approach which considers both the distribution of the data entries to be published and the statistical distribution of the data stream. An extensive performance study using both real data sets and synthetic data sets varies the effectiveness and the efficiency of our methods[2]

A Document Model Management framework based on core components his paper implements a document model management framework, based on core components. This framework is built on an open source basis and may cope with interoperability problems providing transformation and schema generation components[3]

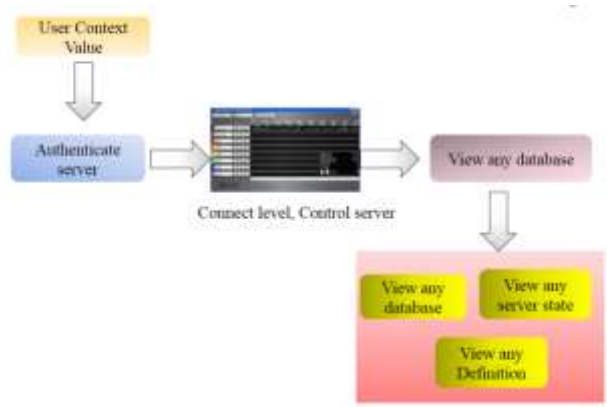
A Content Driven Access Control System

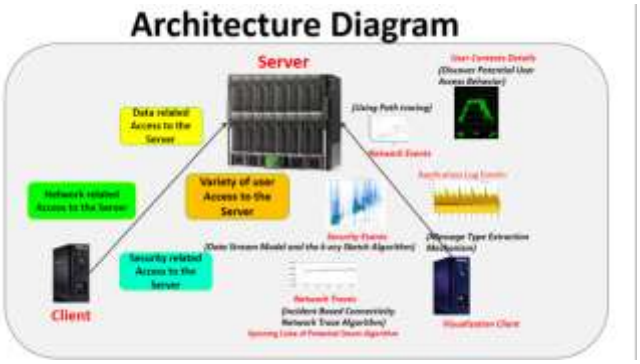
Protecting identity in the Internet age requires the ability to go beyond the identification of explicitly identifying information like social security numbers, to also find the broadly held attributes that, when taken together, are identifying. We present a system that can work in conjunction with natural language pro9cessing algorithms or user-generated tags, to protect identifying attributes in text. The system uses a new attribute-based encryption protocol to control access to such identifying attributes and thus protects identity. The system supports the dentition of user access rights based on role or identity. Our system encrypts not only sensitive personal information, but also groups of personal attributes which may indirectly allow for the inference of a person's identity, even though none of the attributes is directly sensitive. Personal attributes are encrypted with an attribute-based encryption scheme, which allows for efficient, fine-grained access control based on the content of documents

4. 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, we 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, we are 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.

5. SYSTEM DESIGN FOR DISTRIBUTION OF DATA





6. SYSTEM IMPLEMENTATION

- Initial Virtual Machine Information Module:
- Virtual Machine Disk Space Details Module:
- Server Level Information Module:
- Network Path Tracing Module (Server level data info module):
- Read/Write Status Module:
- Application Log Events Visualization Module:
- User Contexts Visualization Module

7. MODULE DESCRIPTION

7.1 Initial Virtual Machine Information Module:

The Initial Virtual Machine Information Module 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.

Machine Name will be defined. Server Name (instance Name) will be noted. Edition Installed will be updated. Product Build Information Level info will be shown.

SP Level & Collation Type will be fixed

Last Query/Server usage will be monitored

Number of Cup's Used is notified

Hyper Thread OS Level will be well-defined

Memory(MB) will be observed.

Virtual Memory(MB) will be shown.

MAX Worker Count will be acquainted

OD Priority Class will be noted. Scheduler Count will be traced.

7.2 Virtual Machine Disk Space Details Module:

The Disk Space Details modules define the "Virtual Disk Space Details information" such as Drive info details (C:/DRIVE, E: DRIVE), Also the memory/Free space allocation in Megabyte(MB) will be observed.

7.3 Server Level Information Module

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

7.4 Network Path Tracing Module (Server level data info module)

Path tracing is a graphical method of rendering traces of the data navigation happening in the network such that the global illumination is faithful to reality.

This algorithm is integrating over all accumulation of data arriving to a single point on the surface of an object. This accumulation is then reduced by an into sub paths based on the different access points in different intervals. Following items were visualized under this module: Number of TOTAL PACKET READS (In terms of bytes) since the last server was started Latest packets read in a specific interval (Data read in bytes) Number OF TOTAL WRITES ON THE PACKETS (In terms of bytes) since the last server starts Latest packets write in a specific interval (Data read in bytes)connection estabilished.

7.5 Read/Write Status Module

Security events from the server and the interaction with the client were visualized in the module:

Detailed analytical values of a login have been added or removed as a database user to a database.

Detailed analytical values of a login were added or removed from a fixed server role.

Detailed analytical values of a login have been added to or removed from a role. Detailed analytical values of a database role were added to or removed from a database. Detailed analytical values of a login have been added or removed. Detailed analytical values of a password have been changed for an application role. Detailed analytical values of a backup or restore statement has been issued. Reports audit messages related to Service Broker dialog security.

Reports audit messages related to Service Broker transport security. Indicates that an audit trace modification has been made. Indicates that the permissions to change the owner of a database have been checked.

7.6 Application and Log Events Visualization Module

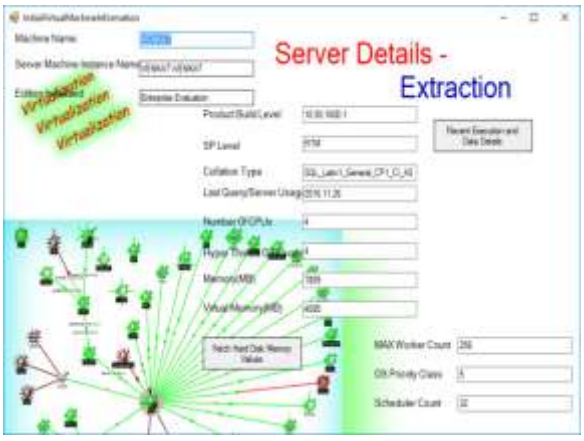
Security events from the server and the interaction with the client were visualized in the module: Successful trusted logins, successful non-trusted logins, failed user logins.

7.7 USER CONTEXTS Visualization Module

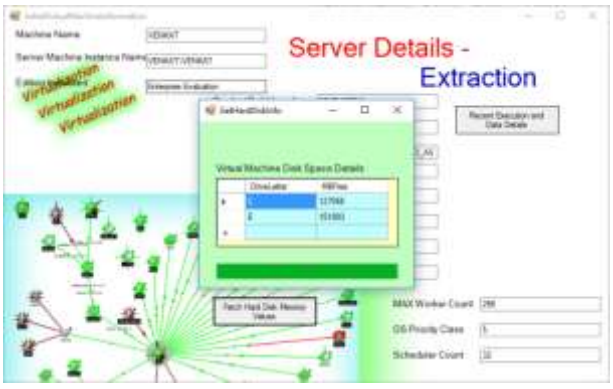
User contexts information were visualized in the module, Identity management indicates the management of individual identifiers, their authentication, authorization privileges/permissions within or across system and enterprise boundaries with the goal of increasing security and productivity. Identity management systems, products, applications, and platforms are commercial Identity management solutions implemented for enterprises and organizations. 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.

8. SCREEN SHOTS

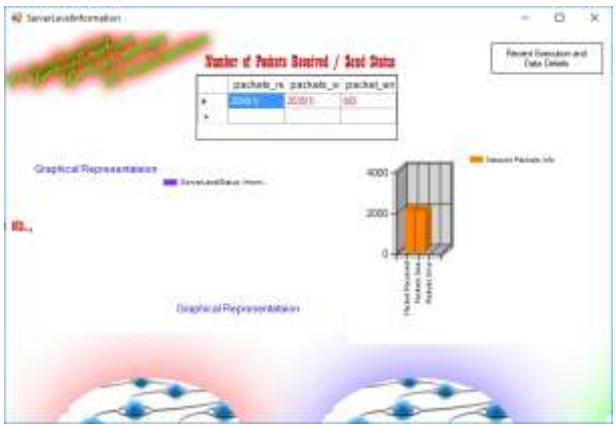
HOMEPAGE



SERVER DETAILS EXTRACTION

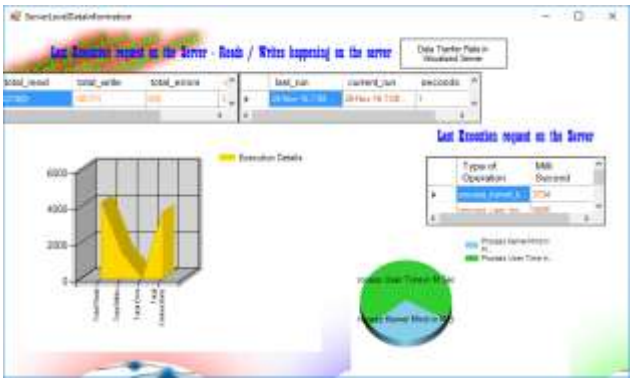


NUMBER OF PACKETS RECIEVED/SEND STATUS

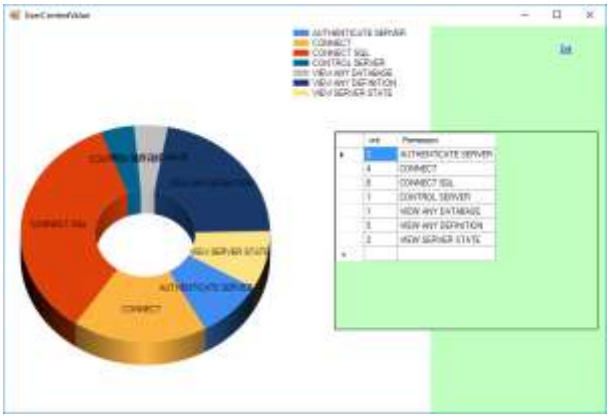


USER LOG EVENT TRACING

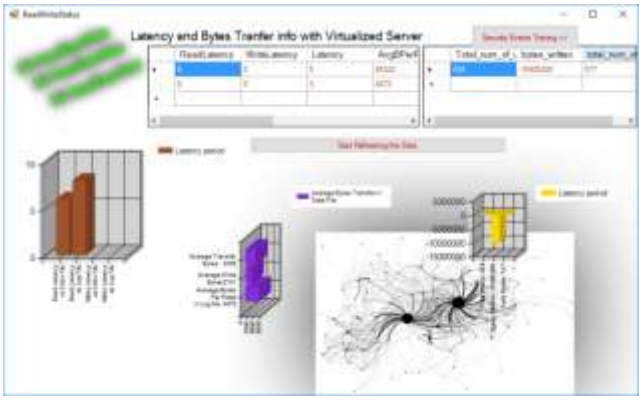
LAST EXECUTION REQUEST ON SERVER READS/WRITES



USER CONTEXT VALUE



LATENCY AND BYTES TRANSFER INFO WITH VIRTUALIZED SERVER



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

FUTURE ENHANCEMENTS

In future work, field. We elaborated on the advantages and shortcomings of all use-case classes and shed light on paths that researchers should focus toward. We aggregated the findings of our work into an informative table for future references. While the field of visualization wide.

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 Visualization, 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.