



### 3 JUNCTURE BASED ISSUER DRIVEN PULL OUT SYSTEM IN DISTIBUTED SERVERS

Siva sankari. A <sup>1</sup> Department of Computer applications, Dhanalakshmi Srinivasan college of arts and science for women, Perambalur, India.	Kanimozhi.M <sup>2</sup> Department of Computer applications, Dhanalakshmi Srinivasan college of arts and science for Women, Perambalur, India.	Kanimozhi.K <sup>3</sup> Department of Computer applications, Dhanalakshmi Srinivasan college of arts and science for women, Perambalur,India.
--	--	---

#### 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. There are many major procedures and technological jargons dominating the security related stuffs in the it industry. 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. 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—Relevance to network security, data processing, visual techniques, Satisfactoriness.**

#### 1. INTRODUCTION

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 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.

## 2. WHAT IS DISTRIBUTED SERVERS

### What Comprises Distributed computing?

Distributed computing is a field of computer science that studies distributed systems. A distributed system is a model in which components located on computers communicate and coordinate their actions by passing messages. A computer program that runs in a distributed system is called a distributed program, and distributed programming is the process of writing such programs.

## SYSTEM ANALYSIS

### Existing system:

#### 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.

### proposed system:

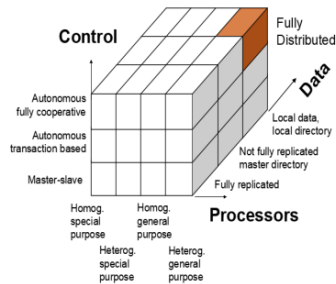
- Number of TOTAL PACKET READS
- Latest packets read in a specific interval
- Number of TOTAL WRITES ON THE PACKETS
- Latest packets write in a specific interval
- Complete Input/output busy time
- Complete CPU busy schedule
- Complete Input/output Reads
- Latest number of seconds Input / Output reads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

### 3. DISTRIBUTED SYSTEM

**Characteristics of Distributed System:**

- Data set can be split in to fragments and can be distributed across different nodes within network.
- Individual data fragments can be replicated and allocated across different nodes.
- Data at each site is under control of a DBMS.
- DBMS at each site can handle local applications autonomously.
- Each DBMS site will participate in at least one global application.

1. Distributed System Types



**Advantages of Distributed System:**

- **Sharing Data:** There is a provision in the environment where user at one site may be able to access the data residing at other sites.
- **Autonomy:** Because of sharing data by means of data distribution each site is able to retain a degree of control over data that are stored locally.

### 4. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system.

**MODULE DESCRIPTION:**

**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.

**Virtual Machine Disk Space Details Module:**

The Disk Space Details modules define the “Virtual Disk Space Details information” such as:

1. Drive info details (C:/DRIVE, E: DRIVE)
2. Also the memory/Free space allocation in Megabyte(MB) will be observed.

**Server Level Information Module:**

The Server level information module tends to define:

The Number of packets Received/Send Status will be notified.

Graphical Representation of the server level status information will be notified and shown in the graphical illustration.

**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.

#### **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.
- 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.

## **5. CONCLUSION AND FUTUREWORK**

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. 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.

#### **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-Wesley Professional, 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.

