# Information Visualization for an Intrusion Detection System

James Blustein
Faculty of Computer Science
Dalhousie University
Halifax, NS, Canada
jamie@cs.dal.ca

Ching-Lung Fu
Faculty of Computer Science
Dalhousie University
Halifax, NS, Canada
cfu@cs.dal.ca

Daniel Silver
Jodery School of Comp. Sci.
Acadia University
Wolfville, NS, Canada
danny.silver@acadiau.ca

## ABSTRACT

Spatial hypertext was developed from studies of how humans deal with information overflow particularly in situations where data needed to be interpreted quickly. Most users of intrusion detection systems (IDS) do not monitor their system continuously and IDS have high false alarm rates. The proposed system that utilizes spatial hypertext workspace as the user interface could reduce the impact of high false alarm from IDS. This system may improvement the user's willingness to continuously monitor the system.

**Categories and Subject Descriptors:**
H.5.4 [**information Interfaces and Presentation**]: Hypertext/Hypermedia—*Theory, User, Issues*
H.5.2 [**Information Interfaces and Presentation**]: User Interfaces—*User-centered design*

**General Terms:** Design, Human Factors, Security.

**Keywords:** Spatial hypertext,

## 1. INTRODUCTION

Intrusion Detection Systems (IDS) look for attack signatures, which are specific patterns that usually indicate suspicious or malicious intent. Computer network administrators use IDS as a security management tool to monitor systems/networks. This task cannot be automated as IDS can report many false alarms and the final decisions have to be made by a human expert. Furthermore, previous surveys [10] showed that the quality of current IDS tools is poor for security administrators. There are two main problems in modern IDS: detection techniques, and user interfaces (UIs) that enable administrators to quickly recognize and respond to attacks [1]. Implementing better detection techniques can, in theory, have significant improvement in IDS performance. However, Whitten and Tygar [9] have shown that advanced technical solutions can fail if their user interfaces are not adapted to the users. A good user interface is particularly important in real-time and security applications where the users are likely to be stressed and errors can have serious consequences [2]. The objective of this work is to develop user interfaces that help to bridge the gap between monitoring software and users by developing interfaces that adapt to their users rather than systems that require the user to adapt their working styles. This article proposes an adaptive UI architecture for an IDS based on an uncommon interface model, namely spatial hypertext, which we feel is well suited to the specialized tasks of intrusion detection.

The article is organized as follows: first we discuss human factors in IDS, and how spatial hypertext can be suitable for user interfaces for IDS. Then, a high level system architecture is presented with how adaptive user interface based on user modelling is fitted in this architecture.

## 2. HUMAN FACTORS IN IDS

The target user group for this study is computer network administrators who need to know the security status in the network. Survey results published by Gates and Whalen [3] support the impression we formed from in-depth survey with several computer security experts in industrial, military, and academic computing [10]. In the survey, 15 out of 17 subjects are not satisfied with the tools they are currently using. Three-quarters of the comments of the current tools complained about the high false alarm rates. Eighty-eight percent of the subjects do not continuously monitor their systems and 30% of the subjects check the systems only after the attacks has been detected.

Whether an IDS is rules-based or machine learning based, high false alarm rates seem to be unavoidable. An 99% accurate IDS algorithm which processes 10,000 events will produce 100 errors; and 10,000 daily events in network traffic consider to be very small. Many tools display potential threats in a list with text messages. Going through many text messages is fatiguing and time consuming. We believe this may be the reason that many system administrators do not continuously monitor their IDS. We believe a good user interface for IDS should use meaningful symbols for each type of events and other means to assist the user to rapidly recognize false alarms and recognize real threats.

## 3. SPATIAL HYPERTEXT AS USER INTERFACE

Spatial Hypertext (SH) allows flexible data presentation. SH supports direct manipulation of the objects and relationships presented in a workspace [5]. By enabling users to manipulate the appearances of the objects and leave relational representations implicit and ambiguous, SH systems


*HT'05,* September 6–9, 2005, Salzburg, Austria.
ACM 1-59593-168-6/05/0009.

allows users to freely express and develop new insights from the materials represented by objects [5, 6]. SH has proven to be effective for dynamic information analysis tasks and it utilizes human's exceptional visual intelligence to rapidly recognize patterns from the spatial arrangement of the objects.

Our hypothesis is that when the events are displayed in the SH workspace, the implicit and subtle differences between the reported false alarms and real attacks from IDS can be rapidly recognized by the experts' eyes. This recognition ability of humans is usually hard to be exactly describe by text or image alone [8]. This recognition takes little time thus allowing the administrators to responds to the attacks very quickly.

'Containment' is an important characteristic of SH [5]. The user can group similar objects in the workspace and drill-down in one of the groups to see the details of that group. Similar IDS events can be grouped to allow a view of the high-level system status, yet drilling-down one of the groups will allow the user to have a more detailed view.

# 4. PROPOSED FRAMEWORK

Figure 1 is the system architecture that we are currently working on. To increase the flexibility, a tool dependent translation module will be developed to convert the commands to and outputs from the current tools. The main challenge in the system is how the detection events are presented to the user. This part of the work is still in progress. The goals of the system design are presented here.

## 4.1 User Modelling & Recommendation Agents

The SH interface must adapt to suit its users. This can be done by incorporating two main machine learning components: The Recommendation Agent will generate suggestions based on the user model developed by User Modelling (UM) Agent to help the user arrange the spatial cues of event objects and clusters of objects.

The UM Agent is to develop and manage user models. A user model is developed from training data that comes in the form of currently displayed events (as provided by the network monitoring system) and their spatial cues as manually established by the user.

## 4.2 SH Interface

Any realistic ML-based monitoring system will always incorrectly identify some of the dangerous and suspicious events, because of the changing nature of network traffic and the types of attacks that can occur. The goal of the SH Interface is lessen the impact of this deficiency by providing: (a) a UI that can tolerate false detections, and (b) a UI that enables users to see the 'big picture' of network activity.

The SH interface will be used to visualize the dynamic state of network traffic. Objects (network events) will be clustered by spatial cues. Safe, dangerous and suspicious events passed from the monitoring system will be displayed as per the the directions of the User Modeling Agent. For example, the User Model may direct the display of Trojan-like events to a particular area of the screen for the current user.

Because of the characteristics of our users and their tasks, the interface will need to be interactive: Users must be able to change any of the presentation features of the display to help interrogate the data, to see patterns, and to focus on particular aspects. We expect that some form of multi-focus fisheye or focus-in-context display will be appropriate [4].

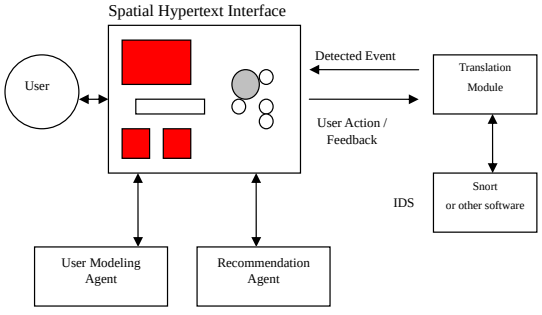


**Figure 1: The proposed system structure**

# 5. CONCLUSION & FUTURE WORK

Intrusion detection systems must handle masses of information (often in real-time) so as to report the abnormal use of networks and computer systems. SH has proven to be effective for dynamic information analysis tasks. Intrusion detection is an information intensive and deeply analytic process that cannot be undertaken without the assistance of a computer.

We hope that the impact of high false alarm rates can be significantly reduced by employing proper SH user interface. The users will be able to rapidly 'recognize' the potential threats from SH workspace. Hopefully, the users will be more willing to continuously monitor the IDS (because less effort is required to be aware of an attack) rather than checking the system after an attack. Our next steps are to: (a) perform more in-depth studies on how IDS users use the system , and (b) perform user studies on the completed system to see the effects of SH user interface.

# 6. REFERENCES


[1] K. Baker and S. Greenberg and C. Gutwin. A review and taxonomy of distortion-oriented presentation techniques. In *CSCW 2002*, pages 96–105, New York, NY, 2002. ACM Press.

[2] A. Dillon. Beyond usability: Process, outcome, and affect in human computer interactions. In *Canadian J. of Info. Sci.*, 26(4):57–69, Dec. 2001.

[3] C. Gates and T. Whalen. Profiling the defenders. In *New Security Paradigms Workshop*, 2004

[4] Y. K. Leung and M. D. Apperley. A review and taxonomy of distortion-oriented presentation techniques. *ACM TOCHI*, 1(2):126–160, 1994.

[5] C. C. Marshall and F. M. Shipman. Spatial hypertext: Designing for change. *CACM*, 38(8):88–97, 1995.

[6] C. C. Marshall, F. M. Shipman, and J. H. Coombs. VIKI: Spatial hypertext supporting emergent structure. In *ECHT*, pages 13–23. ACM Press, 1994.

[7] J. McGrenere, R. M. Baecker and K. S. Booth. An evaluation of a multiple interface design solution for bloated software In *Proc.SIGCHI*, 2002.

[8] F. M. Shipman and C. C. Marshall. Spatial hypertext: An alternative to navigational and semantic links. *ACM Comp. Surv.*, 31(4es), 1999.

[9] A. Whitten and J. D. Tygar. Why Johnny can't encrypt: A usability case study of PGP 5.0. In *Proc. USENIX Security*, 1999.

[10] A. T. Zhou, J. Blustein, and N. Zincir-Heywood. The state of network security management: Issues and directions. TR CS-2003-06, Dalhousie U., Faculty of Comp. Sci., May 2003.