VISUALIZATION TECHNIQUES FOR INTRUSION DETECTION – A SURVEY

Ibrahim Elhenawy[1], Alaa El - Din Riad [2],Ahmed Hassan[3] and Nancy Awadallah[2]

[1]Faculty of Computer Science and Information Systems Zagazig University, Egypt

henawy2000@yahoo.com

[2] Faculty of Computer Science and Information Systems, Mansoura University, Egypt

amriad2000@yahoo.com

rarecore2002@yahoo.com

[3]Faculty of Engineering – Mansoura University , Egypt

arwaahmed1@gmail.com

ABSTRACT

In traditional intrusion detection system (IDS) environments, little activity has been applied to using visual analysis as an aid to intrusion detection. With more information systems being attacked and attack techniques evolving, the task of detecting intrusions is becoming an increasingly difficult. Efficient information visualization is an important element required for urgent detection of intruders.
This paper presents a survey on using visualization techniques in intrusion detection system.
Finally authors proposed a framework for visualization system for ID.

KEYWORDS

Intrusion Detection Systems (IDS), Information Visualization (IV),Visualization Techniques .

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 [1]. Furthermore, previous surveys 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. Implementing better detection techniques can, in theory, have significant improvement in IDS performance [2].

However, previous studies 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 [3].

Visualization techniques allow people to see and comprehend large amounts of complex data [4]. Graphics are used to assist with the ID investigation and reporting process by helping the analyst identify significant incidents and reduce false conditions (positives, negatives and alarms). Visualization is then used in reporting incidents to a broader senior level audience. Complex patterns are clearly displayed over time in an easy to understand and compelling manner [4].

Currently, the research on network security visualization based on intrusion detection technique is mainly focused on alarm as its investigation object, in which alarms are statistically analyzed and their quantity and distribution are usually represented using 2D/3D charts.
This paper is organized as follows. Section 2 introduces the concept of intrusion detection systems (IDS) and its components. In section 3, previous studies are presented. Intrusion visualization, information visualization components, visualization system and techniques are provided in section 4. Finally, we proposed a system acts as a monitoring system which deals with viewer system and IDS.

2. INTRUSION DETECTION SYSTEMS (IDS)

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of security violations that do not adhere to security policy [5]. IDS has been broken up into three key components [6] as illustrated in figure 1

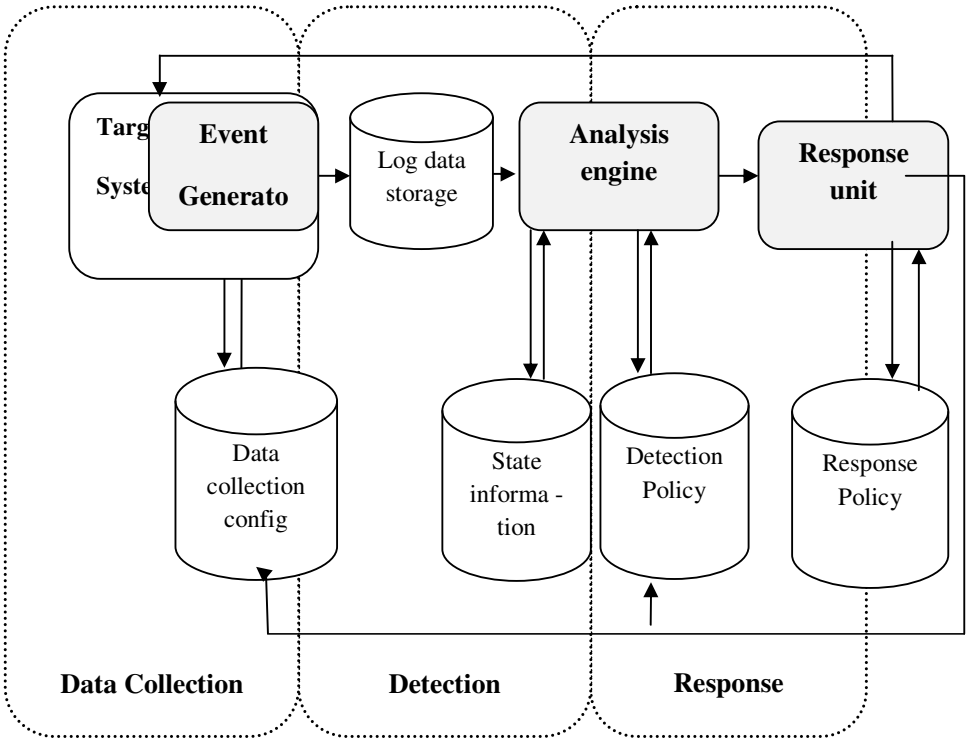

Figure 1. Components of IDS [5]

- **Information Sources:** The different sources of data that are used to determine the occurrence of an intrusion. The common sources are network, host and application monitoring.

- **Analysis:** This part deals with techniques that the system uses to detect an intrusion. The most common approaches are misuse detection and anomaly detection.

- **Response:** This implies the set of actions that the system takes after it has detected an intrusion. The set of actions can be grouped into active and passive actions. An active action involves an automated intervention whereas a passive action involves reporting IDS alerts to humans. The humans are in turn expected to take action. **[5][6]**

As with any solution to a problem, there must be goals to achieve while solving the problem. Intrusion detection is no different. The main goals of IDSs are **a**ccountability, **r**esponse.
Accountability is defined as the capability to map a given activity or event back to the responsible party. This is one of the more difficult tasks of IDS as attacks rarely come from the original host.
Response in intrusion detection is varied. It ranges from taking action against the attacker to just logging the intrusion into an audit log, although most SAs would want a more proactive response from their IDS **[6].**The proposed system in this paper will deal with detection component in IDS to achieve the accountability goal.

3. RELATED WORK

Goodall in [7] ,proposed a visualization tool to support network intrusion detection analysis tasks , based on understanding the work practices of human analysts to inform the design of a task-appropriate information. He evaluated his system using two ways, a field-based qualitative evaluation, uncommon in information visualization, and a lab-based benchmarking evaluation.

Abdullah et all [8], addressed network traffic visualization techniques that aid an administrator in recognizing attacks in real time. Their approach improves upon current techniques that lack effectiveness due to an overemphasis on flow, nodes, or assumed familiarity with the attack tool, causing either late reaction or missed detection.
Min et all [9] , presented the visualization of intrusion detection alerts with alert correlation. Each intrusion alert is represented as a dot of various colors according to the attack class. The location and time of an attack as are represented as graph's coordinates. The correlation of alerts is represented a line of different colors according to context analysis. This helps rapid intrusion analyses and traces many alerts. The proposed idea overcomes alert flooding and false positive alerts, and provides the context information of intrusions by intuition.

Khor et all [10], proposed a system for web application administrators to easily identify and quickly act upon intrusions in a three layered visualization related to a web application. Information on users of each layer can be viewed easily and detection of intrusion will allow administrators immediate engagement to secure a web application based on the visualization of the layer which is under attack.
Koike et all [11][25][26][27][28][29][30][31][32], proposed a visualization system of a NIDS log, named SnortView, which supports administrators in analyzing NIDS alerts much faster and much more easily. Instead of customizing the signature DB, they also propose to utilize visualization to recognize not only each alert but also false detections. The system is based on a 2-D time diagram and alerts are shown as icons with different styles and colors. In addition, the system introduces some visualization techniques such as overlayed statistical information, source destination matrix, and so on. The system was used to detect real attacks while recognizing some false detection. **[33]**
Erbacher in [12][34][36], propose a methodology for analyzing network and computer log information visually based on the analysis of user behavior. Each user's behavior is the key to determining their intent and overriding goals, whether they attempt to hide their actions or not.
He also discussed how user behavior can be exhibited within the visualization techniques, the capabilities provided by the environment, typical characteristics users should look out for, and exploration paradigms effective for identifying the meaning behind the user's behavior.
Oline et all [13], explored three-dimensional approaches to visualizing network intrusion detection system alerts and aggregated network statistics in order to provide the system administrator with a better picture of the events occurring on his or her network.
They showed how a number of attack types in the data set generate visual evidence of abnormal activity that a security administrator might use as motivation for further investigation.

Santos in [14], addressed some relevant issues that should be considered whenever trying to evaluate any visualization tool or technique, which are: motivation, evaluation methods, test data, collected data and data analysis.
Komlodi et all [15], studied ID analysts' daily activities in order to understand their routine work practices and the need for designing information visualization tools. They developed a three-phase process model that frames corresponding requirements for IV tools which are monitoring , analysis , response phases.
C´ardenas et all [16], presented the intrusion detection operating characteristic (IDOC) curves as a new IDS performance tradeoff which combines in an intuitive way the variables that are more relevant to the intrusion detection evaluation problem. They introduce formal framework for reasoning about the performance of an IDS and the proposed metrics against adaptive adversaries.

Peng et all [17][35], proposed a hybrid intrusion detection and visualization system that leverages the advantages of current signature-based and anomaly detection methods. The hybrid instruction detection system deploys these two methods in a two staged manner to identify both known and novel attacks. When intrusion is detected, autonomous agents that reside on the system will automatically take actions against misuse and abuse of computer system, thus protecting the system from internal and external attacks.

YongJoon et all [18], presented web application intrusion detection System (WAIDS), an intrusion detection method based on an anomaly intrusion detection model for detecting input validation attacks against web applications. Their approach is based on web application parameters which has identical structures and values. WAIDS derives a new intrusion detection method using generated profile from web request data in normal situation. By doing this, it is possible to reduce analysis time and false positives rate.

The previous studies discussed several issues such as, intrusion detection systems work, the evaluation of them , the integration between IDSs and visualization to help in intrusion detection **[16][17]**. Also it presented how to analyze intrusion in network domain. Researcher in **[10][18]** focus on using visualization in web application intrusion detection.
This paper proposed a system which deal with IDS and viewer system to visual intrusion in web applications .This proposed system is differ from previous studies as it could visually alerts and will be suitable for visual alerts based on attacks that emit little traffic.

4. INTRUSION VISUALIZATION

Visualization for intrusion detection helps a security administrator to recognize abnormal behavior in an intuitional manner. Visualization of intrusion detection enables fast analysis and response because an intrusion is recognized intuitionally. So, it can overcome alert flooding. Most intrusion detection methods with visualization are anomaly-based detection methods and visualize audit data rather than the alert itself. **[19] .**The host-based visualization method for intrusion detection is to learn normal states of commends or programs that is achieved by the user and compares audit data with profiles for visualization.

Network-based visualization method for intrusion detection expresses the source address, destination address and port number and so forth of the network's packets by visual graph. **[19][20].**So, they detect an intrusion when an attack differs from graph characteristic with normal state, and extract diagnostic features of attack for embodying anomaly detection. However, these methods do not visualize alerts themselves, but visualize audit data. Therefore, these are useful for detecting attacks that emit much traffic such as distributed denial-of-service attack (DDoS) or worm **[8]**. These do not offer clear characteristics for attacks that emit little traffic. **[21]**

4.1. Information Visualization Components

Generally information visualization components are done through some phases as follows:

Phase 1: Monitoring

Phase 1 characteristics are *Simple displays*, *Overview displays*, *Flexibility*

- ***Simple displays***

Researchers preferred simple, 2D displays for this phase, as these allow for continuous monitoring without the need for focused attention, building on pre-attentive visual processing (the fast, parallel recognition of color, shape, and movement by humans). Visualization support for this phase must provide a starting point for recognizing and flagging events that require further analysis in a way that can be done quickly and effectively without requiring the analysts' full attention **[15]**.

- ***Overview displays: Data and visualization attributes***

Displaying an overview of the current activity is essential. As one participant told us "people want the big picture." Graphical overviews can serve this purpose well. All participants were asked to select the most important data attributes to include in the visualization displays.
These attributes are well suited to provide an overview for the monitoring phase. The rest of the attributes (not bolded) must be provided in a drill-down detail view to support later analysis **[15]**.

- ***Flexibility***

The need for end-user customizability with the IV displays was an important finding for both the monitoring and analysis phases. As described above, ID requires a deep understanding of idiosyncratic local networks. Analysts have had to configure IDS's in order to identify attacks on their unique network. This flexibility must be reflected in the visualization displays. Participants were very much in favor of the ability to set up their own visualization display settings and they did not object to the added effort, but voiced the need for saving these settings and being able to reuse them later **[15]** .

Phase 2: Analysis and Diagnosis

Phase 2 characteristics are *filtering and interaction*, *exploration*, *multiple data sources and correlation*, *multiple views and levels of data*

- ***Filtering and interaction***

While monitoring tools should require as little user interaction as possible, supporting analysis is a much more interactive activity. Due to the large size of the data sets, filtering is a very important function for IV tools for ID as a transitional mechanism from monitoring to analysis.
Multiple discrete ranges need to be selected, and predefined, and user-defined clusters should be able to be saved and reused in more complex displays. In addition, filtering data should provide a means for highlighting data without necessarily removing it from the display, as the data that is not the focus of the task is still important in providing vital contextual information for correctly diagnosing the alert **[15][22]** .

- ***Exploration***

The analysis and diagnosis task requires support for user exploration that warrants markedly different IV displays than those used in monitoring. The need for simplistic displays for quickly identifying an alert in monitoring is replaced by a need for more powerful visualizations that are linked and can represent multidimensional data from multiple sources **[15]**.

- ***Multiple data sources and correlation***

The analysis and diagnosis of an alert cannot be accomplished without also taking into account secondary data sources that supplement the information contained in the alert itself.
A visualization tool must effectively fuse these disparate data sources together seamlessly in a single display, that can correlate all of the data together. An example of this is host information that determines if the target of an attack is vulnerable to the attack described in the alert. The breadth of the data sources will depend on the organization, but will include both dynamically collected and static network-level and host-level data **[15]**

- ***Multiple views and levels of data***

In this phase, the ability to have multiple views of the same or related data becomes important. Analysts would like to utilize multiple displays at the same time, such as multiple displays each running the visualization tool on the same data, but with different data attributes or different time spans displayed. Another important need is to display several levels of data (i.e., network sessions, raw packets, host information), and allow users to drill down or zoom in on certain data items. **[15]**

Phase 3: Response

The support necessary for responding to attacks extends IV displays beyond data manipulation and viewing. The ability to save views, keep histories of exploration and activity, and annotating alerts will all help analysts document and report incidents. These functions are often missing from IV tools, although they allow users to make the transition from exploring and finding information to using and reusing this information in their work. Suggesting possible responses for different types of attacks could greatly aid the speed and efficiency of responding to attacks; these suggestions could come from annotations of previously diagnosed similar attacks or from IDS developers. **[15][22]** .

4.2. Visualization Systems

Two graphical applications have been developed for evaluation

- Intrusion Detection Analyst Workbench **[4]**
- Animated Incident Explanation Engine **[4]**

Both display data visually, but currently have two distinct audiences.

- **Intrusion Detection Analysts Workbench**. As shown in figure 2, up to 2,000,000 event records or more can be displayed and analyzed in multiple concurrent dynamic charts. Each event record includes fields such as source and destination IP, port ID, alarm code, date, time. The charts are saleable so that, for example, a bar chart showing number of events by destination IPs can easily display ten's of thousands of IP addresses. The charts are also linked. Selecting events in one chart will highlight those events in all the other charts. So for example, selecting events associated with one type of alarm will cross reference those events in the source IP bar chart, and the destination IP bar chart.
The analyst workbench is used to investigate, isolate and prioritize events. It was evaluated in a side-by-side test with existing methods and proved to be a significantly faster method. **[4]**

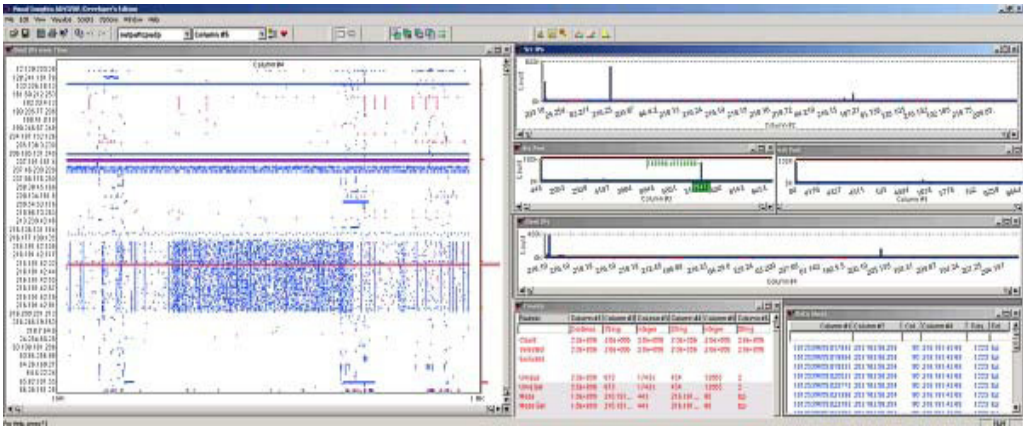

Figure 2. Intrusion Detection Workbench with 2M TCP and UDP Records [4]

- **Animated Incident Reporting component**. As shown in figure 3, it is used to report intrusion activity to senior management, and is designed to show the significance and nature of the events without overwhelming the viewer. The objective is to clearly see who did what to whom and when. A number of interactions are supported including filtering and an adjustable playback speed. This component was evaluated in a series of presentations to senior levels of government and industry. **[4]**

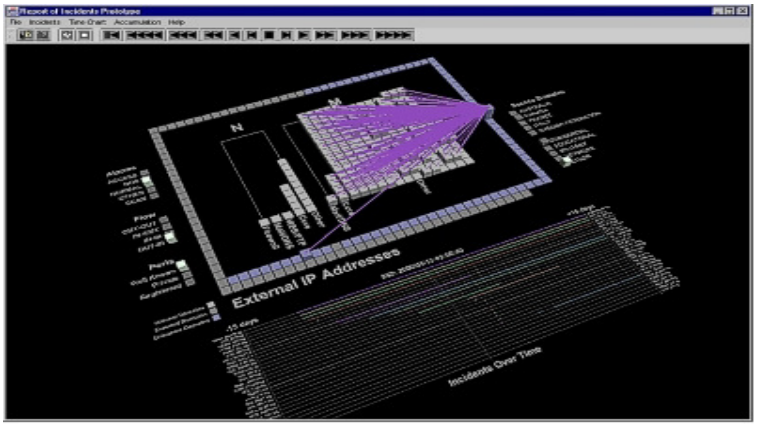

Figure 3. Animated Incident Reporting [4]

4.3. Visualization Techniques

Ed H. Chi, present a detailed analysis of a large number of visualization techniques by using the Data State Model, he also showed that the Data State Model not only helps researchers understand the space of design, but also helps implementers understand how information visualization techniques can be applied more broadly.

Data State Model breaks down each technique into four Data Stages, three types of data transformation and four types of Within Stage operators, so each technique has broken down by not only its data type, but also by its processing operating steps. **[23]**

Table 1. Data Stages in the Data State Model [23]

Stage	Description
Value	The raw data.
Analytical Abstraction	Data about data, or information, meta-data .
Visualization Abstraction	Information that is visualizable on the screen using a visualization technique.
View	The end-product of the visualization mapping, where the user sees and interprets the picture presented to her.[24]

Table 2. Transformation Operators [23]

Processing Step	Description
Data Transformation	Generates some form of analytical abstraction from the value (usually by extraction).
Visualization Transformation	Takes an analytical abstraction and further reduces it into some form of visualization abstraction, which is visualizable content.
Visual Mapping Transformation	Takes information that is in a visualizable format and presents a graphical view. [24]

Table 3 illustrated visualization techniques which be used on web field, a row represents a single visualization technique or system. The cells in that row describe the operators that comprise that technique.

Table 3. Taxonomy using the Data State Model [23]

Web Visualization							
Visualization Technique	**Within Value**	**Data Transformation**	**Within Analytical Abstraction**	**Visualization Transformation**	**Within Visualization Abstraction**	**Visual Mapping Transformation**	**Within View**
WebSpace	*Data: web site*	walk web site and create web linkage graph	value-filtering	Create breadth first traversal tree	*Visualization Abstraction: Tree*	Layout using cone tree	Dynamic view-filtering
3D Hyperbolic	*Data: web site*	walk web site and create web linkage graph	value-filtering	Create breadth first traversal tree	*Visualization Abstraction: Tree*	Layout using 3D Hyperbolic Tree	Dynamic view-filtering
WebMap	*Data: web site traversal history*	Extract user path from traversal history graph	*Abstraction: traversal history graph*	Form navigation **spanning** trees.	*Visualization Abstraction: Tree*	Map to Tree layout, circle layout, rectangle layout, Horizon tree layout	Dynamic view-filtering

Time Tube	*Data: web structure evolving over time and its associated usage statistics (Content, Usage, and Topology of the web site)*	Create graph from web structure by crawling the web site	*Analytical Abstraction: Evolving graph represented as ordered collection of graph*	Do breadth first traversal with global node position over time	*Visualization Abstraction: Evolving tree as ordered list of trees*	Create Time Tube, which is represented using an aggregation of Disk Trees (invisible tube--like shelf)	Recognize gestures for: Focus on a slice; Bring slices back into the Time Tube; Zooming focus on the connectivity of a node by right-clicking on it; Rotate slices; Brushing on pages by highlight URL on all slices; Animate through the slices

it will be useful to focus on this technique as it belong to web visualization field , as the proposed system which presented in this paper concern in visually detect intrusion on web application .

5. PROPOSED SYSTEM

Authors in this paper proposed a system acts as a monitoring system which deals with viewer system and IDS. Whatever Viewer System would be built in server or client site it will be useful for decision maker such as server administrator.
Our proposed system will deals with detection component in IDS as we presented in section **2** about intrusion detection system components. IDS domain will be server side.
The aim of this system is to visually detect any intrusion or attacks which took place on web application.

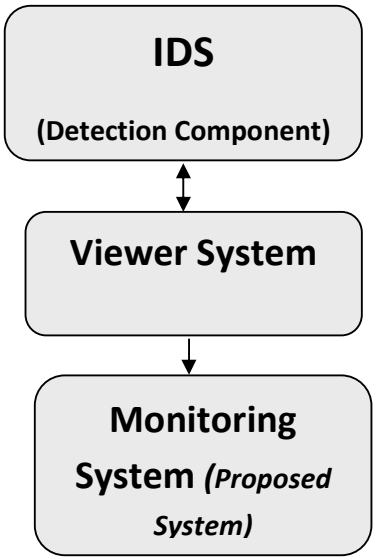

Figure 4. Proposed System

6. CONCLUSION AND FUTURE WORK

The problem of evaluating visualization tools and techniques has long intrigued researchers, which strongly believes it is absolutely fundamental to develop effective and systematic methods to tackle this defying problem in order to allow information visualization to fulfill its promise and serve a wide community of users in diverse areas. Moreover, this problem urgently needs attention by the visualization community, and all the efforts toward tackling it are valid, even if they are at first too native and unsophisticated.
Web applications are popular attack targets due to time and financial constraints, limited programming skills, and lack of security awareness on part of the developers. Therefore, in the Future work we will presents how to use visualization techniques to detect intrusion in web application.

ACKNOWLEDGEMENTS

The authors would like to thank all the people and institutions that have allowed them to use many of the figures present in this paper.

REFERENCES

[1] A. Fuchsberger, (2005) "Intrusion Detection Systems and Intrusion Prevention Systems " , ELSEVIER , Information Security Technical Report, . Vol.10 , Issue 3 .

[2] J. Blustein, Ching-Lung Fu , D.L.Silver, (2005) "Information Visualization for an Intrusion Detection System" , ACM located on http://www.coursehero.com/file/4078999/a11f016220low/ , http://www.pdfgeni.com/book/detection-systems-pdf.html , http://web2.uwindsor.ca/courses/cs/aggarwal/cs60564/projects/SnortSnarf.doc , http://www.mypptsearch.com/search-ppt/intrusion+detection+system+ppt/ , http://www.pdfgeni.com/book/Internet-Systems-pdf.html , http://www.docstoc.com/docs/2725596/IDS,

http://www.cs.utexas.edu/users/ygz/395T-01F/reading/arun.ppt
http://www.inguardians.com/research/docs/switched.pdf ,
http://tmdnet.nothave.com/mirror/www.docshow.net/ids.htm ,
http://www.scribd.com/doc/45944625/Intrusion-Detection-Systems

[3] A. Wood , (2003) "Intrusion Detection: Visualizing Attacks in IDS Data" , SANS Institute .

[4] W.Wright & P.Clarke , (2002) "Visualization Techniques for Intrusion Detection",RTO-MP-105 Workshop , located on http://handle.dtic.mil/100.2/ADA428197 ,
http://www.stormingmedia.us/authors/Wright_William.html ,
http://www.stormingmedia.us/keywords/INFORMATION_SYSTEMS-10.html

[5] E.Lundin & E. Jonsson , (2004) " Survey of Intrusion Detection Research " , Chalmers university of technology, Technical Report , located on
http://www.mvwsd.org/index.php?option=com_content&task=view&id=237&Itemid=668 ,
http://www.opi.mt.gov/pdf/FEDPrgms/pmm/09Private_NonPub.pdf ,
http://www.cde.ca.gov/sp/ps/cd/nclbequitprov.asp ,
http://www.opi.mt.gov/PDF/FEDPrgms/gh/appendices/appendixb/B8OpportParticFed%20.pdf

[6] R. Booysen ,Werner Olivier & R. v. Solms ," IVIDS - The Integration of Information Visualization and ntrusion detection Systems ",2003 , located on
http://www.esc6.net/info/content/documents/294/Application.pdf ,
http://www.pgusd.org:8080/FMPro?-DB=boardpol.fp5&-format=policydisplay.html&-RecID=33075&-Find
http://www.eduhsd.k12.ca.us/ROP/District%20Policies/6171-ar.htm ,
http://www.scribd.com/doc/44466877/Comp-of-Clustering-Method
http://www.michigan.gov/documents/mde/2TitleIPartA_242871_7.pdf
http://www.mde.k12.ms.us/innovative%5Fsupport1/presentations/MAFEPD_Consultation.ppt
http://maverick.tea.state.tx.us:8080/Guidelines/NCLB/NCLBAA11/NCLB_Sample_Application.pdf

[7] J. R. Goodall , (2006) "Visualizing Network Traffic for Intrusion Detection" , ACM , located on
http://portal.acm.org/citation.cfm?id=1142405.1142440 ,
http://portal.acm.org/citation.cfm?doid=1142405.1142439 ,
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.74.3922 ,
http://portal.acm.org/citation.cfm?id=1142414 ,
http://academic.research.microsoft.com/Paper/2196088 ,
http://doi.acm.org/10.1145/1142405.1142415 ,
http://portal.acm.org/citation.cfm?id=1142433 ,
http://portal.acm.org/citation.cfm?id=1142405.1142417,
http://portal.acm.org/citation.cfm?id=1142405.1142443

[8] K. Abdullah, C. Lee, G.Conti & J. A. Copeland ,(2002)" Visualizing Network Data for Intrusion Detection " ,IEEE , located on
http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1495940&isnumber=32124 ,
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.106.5388

[9] B. Min, J. Kim & S. HongIn ,(2004) " Visualization of Intrusion Detection Alerts with Alert Correlation " ,Pohang University of Science and Technology, Korea.

[10] K.Khor, S.K.Lieong & E. Ch'ng , (2005) "Efficient Information Visualization for Intrusion Detection in Web Applications", International Conference on Computer Graphics, Imaging and Vision, Beijing, China , located on
http://pesona.mmu.edu.my/~kckhor/document/kc_khor_cgiv05.pdf ,
http://www.nmmu.ac.za/rbotha/Research/Projects/InfoSec/Booysen.pdf ,
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.100.7655 ,

http://pipl.com/directory/name/Chin/Kok

[11] http://portal.acm.org/citation.cfm?id=1029208.1029230 , H.Koike & K.Ohno , (2004) "SnortView: Visualization System of Snort Logs" , ACM , located on http://doi.acm.org/10.1145/1029208.1029223

[12] R. F. Erbacher , (2003) "Intrusion Behavior Detection Through Visualization" , IEEE , located on http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1244260&isnumber=27877 http://www.citeulike.org/user/cmalek/tag/glyphs , http://www.citeulike.org/group/2518/author/Erbacher , http://www.citeulike.org/group/2518/tag/glyphs, http://www.citeulike.org/group/1990/tag/interaction, http://www.citeulike.org/user/cmalek/tag/event , http://www.citeulike.org/user/cmalek/tag/intrusion, http://academic.research.microsoft.com/Paper/71142 , http://www.citeulike.org/group/2518/tag/visualization

[13] A.Oline , D. Reiners , (2005)"Exploring Three-dimensional Visualization for Intrusion Detection" , IEEE , located on http://www.computer.org/portal/web/csdl/doi/10.1109/INFVIS.2000.885092 http://www.computer.org/portal/web/csdl/doi/10.1109/VIZSEC.2005.6 http://portal.acm.org/citation.cfm?id=1106734 http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1532073&isnumber=32678 http://www.citeulike.org/user/jgoodall/article/2305168 http://portal.acm.org/citation.cfm?id=1106610.1106733

[14] B. S. Santos, (2005) "Evaluating Visualization techniques and tools: what are the main issues? ",position paper , located on http://www.dis.uniroma1.it/~beliv08/pospap/santos.pdf

[15] A. Komlodi, J. R. Goodall & W. G. Lutters , (2004) "An Information Visualization Framework for Intrusion Detection" , ACM , located on http://vizsec.org/johng/ , http://academic.research.microsoft.com/Paper/1237397 , http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.1.9560, http://www.pcauthority.com.au/Review/16642,adobe-indesign.aspx , http://www.svgopen.org/2004/papers/SPARK/ , http://www.academicjournals.org/AJMCSR/PDF/Pdf2009/Nov/Yusuf%20%20et%20al.pdf , http://www.academicjournals.org/AJMCSR/abstracts/abstracts/Abstract2009/Nov/Yusuf%20et%20al.htm , http://www.designer-info.com/Writing/adobe_indesign_1.htm

[16] A.C´ardenas , J. Baras & K.Seamon , (2006)"A Framework for the Evaluation of Intrusion Detection Systems " , IEEE , located on http://www.computer.org/portal/web/csdl/doi/10.1109/SP.2006.2 , http://www.isr.umd.edu/~baras/publications/papers/2006/CardenasBS_2006.htm , http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1624001&isnumber=34091 , http://portal.acm.org/citation.cfm?id=1130366 , http://portal.acm.org/citation.cfm?id=1130373 , http://portal.acm.org/citation.cfm?id=1130381 , http://portal.acm.org/citation.cfm?id=1130235.1130364 , http://portal.acm.org/citation.cfm?id=1130389 , http://portal.acm.org/citation.cfm?id=1130383 , http://portal.acm.org/citation.cfm?id=1130391 , http://news.ycombinator.com/item?id=2148161 , http://www.softpanorama.org/Articles/orthodox_editors.shtml

[17] J. Peng, C. Feng, J.W. Rozenblit, (2006) "A Hybrid Intrusion Detection and Visualization System", IEEE , located on http://portal.acm.org/citation.cfm?id=1126213 , http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1607413&isnumber=33752, http://ijsdia.org/main/wp-content/uploads/2009/08/71.pdf

[18] Y.J. Park & J. Park,(2008) "Web Application Intrusion Detection System for Input Validation Attack", IEEE , located on : http://portal.acm.org/citation.cfm?id=1472086

[19] H .Hiraishi. & Mizoguchi. F, (2001) "Design of a Visual Browser for Network Intrusion Detection" ,Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE).

[20] R. Becker, S. Eick, & A. Wilks,(1995) "Visualizing Network Data" In IEEE Transactions on Visualization and Computer Graphics, Vol 1, no. 1.

[21] J. Xin, J. E. Dickerson, & J. A. Dickerson, (2003) "Fuzzy Feature Extraction and Visualization for Intrusion Detection ", The IEEE International Conference on Fuzzy Systems, located on http://www.h3c.com/portal/Products___Solutions/Products/Other_Products/Routers/Quidway_AR18-3X_Series_Routers/White_Paper/200701/194247_57_0.htm , http://www.scribd.com/doc/40634124/5500G-ConfGuide

[22] S.Bassi1 & R.K. Keller, (2001) "Software Visualization Tools: Survey and Analysis", IEEE.

[23] http://www-users.cs.umn.edu/~echi/papers/infovis00/Chi-TaxonomyVisualization.pdf
Ed H. Chi , (1999) "A Taxonomy of Visualization Techniques using the Data State Reference Model" , located on http://www.coursehero.com/file/1545327/Chi-TaxonomyVisualization/ , http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=885092 , http://en.wikipedia.org/wiki/Information_visualization_reference_model , http://portal.acm.org/citation.cfm?id=857699 , http://www.citeulike.org/user/suze/article/108977 , http://portal.acm.org/citation.cfm?id=857691 , http://portal.acm.org/citation.cfm?id=857679 , http://portal.acm.org/citation.cfm?id=857687 , http://portal.acm.org/citation.cfm?id=857190.857700, http://portal.acm.org/citation.cfm?id=857190.857683

[24] http://www-users.cs.umn.edu/~echi/papers/2002-03-duality-avi-final.pdf

[25] http://portal.acm.org/citation.cfm?id=1029231

[26] http://portal.acm.org/citation.cfm?id=1029208.1029229

[27] http://portal.acm.org/citation.cfm?id=1029208.1029224

[28] http://portal.acm.org/citation.cfm?id=1029210

[29] http://portal.acm.org/citation.cfm?id=1029208.1029225

[30] http://portal.acm.org/citation.cfm?id=1029208&picked=prox

[31] http://portal.acm.org/citation.cfm?id=1029208.1029220

[32] http://portal.acm.org/citation.cfm?id=1029208.1029217

[33] http://portal.acm.org/citation.cfm?id=1029211

[34] http://www.citeulike.org/group/2518/article/678516
http://www.citeulike.org/user/cmalek/article/678516
http://www.citeulike.org/group/1990/article/678516

[35] http://www.computer.org/portal/web/csdl/doi/10.1109/ECBS.2006.8
http://doi.ieeecomputersociety.org/10.1109/ECBS.2006.8

[36] http://www.citeulike.org/tag/glyphs