Data Visualization Technique Framework for Intrusion detection

Alaa El - Din Riad [1] , Ibrahim Elhenawy[2], Ahmed Hassan[3] and Nancy Awadallah[4]

[1]Head of Information Systems Dep, Faculty of Computer Science and Information Systems, Mansoura University, Egypt
Mansoura,,DK, 35513, Egypt

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

[3]Faculty of Engineering , Mansoura University , Egypt
Mansoura,,DK, 35513, Egypt

[4]Faculty of Computer Science and Information Systems, Mansoura University, Egypt
Mansoura,,DK, 35513, Egypt

Abstract

Network attacks have become the fundamental threat to today's largely interconnected computer system. Intrusion detection system (IDS) is indispensable to defend the system in the face of increasing vulnerabilities.
While a number of information visualization software frameworks exist, creating new visualizations, especially those that involve novel visualization metaphors, interaction techniques, data analysis strategies, and specialized rendering algorithms, is still often a difficult process. To facilitate the creation of novel visualizations this paper presents a new framework that is designed with using data visualization technique for analysis and visualizes snort result data for user. The framework suggests PHP and CSS as data visualization technique and snort as intrusion detection system (IDS).

Keywords: *Intrusion Detection System, Visualization techniques, Snort, PHP and CSS.*

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 networks [1].

2. Related Research

J. Blustein, C. Fu and D. L. Silver presents 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 [1].

Network security visualization is a new research field as a result of introducing information visualization into network security area. Taking advantage of the ability of human vision perception to model structure, this technique turns abstract network and system data into graphical displays to help analysts explore network status and identify network anomalies or intrusion and even forecast the trend of security events [2].

Using data visualization technique to support the result of snort (IDS) , we consider that PHP and CSS as data visualization technique , we will deal with data of snort database to detect which data will be useful for network administrator to be visualized .

The framework introduced here is powerful because it is general, it can be applied to a wide domain of visualization problems. This research will assist users of visualization to explore, communicate, and understand their results.
The organization of this paper: next section discusses related research, section 3 presents proposed framework by using data visualization techniques for intrusion detection.

R.F.Erbacher discuss how user behavior can be exhibited within the visualization techniques, the capabilities provided by the environment, typical characteristics users should look out for (i.e., how unusual behavior exhibits itself), and exploration paradigms effective for identifying the meaning behind the user's behavior [3] .

H.Koike and K.Ohno propose 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 propose to utilize visualization to recognize not only each alert but also false detections [4].

N.Rangaraju and M.Terk describe a framework that is designed to simplify the process of building immersive visualization of structural analysis of building structures. They describe the components of the framework and describe two applications that were created to test their functionality [5].

J.Peng, C.Feng and J.W.Rozenblit propose 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 [6].

Y.Park and J.Park presents 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 [7].

R.U. Rehman consider snort as an open source packet sniffer and logger that can be used as a lightweight Intrusion Detection System (IDS) to detect a variety of attacks and probes such as buffer overflows, stealth port scans, CGI attacks, and more. The Basic Analysis and Security Engine (BASE) displays and reports intrusions and attacks logged in the Snort database in a web browser for convenient analysis [8].

A.Komlodi, J. R. Goodall and W.G. Lutters report a framework for designing information visualization (IV) tools for monitoring and analysis activities.They studied ID analysts' daily activities in order to understand their routine work practices and the need for designing IV tools [9].

K.Abdullah presents new techniques to aid in network security using information visualization. Research contributions have been made in network data scaling and processing, port activity visualization, useful visualization showing a larger amount of information than textual methods, scaling port numbers and IP address for maximum use of screen space without occlusion, performing and using user study results to design an IDS alarm visualization tool [10].

From previous studies we present our framework which be overcome on the problem of how to describe intrusion detection system results for network administrator.

3. Proposed Framework

This research aims to design a system for visualize intrusion detection by using PHP & CSS as data visualization technique .The system introduces four components which are described in detail on next sections .

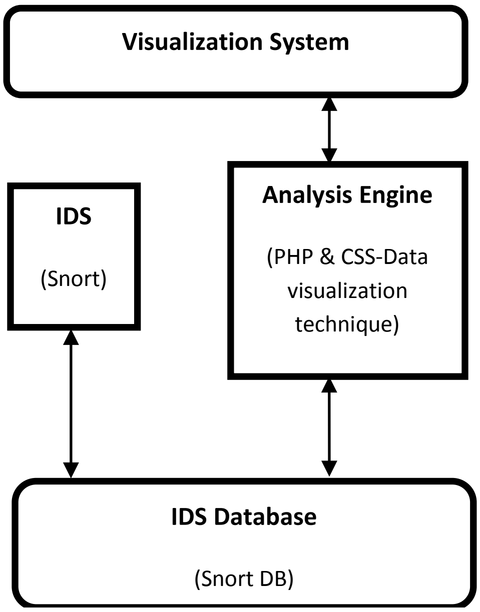


Fig. 1: Proposed System Structure

3.1 Snort Component

Snort is logically divided into multiple components. These components work together to detect particular attacks and to generate output in a required format from the detection system. A Snort-based IDS consists of the following major components:

- Packet Decoder
- Preprocessors
- Detection Engine
- Logging and Alerting System
- Output Modules [8]

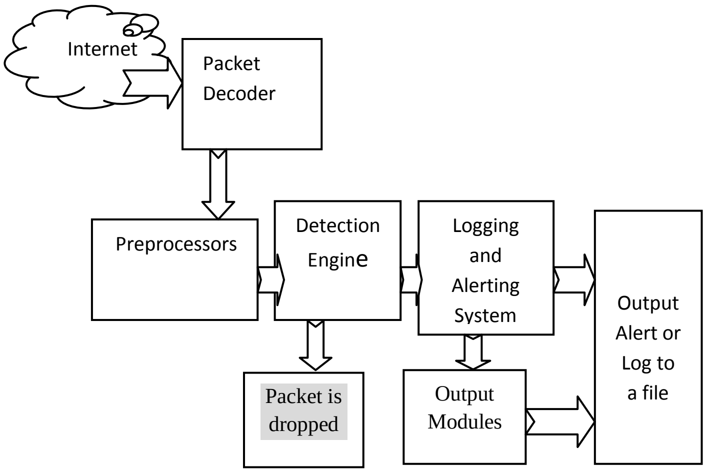


Fig. 2: Components of Snort [8]

Fig. 2 shows how these components are arranged. Any data packet coming from the Internet enters the packet decoder. On its way towards the output modules, it is either dropped, logged or an alert is generated. [9]

3.2 IDS (Snort) Database

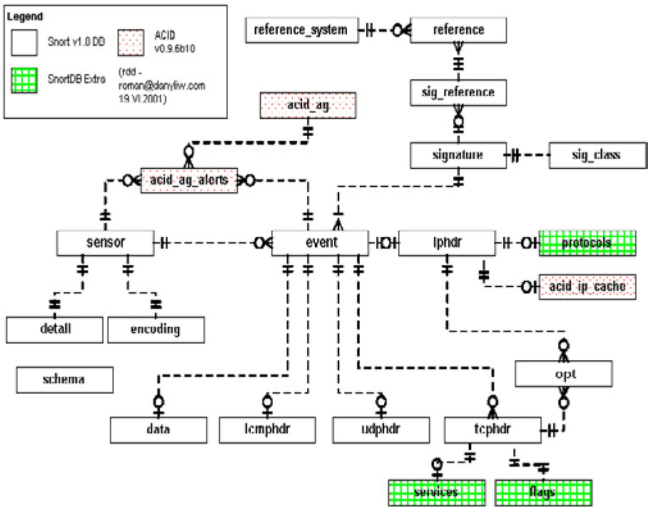


Fig. 3: Snort database schema [11]

The next table illustrates each table of Snort database from which component related to (Snort or ACID) and its description.

Table 1: snort tables [11]

Table	Component	Description
schema	Snort	Self-documented information about the database
sensor	Snort	Sensor name
event	Snort	Meta-data about the detected alert
signature	Snort	Normalized listing of alert/signature names, priorities, and revision IDs
sig_reference	Snort	Reference information for a signature
reference	Snort	Reference IDs for a signature
reference_system	Snort	(lookup table) Reference system list
sig_class	Snort	Normalized listing of alert/signature classifications
data	Snort	Contents of packet payload
iphdr	Snort	IP protocol fields
tcphdr	Snort	TCP protocol fields
udphdr	Snort	UDP protocol fields
icmphdr	Snort	ICMP protocol fields

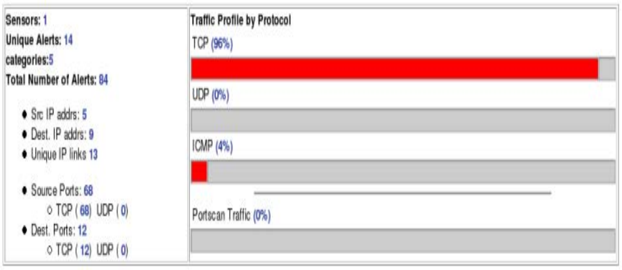
opt	Snort	IP and TCP options
detail	Snort	(lookup table) Level of detail with which a sensor is logging
encoding	Snort	(lookup table) Type of encoding used for the packet payload
protocols	SnortDB extra	(lookup table) Layer-4 (IP encoded) protocol list
services	SnortDB extra	(lookup table) TCP and UDP service list
flags	SnortDB extra	(lookup table) TCP flag list
acid_ag	ACID	Meta-data for alert groups
acid_ag_alert	ACID	Alerts in each alert group
acid_ip_cache	ACID	Cached DNS and who is information

3.3 Analysis Engine

This component responsible for retrieving data from snort database which be detected from snort (IDS) to be analyzed and processed it by CSS & PHP.

3.4 Visualization System

This component will be user interface for snort intrusion detection system result implemented by CSS & PHP (Data Visualization Technique).



Sensors: 1
Unique Alerts: 14
categories:5
Total Number of Alerts: 84

- Src IP addrs: 5
- Dest. IP addrs: 9
- Unique IP links 13

- Source Ports: 68
  - TCP (68) UDP (0)
- Dest. Ports: 12
  - TCP (12) UDP (0)

Traffic Profile by Protocol
TCP (96%)
UDP (0%)
ICMP (4%)
Portscan Traffic (0%)

Fig. 4: Visualization System

4. Conclusion and Future Work

Intrusion detection is an information intensive and deeply analytic process that cannot be undertaken without the assistance of a computer.
Intrusion detection systems must handle masses of information (often in real-time) so as to report the abnormal use of networks and computer systems.
Our proposed system has proven to be effective for visually the intrusion which be detected by snort system.
In the future work we will use JQUERY as data visualization technique to visually intrusion detection and comparing between using it, CSS & PHP technique.

References

[1] J.Blustein , C.Fu , D.L.Silver ," Information Visualization for an Intrusion Detection System",ACM , 2005.
[2] Nurbol, H. Xu, H.Yang, F.Meng, L. Hu,"A real-time intrusion detection security visualization framework based on planner-scheduler",IEEE ,2009 .
[3] R.F.Erbacher," Intrusion Behavior Detection Through Visualization", IEEE , 2003 .
[4] H.Koike and K.Ohno ,"SnortView: Visualization System of Snort Logs" IEEE , 2004 .
[5] N.Rangaraju and M.Terk ," Framework for Immersive Visualization of Building Analysis Data " , IEEE , 2001 .
[6] J.Peng, C.Feng and J.W.Rozenblit,"A Hybrid Intrusion Detection and Visualization System", IEEE , 2006 .
[7] Y.Park and J.Park ," Web Application Intrusion Detection System for Input alidation Attack" , IEEE , 2008 .
[8] R.U. Rehman " Intrusion Detection Systems with Snort Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID" , Publishing as Prentice Hall PTR Upper Saddle River, New Jersey, 2003.
[9] A.Komlodi, J.R. Goodall, W. G. Lutters , "An Information Visualization Framework for Intrusion Detection , 2004 , IEEE
[10] K.Abdullah , " Scaling and Visualizing Network Data to Facilitate in Intrusion Detection Tasks " ,Phd., School of Electrical and Computer Engineering ,Georgia Institute of Technology ,May 2006 .
[11] http://www.andrew.cmu.edu/user/rdanyliw/snort/acid_db_er_v102.html - last visit 22/07/2011

Authors

Alaa El - Din Riad, Head of Information Systems Department, Faculty of Computer and Information SciencesMansoura University

Ibrahim Elhenawy , Faculty of Computer and Information Sciences, Zagazig University

Ahmed Hassan ,Department of Electrical Engineering ,Faculty of Engineering , Mansoura University

Nancy Awadallah Researcher Assistant , Master in E-commerce Security 2008 , Faculty of computer science & Information System - Mansoura University - Egypt