NETWORK EARLY WARNING SYSTEM (NEWS)

**Samuel E. Moore, Robert G. Walters, Kimberley Frawley Braun,
Andrew M. Perron, William D. Cornish**

CSE IT Security Symposium June 22, 2000

Electronic Warfare Associates-Canada, Ltd.
275 Slater Street, Suite 1600
Ottawa, Ontario
K1P 5H9

Abstract

The security aspects of network system administration are currently largely based on the use of isolated tools, such as Firewalls and Intrusion Detection (ID) systems, each providing only a partial picture of the security state of a system. The system administrator must examine the outputs of these tools and assess their validity, in relation to the system policy, the current system state, and the outputs of other system tools, in order to determine whether or not the system is under attack. If an attack is in progress, it may then be necessary to examine system logs or use real-time analysis tools to determine the extent of damage to the system. NEWS is a tool that is being developed to assist the administrator in this examination by providing an integrated view of network security posture. It will amalgamate data from a variety of sensors and allow a decision-maker to see a highly visual display of the network links, nodes and traffic, including coordinated attacks on multiple nodes.

INTRODUCTION

The security aspects of network system administration are currently largely based on the use of isolated tools, such as Firewalls and Intrusion Detection (ID) systems, that each provide only a partial picture of the security state of a system. The system administrator must examine the outputs of these tools and assess their validity, in relation to the system policy, the current system state, and the outputs of other system tools, in order to determine whether or not the system is under attack. If it is determined that an attack is in progress, it may then be necessary to examine full or partial system logs or use real-time analysis tools, such as 'banner' or 'pinger' tools to determine the extent of damage to the system. It may also be necessary to consult reference tools, such as threat and vulnerability databases, to determine the vulnerability of the system to specific attacks or to obtain information about countermeasures.

Imperfections in existing tools compound the problem:

- Current intrusion detection systems, both host- and network-based, provide a poor assessment as to whether a 'real' attack is underway since they may either miss events or produce false alarms.
- Both intrusion detection systems and firewalls generate a lot of logged data, of which only a small part is relevant to the event. No satisfactory mechanism currently exists for extracting the relevant data from the background 'noise' data.
- Vulnerability analysis tools generate a lot of "system-specific" vulnerability information, much of which may easily be shown to be irrelevant to the system under test, e.g., Unix vulnerabilities on an NT system.

This paper presents the results of a study undertaken to define, build and demonstrate a proof-of-concept Network Early Warning System (NEWS). NEWS is a tool that will provide an integrated view of network security posture. Once completed, it will serve as an efficient network security monitoring tool for system administrators, a general-purpose network and data analysis tool for incident response, a testbed for network security research, development and training, and a profiling tool for network security analysis. It is intended to provide users the ability to tailor its installation to accept information from the security products installed on their network.

The Proof-of-Concept phase comprises the integration of two firewalls and two intrusion detection systems with a data visualization capability. Because the final configuration is not fully defined, the development has been planned as an evolutionary process with a number of cycles. The first cycle included the production of the requirements and system design specifications as well as the installation of network hardware and software modules to support the development. The current cycle completed the proof-of-concept interface of an intrusion detection system (Shadow and selected real-time tools) and the data visualization station.

SYSTEM DESIGN

Development Approach

The goal of NEWS is to integrate the data from various intrusion detection (ID) systems, firewalls, a threat and vulnerability (T&V) database, and a defined security policy to answer questions such as:

- Is a system or network really under attack?

- How is the system being attacked (i.e., probable tools or techniques)?
- What parts of the network, or systems, are vulnerable to the attack?
- What countermeasures should/could be used to mitigate the attack?

In the context of the above, "integrate" may simply mean presenting all of the data to a human operator in a readily usable format that permits a manual "integration", vice the "system" integrating the data to determine current status. The degree to which the process may be automated is to be examined during the proof-of-concept phase of the project.

As the NEWS is anticipated to consist entirely of software and associated databases, a software development methodology that followed the evolutionary model described in IEEE Std. P1498/EIA IS 640 was selected. This approach has the following characteristics:

- The system requirements are not all defined before development is undertaken.
- Multiple development cycles are used to progressively focus and refine the system.
- The interim software system is distributed.

This approach has been selected because an early capability would be useful, funding and staffing will be incremental, and user feedback and monitoring of technology changes are needed to understand the full requirements.

System Architecture

Figure 1 shows the high level NEWS architecture. It includes sensors and tools that are connected to a common interface function. The Interface function connects to a System Operator function. The System Operator will perform the day-to-day activities involved with entering NEWS Control and Data and observing and interpreting the System Status and Detailed System Information data flows.

The original concept was to integrate NEWS with standalone sensors, databases and tools. It became evident, however, that the design, configuration and management of these items form an important part of the NEWS and should therefore be included as part of the overall design.

While not shown on the diagram, NEWS also has an interface to the System Security Administrator, who will be performing the definition, set-up and maintenance of the NEWS configuration. This interface will involve NEWS Control and Data, those aspects of system policy that must be transferred to NEWS, and an interpretation of the System Status and Detailed System Information data flows. The System Security Administrator interface will not be built as an integrated entity. Administration of the intrusion detection devices and firewall will be performed via the individual consoles. It was felt that integration of these was a low priority for NEWS because most of the modern systems already provide a remote administration capability. Configuration of those systems that do not have such a capability will be performed by going to the appropriate console to do the work.

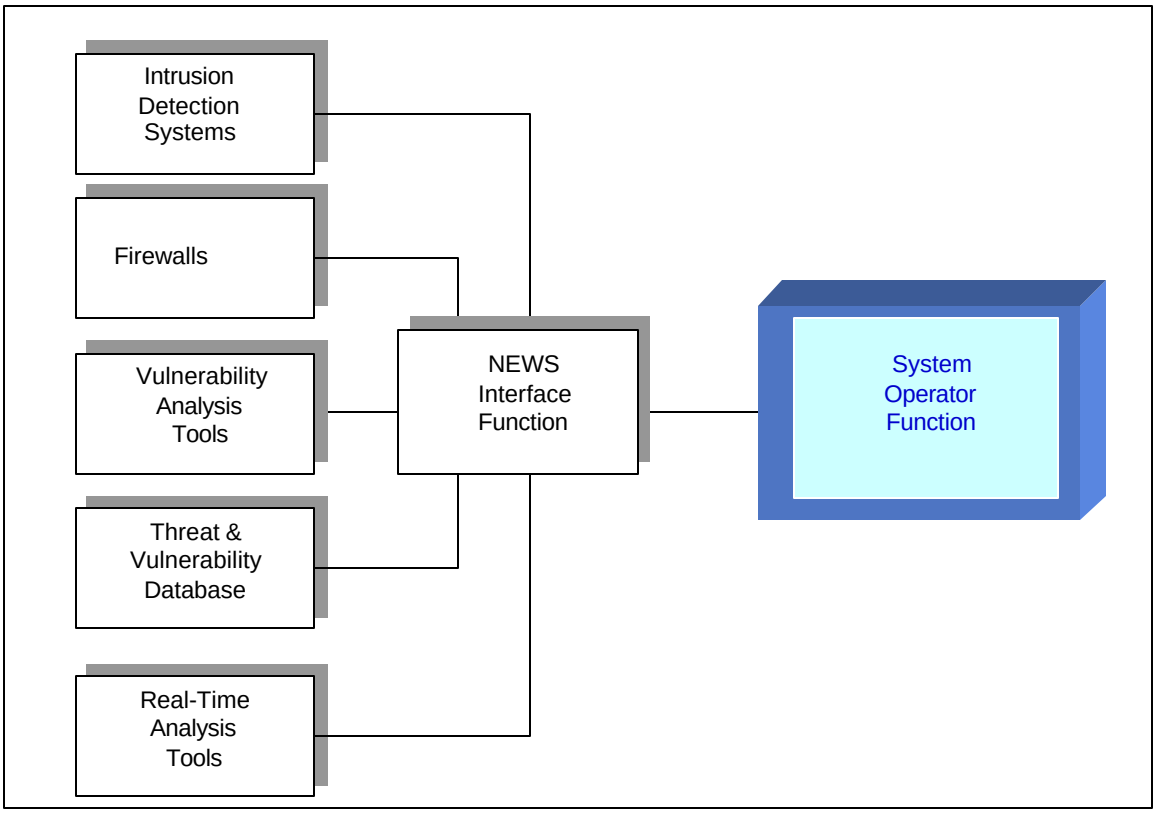

Figure 1 –NEWS Context Diagram

Internal Components

The intent in designing NEWS was to make it flexible enough to be integrated with a wide range of components. Numerous candidates were identified. Initially though, the focus was on showing that integration can yield a system that is useful to a system operator. The list of potential components was therefore cut to include only those with which EWA-Canada had some recent operational familiarity. A final selection of components was then made based on criteria discussed individually below.

Intrusion Detection Systems

The short list included NetRanger, RealSecure and the Secondary Heuristic Analysis for Defensive On-Line Warfare (SHADOW) Intrusion Detection Systems. It was decided to retain NetRanger because EWA-Canada has used it extensively and therefore it can serve as a source of data without requiring additional collection effort. SHADOW was selected as the second system because several potential clients have chosen it and because it is highly configurable.

Firewalls

The short list included BorderGuard, Internet Protocol (IP)Chains and the ConSeal Personal Computer (PC) Firewall. BorderGuard feeds information directly to the NetRanger. NEWS will therefore get the information via NetRanger. It was therefore decided to integrate IPChains and the ConSeal Firewall as the two firewalls.

Vulnerability Analysis Tools

The short list included CyberCop, Internet Security Scanner and Nessus. CyberCop has recently implemented a new database format for its output data and it was therefore felt risky to base NEWS on it because of potential problems with a new product. Of the remaining two, it was felt that it would be preferable to integrate with Nessus because additional experience and reporting capability for this tool would be more beneficial to the project.

Threat and Vulnerability Database

A threat and vulnerability database being developed under a separate project will be interfaced to NEWS. The tables implemented in versions 1.0 and 2.0 of this software are augmented by a Support Countermeasures table and an Event table, along with their associated link tables. The user interface is enhanced to incorporate these tables and reports are added to display the additional information.

Real-Time Analysis Tools

The short list included nmap, strobe, whois, nslookup, ping, fping, netcat, telnet, whisker, guile-scan or another cgi-bin scanner, Ethereal, tcpdump and traceroute.

Strobe is a Transmission Control Protocol (TCP) port scanner, whose capability is included in nmap. It is therefore not needed.

Fping is a variant of ping, and is not needed for a demonstration application.

Netcat, telnet, and the cgi-bin scanners (e.g., whisker, guile-scan) are not used often, and are therefore low priority for integration with NEWS.

Tcpdump is the basis for SHADOW, and therefore will be included in the Intrusion Detection section. Ethereal is a graphical interface for SHADOW. While it will provide a user interface for generating and examining the SHADOW data during development, and might provide assistance in defining the prototype user interface for NEWS, it need not be integrated with it.

The real-time analysis tools were therefore nmap, whois, nslookup, ping and traceroute.

Functional Design

Figure 2 shows the relationship between the major functions and the interface data. The top-level functions are described briefly the following paragraphs.

Administer Remote System

The Administer Remote System function provides remote logon and administration privileges on the external ID systems and Firewalls. The capability already exists for some firewalls [1].

Analyze Alerts

The Analyze Alerts function examines the alert data from firewalls and ID systems and decides, with the aid of information provided by other externals, such as the Threat and Vulnerability database, whether or not the system is under attack. The complexity of this function is judged to be medium to high. It is felt

[1] Examples include Gauntlet and CA GuardIT.

that a simple rule-based system might provide some assistance to the operator, but will not provide a general solution. An artificial intelligence solution will probably be required. This function requires a populated T&V database and a means of reducing the outputs of the firewalls and ID systems to a common enumeration.

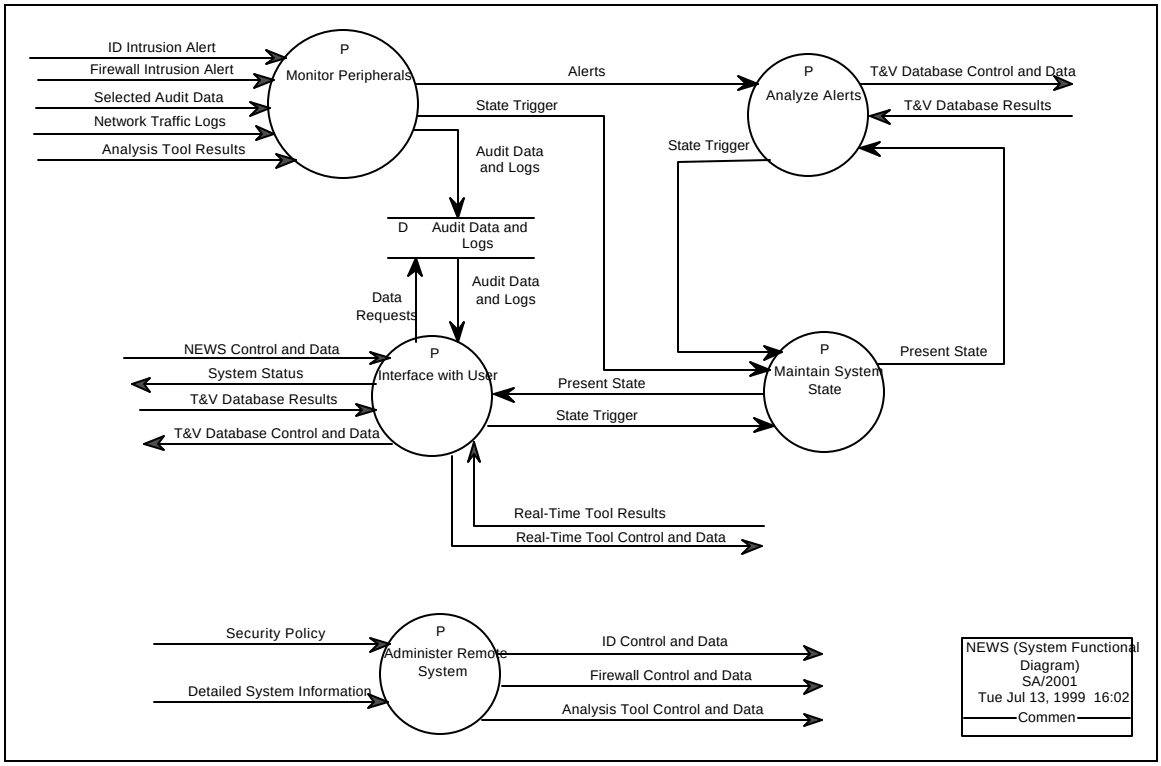

Figure 2: NEWS Top-Level Functions

Interface with User

This function enables NEWS to interact with the user in an intuitive, easy-to-use manner. It should support multiple views (e.g., network, service, host) of the system and present graphics related to performance or configuration (e.g., World Wide Web (WWW) traffic vs. time, IP Address and associated active ports). Although the complexity of the user interface is considered low, it is a high priority function. The success of the NEWS depends on its acceptance by the users.

Maintain System State

This function implements a finite state machine that changes the system mode in response to system events. This is a low complexity function and is considered to be medium priority. At least one of the state trigger sources is required. These include:

- Interface with User.
- Monitor Peripherals.

- Analyze Alerts.

Monitor Peripherals

The Monitor Peripherals function provides the real-time interface between the NEWS and the firewalls, the IDs, and the automated analysis tools. It receives alerts and triggers their analysis. It receives supporting audit or traffic log data and buffers it for later use. The complexity of this function is deemed to be medium, primarily because of the disparate interfaces that must be accommodated. This is a high priority function.

Testbed Architecture

The architecture of the testbed is shown in Figure 3. Here we show an Internet connection through a Cisco router. This allows for the inclusion of external attacks for the prototype system. All other attacks are generated internally by the attack tool function.

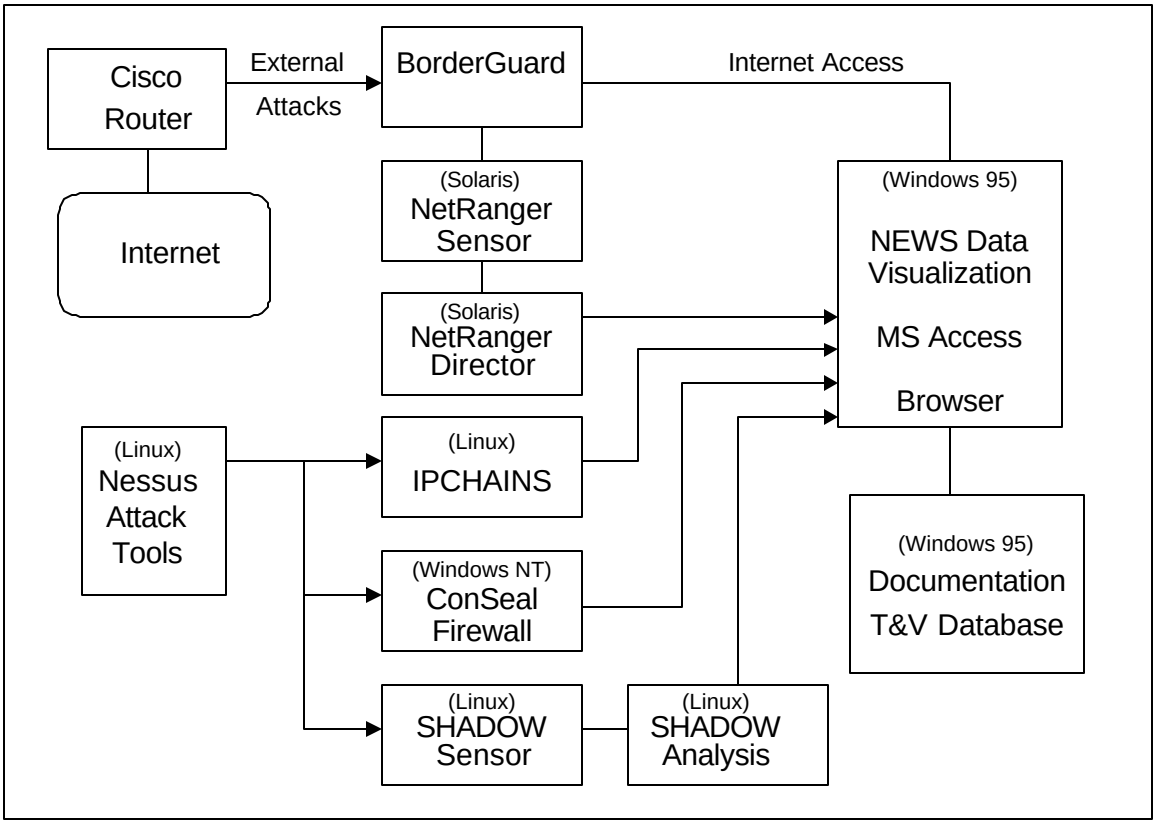

Figure 3 - NEWS Testbed Mode Architecture

The testbed mode of NEWS, as shown in Figure 3, consists of four subsystems:

1. The shared components in the upper left of the diagram (Internet connection, Router, BorderGuard, and NetRanger) form part of the internal EWA-Canada computing infrastructure, and therefore cannot be deliberately attacked during NEWS exercises.

2. The dedicated components in the lower left of the diagram (Nessus, Attack Tools, IPChains, SHADOW and the ConSeal PC Firewall) are configured in such a way that Nessus and the Attack Tools could target any and all of the test countermeasures.

3. The NEWS Interface module, in the centre of the diagram, consolidates information from the other devices and presents it visually to the operator module.

4. The NEWS Documentation and Threat and Vulnerability Database, in the lower right, is a resource that may be called upon by the visualization software or by the operators.

This prototype architecture is currently distributed over many PCs, each with a dedicated user interface.

Software Components

The NEWS software components are listed in Table 1.

Software	Comments
Attack Tools	The Attack Tools will be used to conduct controlled attacks on the systems protected by the firewalls and intrusion detection devices for the purpose of determining their effectiveness. A library of attack tools exists at EWA-Canada. Others may be downloaded from the Internet as required.
Browser	A Browser is a program that allows a person to read hypertext. The browser gives some means of viewing the contents of pages of information and of navigating from one node to another. The browsers are provided as part of the operating system or may be downloaded from the World Wide Web (WWW) and installed.
E-Mail client	The E-mail Client supports sending and receiving e-mail messages.
File Transfer Protocol (FTP) Client	The FTP Client provides file transfer capability over the Internet.
IPChains	IPChains is a Linux-based packet filtering firewall. It is an open source product, available for download from the WWW. It needs to be configured with filter-definition files.
Linux	Linux is an operating system that provides system resources and tools to support other NEWS software units. A commercial distribution of Linux is to be used.
Microsoft Access	Microsoft Access is a database development and management package. This is a commercial product.
Nessus	Nessus is a remote security scanner that can audit a given network and determine whether it exhibits selected vulnerabilities. Nessus is available for free download from the WWW.
NetRanger	NetRanger is an intrusion detection device that examines network events to identify and report those that might be related to real or attempted intrusions.
NEWS Data Visualization	The NEWS Data Visualization item provides a graphical user interface for displaying and manipulating large volumes of data in real time.
Real-Time Tools	The Real-Time Tools provide support for the analysis of anomalous events that are identified by the sensors or the Data Visualization Tool. Downloadable from the WWW. Tools are: nmap, whois, nslookup, ping, and

	traceroute. Nmap, whois and nslookup are already integrated with SHADOW.
SHADOW	SHADOW is an open-source Intrusion Detection System, downloadable from the WWW. It needs installation and configuration as wellas control data files.
Threat and Vulnerability Database	The Threat and Vulnerability Database provides information about the vulnerabilities in system components, attacks that might exploit these vulnerabilities, countermeasures to identify and prevent damage by the attacks, test tools and exploit tools.
Windows 95, NT	Windows 95 and Windows NT are Microsoft operating systems. They provide system resources and tools to support other NEWS software units.

Table 1: NEWS Software Components

Interface Design

Table 2 lists the data interface functions for the system. Although the functions for each component class are the same, the structure of the data differs. As an example, the data and the format provided by each of the firewalls and the intrusion detection systems varies considerably.

Name	From	To	Content
ID Control and Data	NEWS	Intrusion Detection Systems	ID control commands, ID data requests, ID configuration data
Selected Audit Data	Intrusion Detection Systems	NEWS	Segment of audit data of relevance to a suspected intrusion.
ID Intrusion Alert	Intrusion Detection Systems	NEWS	Signal that the ID has detected a security event. An event is considered to be anything that may indicate that an intrusion is in progress.
Firewall Control and Data	NEWS	Firewalls	Firewall control commands, Firewall data requests, Firewall configuration data
Network Traffic Logs	Firewalls	NEWS	Segment of log files of relevance to a suspected intrusion.
Firewall Intrusion Alert	Firewall	NEWS	Signal that the Firewall believes an intrusion is taking place or has taken place.
Analysis Tool Control and Data	NEWS	Vulnerability Analysis Tools	Analysis tool control commands, Analysis tool data requests, Analysis tool configuration data
Analysis Tool Results	Vulnerability Analysis Tools	NEWS	Suspected vulnerabilities and supporting information, perhaps including recommended countermeasures.
T&V Database Control and Data	NEWS	T&V Database	Requests for database information, Data to be placed in database, Data display control commands.
T&V Database Results	T&V Database	NEWS	Information from the database.
NEWS Control and Data	System Operator	NEWS	NEWS system commands, NEWS system requests for data, data to be forwarded to interfaced applications.
System Status	NEWS	System Operator	System security state: safe, warning or attack.
Detailed System	NEWS	System Operator	Additional information about the system,

Information			its applications or data.
Security Policy	System Security Administrator	NEWS	Intended security policy for the system components.
NEWS Control and Data	System Security Administrator	NEWS	NEWS system commands, NEWS system requests for data, data to be forwarded to interfaced applications.
Detailed System Information	NEWS	System Security Administrator	Forwarded data from interfaced applications, system status, system security state, additional information about the system, its applications or data.

Table 2: NEWS Interface Data

Table 3 summarizes the IDS and firewall log data. The differences must be accommodated in the interface to the data visualization function.

Item	NetRanger	SHADOW	ConSeal PC Firewall	IPChains
Record Type	X	X[2]		
Record ID	X		X	
GMT Date	X			
GMT Time	X			
Local Date	X	X[3]	X	X
Local Time	X	X	X	X
Application ID	X			
Host ID	X		X	
Organization ID	X			
Source Direction	X		X	
Destination Direction	X			
Alarm Level	X			
SigID	X			X
SubSigID	X			
Protocol	X		X	X
Source IP Address	X	X	X	X
Destination IP Address	X	X	X	X
Source Port	X	X	X	X
Destination Port	X	X	X	X
Router IP Address	X			
Actual error string	X			
Action taken			X	X
Message type			X	
ICMP type number			X	
Packet type				X
Rule			X	X
Packet length		X		X
Type of service				X
IP ID				X

[2] Implied by the format of the line of data.
[3] Implied by the name of the SHADOW text file, which is in the form YYYYMMDD.txt.

Item	NetRanger	SHADOW	ConSeal PC Firewall	IPChains
Fragment offset/flags				X
Time to live				X
Flags		X		
Data Sequence Numbers		X		
Buffer Space		X		
TCP Options		X		

Table 3: Log File Data Element Summary

RESULTS AND CURRENT STATUS

Testbed

Shadow was chosen as the first IDS to integrate under NEWS. The following outlines the configuration of the Shadow system as used in the testbed architecture. The "sensor" and "analysis" stations were two separate systems. The sensor station currently has one network interface card connected to the main Internet connection, this card has no IP address and is therefore unreachable by other systems. The second interface is on a protected network currently consisting of only this system and the analysis station. The installation of the sensor station was conducted according to the installation instructions by the Naval Surface Warfare Center with only a single modification. In order to overcome an incompatibility with the current version of the startup script and the installed version of tcpdump, it was necessary to add an instruction to force the network interface card into promiscuous mode. This action only occurred every second hour in the absence of this correction, leading to loss of data for the hour when it wasn't performed. More changes from the standard Shadow installation were implemented in the analysis station. Initial configuration of the two systems included the following:

Installed components for both systems:

- Red Hat Linux 6.1
- Libpcap
- Tcpdump
- Perl
- Sudo (so that the unprivileged user Shadow runs as can use some tools as root)
- SSH (These components can be installed by a default installation of Red Hat Linux 6.1.)

Installed components on the sensor station:

- Shadow scripts specific to the sensor in their appropriate locations.

Installed components on the analysis station:

- Apache web-server
- Tcpslice (included in current versions of tcpdump)
- Argus

- Nlog and nlog conversion utilities
- Nmap
- Analysis station specific scripts and filters in their appropriate locations
- Whois (included in the default Red Hat Linux installation)
- Nslookup (included in the default Red Hat Linux installation)

Originally it was anticipated that differential nmap would be used to show configuration changes in the monitored system. However, the need for this function has been circumvented by an increased reliance on nlog that provides richer information because of its ability to provide historical information as well.

In addition to the work involving Shadow, sample data files were obtained for:

- NetRanger.
- IPChains.
- Nessus.
- ConSeal PC Firewall.

Threat and Vulnerability Database

The threat and vulnerability database had been modified by CSE. The modifications were analyzed to find out what they had done and what needed to be done to complete it so that only one version would be maintained in the future. These changes were integrated with the additional requirements to build the Support Countermeasures and Event tables and associated links. The tables and links were built and tested. An early list of vulnerabilities at the CVE web site was imported manually into the existing threat and vulnerability database. Limited population of the database was conducted, with emphasis placed on Denial of Service attacks.

Data Visualization Module

To demonstrate the concept of displaying anomalous traffic in a network a rapid-prototype, three-dimensional graphical user interface (GUI) was developed. The intent was to explore methods of providing an operator with an easy way to see events that may be of concern from a network security point of view.

Figure 4 shows a screen shot of the GUI. Each cube represents a machine within the network that has an IP address. The cubes are arranged such that machines with near-by IP addresses are clustered near each other

on the screen. An example of this can be seen at the bottom, right of the figure where two cubes with adjacent IP addresses are stacked.

Data from an IDS or firewall is passed to a central database and then displayed on the GUI. This type of display can help decipher the nature of attacks. The lines connecting cubes indicate that traffic has been detected between the machines. A single machine scanning through a range of IP addresses would immediately be apparent. In the centre of the figure, a rectangle with an IP address is shown. This flag lights up when the cursor is placed on the cube. Double-clicking on a cube will allow the operator to “drill down” for additional information such as the number of incidents of different alarm types.

At the left of the figure, a few operator-selectable functions are shown. These allow the operator to select the IP addresses to be displayed, the time window of interest and the protocol type. Additional functions are relatively easy to implement. We are currently seeking feed-back from operators as to which functions they would like to have.

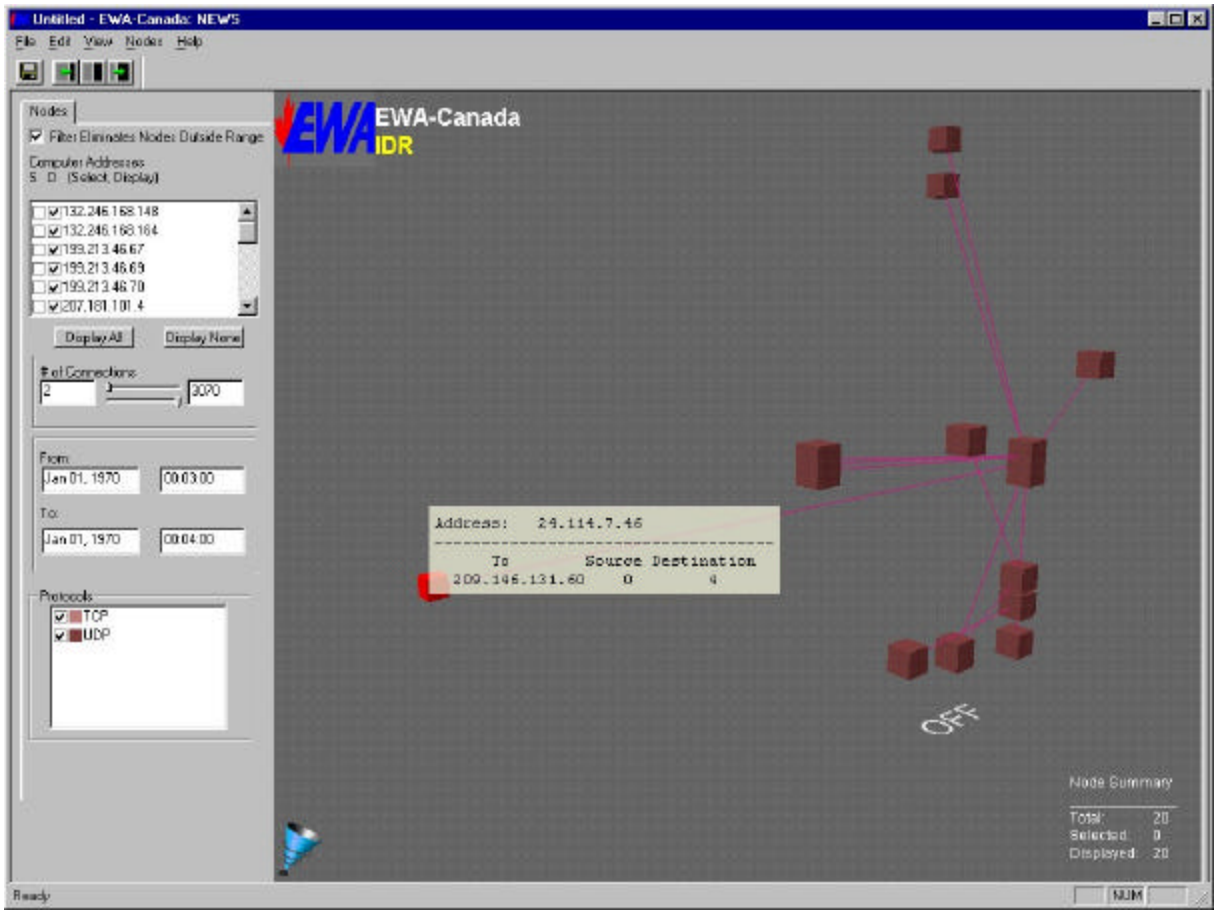

Figure 4: Prototype Visualization Screen

Library Database

A repository of information on firewalls, intrusion detection systems, and related items, has been created. The NEWS Library database is being built to allow operators to pull up referenced documents that may be pertinent to their task. The database consists of:

- A Microsoft Access database that retains information on those documents referenced by the NEWS project documents plus selected others.
- Macros and mail-merge documents for converting this database into Word for Windows 97 reference format.
- A NEWS library operations guide, which describes the library and how to use it.

- Macros for manipulating referenced documents and inserting cross-references to them into a Word for Windows 97 document.

SUMMARY

The internal research and development program conducted to date has created a sound basis for NEWS by:

- creating a conceptual system overview document to guide the NEWS development;
- creating requirements and top-level design documents for those portions currently under construction;
- installing and configuring a representative set of firewalls, intrusion detection systems, vulnerability analysis tools, and real-time analysis tools;
- developing a prototype graphical visualization interface for sensor log data; and
- extending the threat and vulnerability database to include support countermeasures, alarms, events and signatures and populating it with limited representative data.

The real value added by NEWS is the provision of:

- a network monitoring tool, which could be used by a network administrator;
- an incident response tool, which supports general-purpose network exploration and analysis when responding to a reported incident;
- a network security testbed, which supports network security research and development; and
- a network profiling tool, which supports network security analysis.

Follow-on research and development activities will include:

- extending the visualization module prototype interfaces to include the remaining configured sensors;
- using standard scanners and attack tools to provide realistic data for visualization and threat and vulnerability database signature population;
- conducting tests and demonstrations to elicit more detailed requirements and to develop realistic usage scenarios;
- defining an integrated alert processing module;
- investigating system security policy concepts, including both flow-down from the enterprise level to the detailed sensor rulebases and reverse-engineering concepts to abstract the detailed sensor rulebases into higher-level policy;
- upgrading the integrated tools and sensors to keep pace with the latest developments;
- continuing to develop and populate the threat and vulnerability and related knowledgebases; and
- evolving the prototype into a defined product, complete with standard tests, scenario-driven demonstrations, and user and maintenance documentation.