Software Requirements Specification

for

Design and Development of an Enterprise Anomaly Detection Solution

Version 1.0

Prepared by Maria J. Robert & Adnan Iqbal

NUST School of Electrical Engineering and Computer Science

30th August, 2008

Table of Contents

Revision History

Name	Date	Reason For Changes	Version

1. Introduction

1.1 Purpose

This Software Requirements Specification (SRS) documents key specifications, functional and non-functional requirements of Enterprise Anomaly Detection Solution (EADS). The information documented, helps the intended audience to design, develop and then use the product. The product, EADS provides real-time detection for Internet threats with the analysis of attack forensics. EADS allows its users to select data capturing and detection technique from a variety of available techniques. All detection techniques used to build complete solution support adaptive thresholding. This adaptive thresholding is unique as it does not require any human intervention. It also facilitates users to generate different reports for a variety of managerial tasks. This is release 1.0 of the document and covers preliminary known features and requirements.

1.2 Document Conventions

The document covers the conventions as described by IEEE SRS template. The template standards are published in "IEEE Standards Collection," and can be downloaded from http://www.csc.villanova.edu/~tway/courses/csc4181/srs_template-1.doc.

1.3 Intended Audience and Reading Suggestions

The intended audience of this document includes project managers, designers, developers and end users (system/network administrators) of EADS.

1.4 Product Scope

EADS is a network based anomaly detector aimed to provide accurate and real-time enterprise intrusion detection and prevention solution to combat zero-day as well as known attacks. EADS is developed to provide a complete, better than existing and an open source solution to the rising number of insecure enterprise networks.

The proposed solution, EADS promises to provide:

1. A low complexity network security solution that will defy threats appearing at network gateway and end-host level.
2. High detection rate and very low false alarm rates.
3. Low detection delays.

4. Online support.
5. Open-source access to implementation files.

This projects aims to:

1. Achieve maximum (nearly 100 %) detection and negligible false alarm rates.
2. Detection of malicious events with negligible delay.
3. Minimize the utilization of processing resources.
4. Provide availability of a complete open-source library for further research and development.

The project outlines the following objectives:

1. Smooth running of product with complete error handling.
2. Achieving expected detection and false alarm rates.
3. Providing a user friendly menu for configuring and scaling the available options.

1.5 References

More information about the project, anomaly detection techniques used and improvement techniques is available at www.wisnet.niit.edu.pk

2. Overall Description

2.1 Product Perspective

EADS is a real-time intrusion detection and prevention solution to mainly detect zero-day network attacks. The solution is also capable of detecting and defying previously known attacks. The solution is composed of several modules performing different tasks. The module for data capturing implies a hybrid approach such that the data is collected at both gateway and end-host level. The use of network and end-host data simultaneously significantly improves the chances of detecting of correlated attacks. The anomaly detector module implies several approaches to correctly identify malicious events. This module evaluates existing and new traffic features of incoming and outgoing traffic for real-time attack characterization. These features are used for attack detection in novel information-theoretic, statistical, and machine learning frameworks. The anomaly detector module is further decomposed into several sub-modules such as passive and active anomaly detectors. The passive anomaly detector is designed to capture incoming traffic that is bound for inactive IP addresses and ports inside an enterprise network. The passive detector develops a baseline model of mis-configured incoming network traffic. Deviations from this model are used to detect malicious traffic patterns. The active anomaly detector preemptively and quickly detects Internet-scale and

targeted threats and also facilitates attack forensics. The details of these sub-modules shall be made available in the design document of the proposed solution. All these operations of EADS are supported by a user friendly and interactive graphical interface, which lets user select variety of options and customize the usage of EADS. The general deployment of EADS is shown in Figure 1.

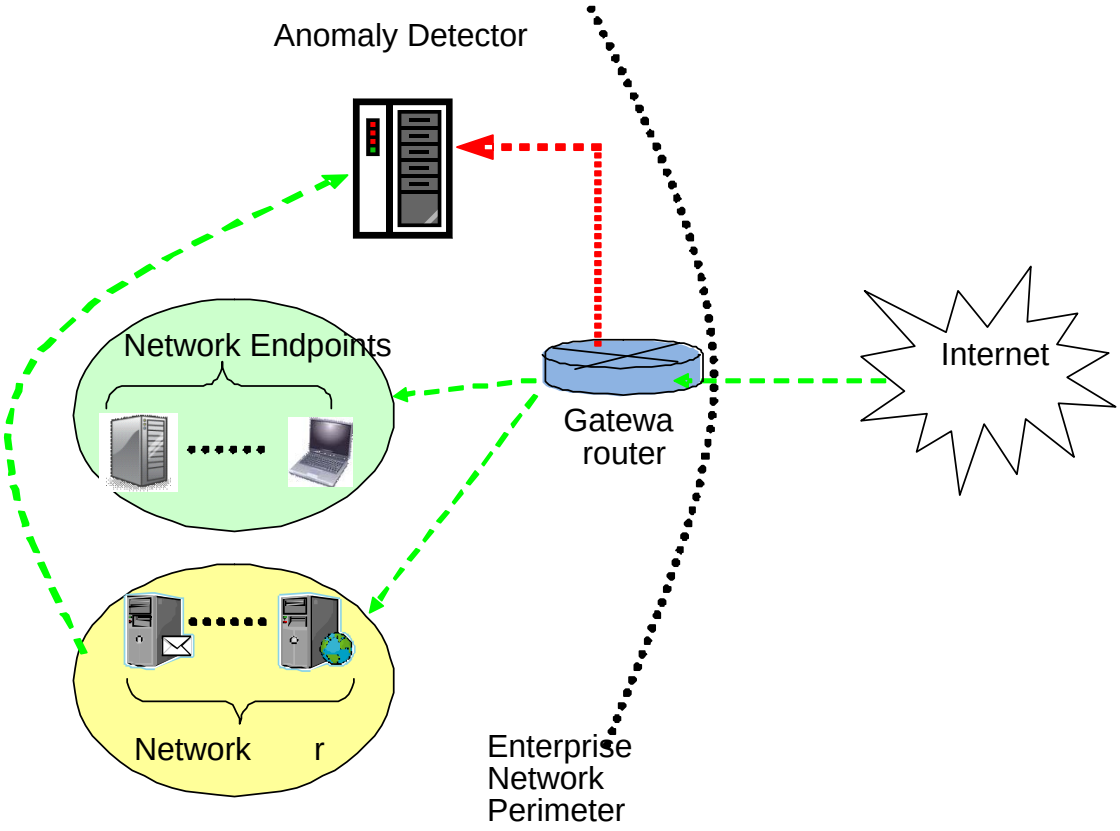

Figure 1 ***A potential deployment strategy for the proposed solution***

2.2 Product Features

The proposed solution will include both detection and prevention mechanisms to combat zero-day and known attacks. This task poses several challenges to be met so that the objectives are achieved successfully. These challenges and their respective scope are outlined below.

1) Data:

   As mentioned earlier, we shall adapt a hybrid approach that includes capturing audit information at network level as well as end-host level. The main building block of data to be evaluated is the incoming or outgoing packet. Captured packets shall be processed to filter session level information. The session level data will be stored in a predefined format such as S-flow or Peakflow. User will have the option to choose the preferred data type. The anonymization of the captured data is not in the scope of the proposed solution. The data archiving will not be available by default.

2) Anomaly detection:

   The anomaly detection method is primarily dependant on the user chosen algorithm. Every algorithm has its own mechanism of detecting malware; however, user will have the option to choose static or dynamic thresholding with each algorithm. Only one algorithm can be used at one time but user will have the option to switch among them. Intelligent change in thresholds is visible if adaptive thresholding is turned on. Such automation is not available in static thresholding. In the case of static thresholding, network managers will need to manually change the threshold, if needed..

3) Prevention:

   Apart from detection, prevention solution will also be provided in EADS. Prevention methods include blocking the malicious host dropping of malicious packets and sessions from the hosts. EADS will provide prevention by using all these methods and choosing the best suitable for a particular situation.

4) Accuracy:

   We aim to develop a solution with high detection rate and negligible false positives. This is a crucial requirement as most of the existing systems suffer from a very high false positive rate. On the other hand, high detection rates are equally important. We propose to use several different techniques of anomaly detection to achieve this goal. The detailed description of these schemes shall be available in the design document.

5) Human intervention:

   The proposed solution does not require any human intervention in the process of data capturing, anomaly detection and prevention process. Human interaction is however needed while configuring the solution to accommodate customized preferences of different end users.

6) User interface

   For configuration and customization purposes, a user friendly graphical interface shall be provided. This interface shall provide the options of selecting any algorithm of choice and tuning parameters like anomaly detection window and archiving options.

2.3 User Classes and Characteristics

The solution is intended to be used primarily by network managers and system administrators. The solution shall also work as a useful tool for top level management such that they can have a broader picture of network in terms of security. System administrators will have most direct contact with the solution. System administrators will install, configure and constantly monitor the solution. They will also view and analyze the reports generated from the solution. Fine tuning of the solution and selection of algorithm is also the duty of system administrators. The interest of top level

management is restricted to the overall network conditions which can be facilitated by generating detailed report. Therefore, the most privileged user class consists of system administrators.

2.4 Operating Environment

The target operating system of EADS is Linux. The solution should be developed such that it can smoothly run on several different distributions of Linux.

2.5 Design and Implementation Constraints

Processing Power:

> EADS requires high speed data capturing, analysis, detection and prevention with in negligible. With these features, high speed processing machine is required to fulfill all the tasks.

Deployment Point:

> EADS is meant to be deployed at the gateway router of a network. In any other case, EADS does not work properly.

Routers:

> EADS is compatible with only Cisco and Arbor routers. In case of any other router, dumping data format will change and cannot be used for detection purposes. However, using EADS's own sniffer is an option that the users can avail.

Detection/False Alarm Rates:

> Detection and false alarm rates depend on the choice of algorithm from the user. As for now, EADS at maximum can detect anomalies up to a certain value. With detections, come a number of false alarms as well. Future releases might improve these parameters.

Operating Platform:

> EADS will work for several distributions of Linux and Windows.

2.6 User Documentation

User manual and CD will be made available for troubleshooting and help. The user manual will contain detailed information about the usage of the product from a layman perspective to an expert network/system administrator. The manual shall also be made available online.

2.7 Assumptions and Dependencies

The proposed solution will be designed to work in an enterprise environment. The target environment may consist of wired and wireless links inside the network. All outbound and incoming traffic is supposed to go through edge routers.

The solution has to be self sufficient and free from any unfamiliar dependencies. Well known and widely available libraries, such as libpcap are however permitted.

3. External Interface Requirements

3.1 User Interfaces

A graphical user interface is available providing following functionalities:

- Drop down menu for algorithm selection
- Selection list for scaling the threshold up or down
- Push buttons to observe different traffic statistics
- Graphs to show traffic characteristics in a user chosen time frame
- Help button

A screenshot of proposed user interface is shown in Figure 2.

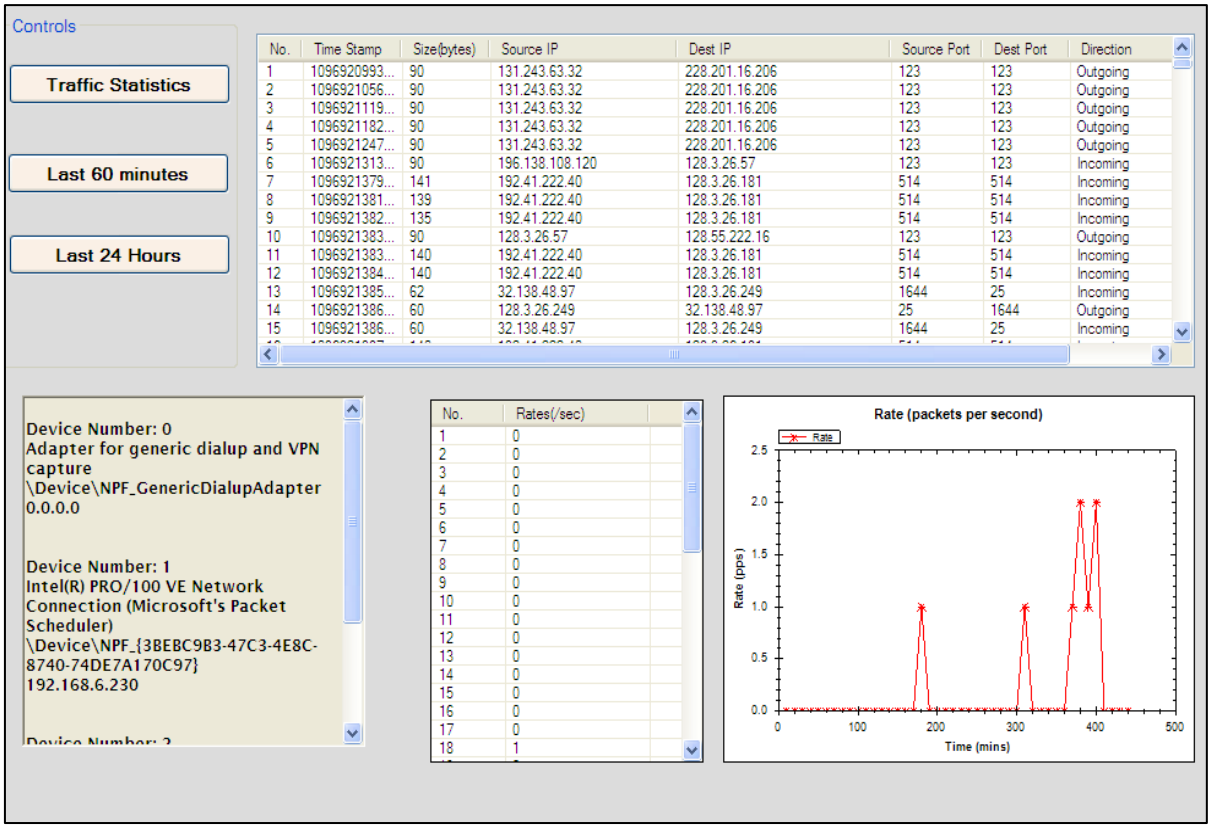

Figure 2 ***Screenshot of user interface***

3.2 Hardware Interfaces

The solution makes extensive use of several hardware devices. These devices include;

- Network Interface Cards
- Cisco/Arbor Routers
- Windows and Linux(any distribution) client computers

3.3 Software Interfaces

EADS will allow users to select one of the software interfaces available for capturing incoming traffic. These interfaces will store packet/session data in their own defined structured format. The interface can have:

1. EADS's own defined format
2. PeakFlow format
3. SFlow Format

MySQL database is used for storing the data. This whole product runs on different distributions of Linux. As an underlying communication mechanism between modules on different systems, TCP is used because of its reliable services.

3.4 Communications Interfaces

EADS is a large scale project and is needed to deploy on different systems. For storing and retrieving packets and other data, a database of audit data and reported events is stored on another system. Retrieval of data for monitoring and reports is entirely an independent process than detection and prevention. Database server is central and needs to be communicated in a reliable and efficient way, so that real-time results can be generated. For this purpose TCP protocol is used for underlying communication needs.

4. System Features

The proposed solution shall provide several services to its users. Major services provided by the EADS system are briefly discussed below.

4.1 Passive Anomaly Detection

4.1.1 Description and Priority

The passive anomaly detector is designed to capture incoming traffic that is bound for inactive IP addresses and ports inside an enterprise network. This is a high priority feature because it develops a baseline model of misconfigured incoming network traffic. Deviations from this model are used to detect malicious traffic patterns.

4.1.2 Stimulus/Response Sequences

Stimulus: Network traffic reaches the detector.

Response: Network traffic is checked for misdirection.

Stimulus: Network traffic reaching the detector is legitimate.

Response: Drop the traffic data.

Stimulus: Network traffic reaching the detector is misdirected.

Response: Misdirected traffic data is stored in a database.

Stimulus: Database is updated.

Response: Data is used for baseline formation analysis.

4.1.3 Functional Requirements

REQ-1: User is asked for username and password
REQ-2: User is given three chances to enter his login name and password failing which the screen is locked and alert is generated in the form of a popup box and beep at the backend (main server) of a security breach.
REQ-3: After verifying the login, the user is granted access to the front end of the passive anomaly detector.
REQ-4: The interface has pushbuttons for starting/stopping the detector, pushbutton for logging out and grid for viewing session /packet details. The interface displays graphs to show the number of packets/sessions arriving in the adopted timeframe and locked text box to show current statistics of normal profile including threshold.
REQ-5: If the user presses the start button the detector, with the chosen detection technique, starts execution and looking for misdirected traffic.
REQ-6: If the user presses stop, the detector stops working.
REQ-7: Once a user logs out he is be asked to provide the login information again to access the application.

4.2 Active Anomaly Detector

4.2.1 Description and Priority

The detection will be done by the active component of the product. As soon as a deviation from the baseline or any malware is observed, this component raises an alert. The anomaly detector will evaluate existing and new traffic features of incoming and outgoing traffic for real-time attack characterization. These features will be used for attack detection in novel information-theoretic, statistical, and machine learning frameworks.

4.2.2 Stimulus/Response Sequences

Stimulus: Real-time traffic reaches detector

Response: Compare real-time traffic with baseline profile

Stimulus: No considerable deviation from the normal profile is observed.

Response: Ignore and continue detection

Stimulus: Considerable deviation from normal profile is observed.

Response: Raise an alert.

4.2.3 Functional Requirements

REQ-1: User is asked for username and password
REQ-2: User is given three chances to enter his login name and password failing which the screen is locked and alert is generated in the form of a popup box and beep at the backend (main server) of a security breach.
REQ-3: After verifying the login, the user is granted access to the front end of the active anomaly detector.
REQ-4: The interface has pushbutton for starting/stopping the detector, pushbutton for logging out and grid for viewing session /packet details. The interface also displays the number of packets/sessions, graphically, arriving in the adopted timeframe and locked text box to show current statistics of normal and incoming profile including threshold. The menu has selection list for choosing detecting algorithm and threshold.
REQ-5: If an anomaly occurs the pop-up box appears along with a beep to alert the administrators of a malware.
REQ-6: If the user presses the start button the detector starts executing and looking for misdirected traffic.
REQ-7: If the user presses stop, the detector stops working.
REQ-8: Once a user logs out he is asked to provide the login information again to access the application.

4.3 Capturing Audit Data

4.3.1 Description and Priority

Collection of audit data is the basic prerequisite of anomaly detection. Captured audit data shall consist of information at network level as well as end-host level. Initially, complete packets shall be captured. Session level information will be filtered from this data for anomaly detection purposes. This is a high priority feature of the solution.

4.3.2 Stimulus/Response Sequences

Stimulus: Real-time traffic reaches detector

Response: traffic is captured as it is and stored in the database.

4.3.3 Functional Requirements

REQ-1: All the data reaching any of the hardware interfaces of the solution is captured.

REQ-2: Captured data is initially stored completely.
REQ-3: Incase of extra-ordinary incoming traffic, it is permissible to miss few packets.

4.4 Alert Reporting

4.4.1 Description and Priority

The output of anomaly detection process is the generation of alerts in case of any event. These alerts are reported to relevant people using different methods and also stored for further investigation. The alerts are reported using pop ups and e-mail. Pop ups are displayed on the screen of network administrator whenever a critical event is detected. E-mails are sent to the people enlisted on the relevant mailing list. Network administrators are sent the mail whenever an event is detected. Only a summary e-mail is sent to the management.

4.4.2 Stimulus/Response Sequences

Stimulus: Enough data is captured so that the detection algorithms can operate.

Response: Anomaly detection algorithm is operated over collected data.

Stimulus: An anomaly is detected by the algorithm.

Response(s):

i. An alert is generated and pop up appears on network administrator's screen.

ii. An e-mail is sent to the members of a mailing list created for the same purpose.

iii. The anomaly detection results are stored in a database for further investigation.

4.4.3 Functional Requirements

REQ-1: Alerts should be concise and brief; however they must not miss any critical information.
REQ-2: Mailing list must contain the addresses of relevant people only.
REQ-3: Alert report for management must not be very technical.

5. Other Nonfunctional Requirements

5.1 Performance Requirements

The solution has to exhibit very stringent performance requirements. The system has very high detection rate (i.e., no less than 99%) in any circumstances. Similarly the system has very low false alarm rate (i.e., no more than 1%) in any circumstances. These requirements shall be achieved by using adaptive thresholding and a combination of several algorithms. Another performance requirement is the detection of anomalies in real time. The active anomaly detection module is proposed for the same purpose.

5.2 Safety Requirements

There are no specific safety requirements associated with the proposed system. The EADS is composed of well known and commonly used hardware which does not cause any safety hazards.

5.3 Security Requirements

Only authorized personnel are allowed to use the product and go through selection procedures. In case of forgotten passwords contact the developers. Similarly, changing the features of the solutions at runtime also requires password based authentication.

5.4 Software Quality Attributes

- **Reliability**

  EADS should provide reliability to the user that the product will run stably with all the features mentioned above available and executing perfectly. It should be tested and debugged completely. All exceptions should be well handled.

- **Accuracy**

  EADS should be able to reach the desired detection level. It should generate minimum false positive alerts with maximum detection rate.

- **Resources**

  EADS should use minimal resources in terms of memory, time and CPU.

- **User Friendliness**

  EADS should have a graphical user interface with user friendly menu.

5.5 Business Rules

EADS is most suitable for network administrators of large enterprises. The product should be used with precaution to avoid loss of data. Please see the manual for help.

6. Other Requirements

This is a copyrighted product.

Appendix A: Glossary

EADS: Enterprise Anomaly Detection System

ADS: Anomaly Detection System

GUI: Graphical User Interface

UI: User Interface

Appendix B: Analysis Models

Data Flow Diagram:

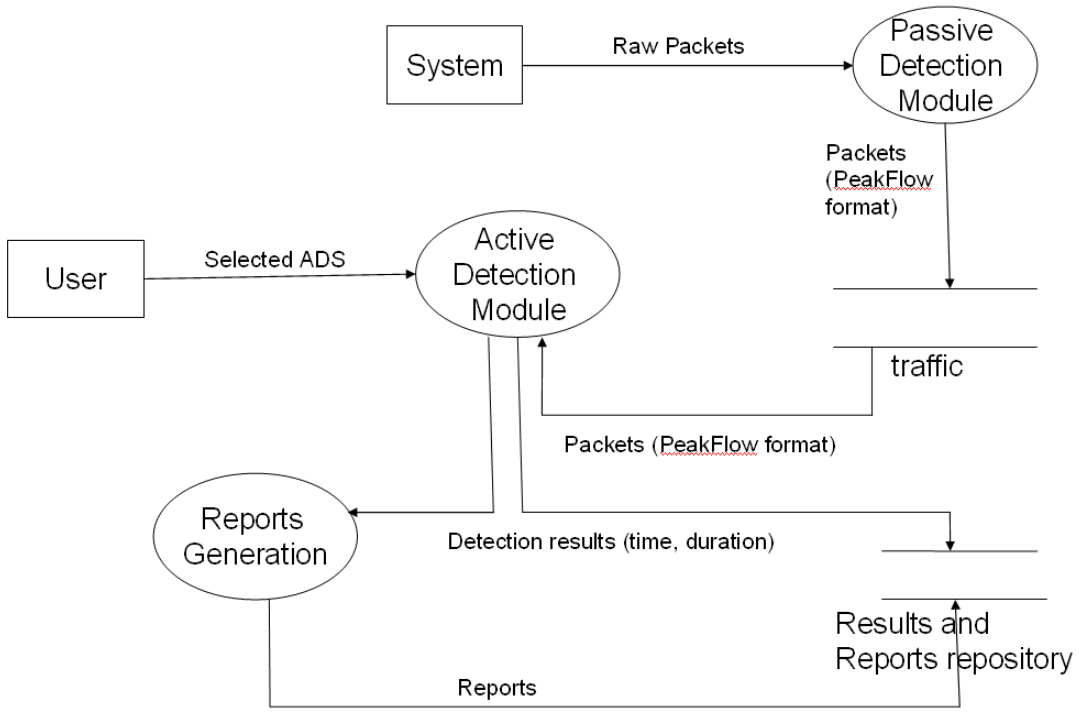

Figure 3: Data Flow Diagram