Experimental Research on DFA-Based MLML IDS Security Evaluation

Hongbin Wang, Zhiyi Fang, Simon Fong, Yain-Whar Si, Liyang Liu

Abstract: Many manufacturers and researchers have established various Intrusion Detection System (IDS) evaluation standards, most of which involve tests of IDS functions but neglect evaluation of IDS security. On the basis of IDS security evaluation, this paper describes segmented and multi-level mixed evaluation methods, classifies intrusions by type of TCP/IP, and illustrates the evaluation process by means of the Deterministic Finite Automaton (DFA) in fragmentation, making the test process more straightforward and vivid. Credibility levels are assigned to measures which are taken to make products meet basic functional requirements, thus dividing the evaluation process into three levels.

Key words: IDS, Multi-level evaluation, Multi-layer evaluation, DFA, security

1. Introduction

In recent years, the development of researches on the intrusion detection technology has given rise to various IDSs [1-5]. As a result, the requirements for IDS functions and performance evaluation emerge. Currently, many manufacturers and researchers have established various IDS evaluation standards, most of which involve IDS function test but not IDS security evaluation. This paper describes how to conduct IDS security tests through multi-layer and multi-level (MLML) evaluations and by using the DFA. The method of illustrating the security evaluation process through DFA fragments takes advantage of states and processes. Multi-level evaluation assigns credibility levels to measures taken to make products meet basic function requirements, thus helping users judge whether information products are safe to their applications. Multi-level evaluation conducts independent vulnerability analysis. Based on the vulnerability analysis, a security test is carried out to check whether the product is resistible to attacks. The tests in this paper are divided into three levels.

For testing IDS security, the attack data set should be as complete as possible. However, to reduce the overhead in testing, all known attacks should not be included in the set. Therefore, we must strike a balance between completeness and coverage. An effective solution to this issue is to classify attacks by a certain standard. This paper classifies attacks by type of TCP/IP, and then selects one or more representative attacks from each classification for test use. In addition, in our approach, attacks can be conveniently added, which is another advantage of this method.

The security test aims to check two aspects: whether the program works normally under various network circumstances, and whether communication among modules of the program can be protected from damage and counterfeiting. This paper focuses on resistance to denial of service (DoS) attacks. The detection content covers fault tolerance and recovery capability. Fault tolerance indicates that the IDS can detect intrusions when being attacked. To put it another way, the DoS attack and other attacks can be tested at the same time. Recovery capability indicates that the IDS can detect intrusions after being attacked.

2. IDS Security Evaluation Based on DFA

2.1 Introduction to DFA

The Finite Automata Machine is an automatic recognition device. The DFA is a five-parameter model, namely \( M = (K, \Sigma, F, S, Z) \). \( K \) indicates a finite set, each element of which stands for a state of the current system. \( \Sigma \) indicates a collection of conditions. \( F \) indicates the single-valued mapping from the state transition diagram displays transition between states. Suppose that there are \( M \) state nodes and \( n \) transition conditions. Thus, the state transition diagram has \( M \) state transition nodes. The maximum out-degree of each node is \( n \), and each arc is marked with an input condition. Each state transition diagram has a unique start state node and multiple end state nodes.
The state transition condition is the attack function of system parameters that change during the attack. As the attack detection information accumulates, the attack function is instantiated. If the function return value is true and the system state changes, the attack goal is attained.

A large and successful intrusion is achieved through logical combinations of multiple attack functions. Commonly, logical combinations are formed among OR, AND, and SAND (and in sequence). C=A OR B indicates that the goal of attack C is achieved when the goal of attack A or B is achieved. C=A AND B indicates that the goal of attack C is achieved when the goals of attacks A and B are achieved. C=A SAND B indicates that the goal of attack C is achieved when the goals of attacks A and B are achieved in sequence. Figure 1-1 shows the logical combination of attack functions in DFA. Each node stands for a system state. A and B can be instantiated by specific attack functions.

![Logical combination of attack functions](image)

**Figure 1-1** Logical combination of attack functions

### 2.2 Application Example

The detection of an intrusion goal depends on the detection of multiple attack sub-goals. Relations between sub-goals can be OR, AND, and SAND. To facilitate reuse and simplify the attack mode, this paper describes the intrusion model building method based on the DFA.

The common security test based on the DFA is described as Figure 1-2:

![State of security evaluation based on the DFA](image)

**Figure 1-2** State of security evaluation based on the DFA

Si indicates the system state. For example, S0 and S1 indicate the normal state and the DoS attack state. S2 and S3 are the end states.

Ei indicates the attack function. For example, E1 indicates that data packets of DoS attacks are sent to the detected host, and E0 indicates the attacks to be tested.

### 2.3 Significance of IDS Security Evaluation Based on DFA

The original IDS security evaluation system has the following disadvantages:

- Direct attack test and log analysis are not flexible.
- The test at the subsequent step is unpredictable.

This paper proposes that the DFA should be applied to the IDS evaluation as an auxiliary analysis and processing technology, aiming to effectively improve performance and flexibility of the current system.
3. Multi-Level IDS Security Evaluation

3.1 Multi-Level Evaluation

Traffic per second refers to the traffic that flows through one node per second. It is a key indicator that shows the performance of the network intrusion detection system (NIDS), and is measured in Mbps.

The network adapter processes a finite number of data packets per second (pps). Generally, the processing capability of the network adapter is inversely proportional to the size of a data packet. In addition, the number of data packets that the network adapter can handle every second is limited. This paper puts forward the new idea of multi-level evaluation according to the features of data packets and attacks in the IDS security test.

Multi-level evaluation assigns credibility levels to the measures which are taken to make products meet basic requirements for functions, thus helping users judge whether information products are secure to their applications, and whether potential security risks are tolerable. Multi-level evaluation conducts independent vulnerability analysis. Based on the vulnerability analysis, the security test is performed to check whether the product is resistible to attacks from attackers with potential capability.

DoS attacks can be divided into multiple levels according to their types. On the basis of characteristics and particularity of DoS attacks, an appropriate size of data packet is specified at the start of the test. Therefore, it is unnecessary to modify the size of data packet during the test, and only the packet rate needs to be considered. The capability of the NIDS to capture packets is related to many factors. For example, if the packet size is 1500 bytes, the processing capability of the NIDS is 100 MB/s, or even more than 500 MB/s. If the packet size is 50 bytes, the traffic of 100 MB/s means 2000000 pps, which exceeds processing capabilities of most network adapters and switches. This paper aims to test the maximum processing capability of the 100 Mbps network adapter. The packet rates have three levels: 10 Mbps, 50 Mbps, and 100 Mbps. In this paper, the rate of 100 Mbps is the upper limit of the multi-level evaluation. The experiment results indicate that larger traffic of data packets have greater impact on the detection.

Figure 1-3 displays state transition of the multi-level security evaluation based on the DFA.

![Figure 1-3 State of multi-level security evaluation based on the DFA](image)

Si indicates the system state. For example, S1 indicate the normal state, S2, S3, and S4 indicate the DoS attack state, and S5, S6, S7 and S8 are the end states.

Ei indicates the attack function. For example, E1, E2, and E3 indicate that data packets of DoS attacks are sent to the detected host at the rates of 10 Mbps, 50 Mbps, and 100 Mbps respectively, and E0 indicates the attacks to be tested.

3.2 Significance of Multi-Level Evaluation

Currently, an increasing number of institutes conduct researches on IDS evaluation technologies. Each year witnesses new IDSs coming into being. Investors are eager to know practical effects and operation situation of the
When selecting IDS products, in addition to the detection scope and capabilities, users also pay great importance to security. To achieve certain level of security, users should consider what DoS attacks the IDS can resist, and what DoS attacks disable the IDS. Multi-level security detection can bring about credible and accurate results.


Figure 1-4 OSI reference model

The first challenge confronting the IDS evaluation is how to generate the evaluation data, namely generate the network data packet for the purpose of evaluating the IDS.

The IDS aims to detect attacks, which means that the attack detection rate is an important indicator. As far as the data set is concerned, the attack coverage is of great significance. It is unrealistic to add all known attacks to the data set because the work load will be overlarge; therefore, we must strike a balance between completeness and coverage. An effective solution to this issue is to classify attacks by a certain standard, and then select one or more representative attacks from each classification for test use.

Figure 1-44 shows the OSI reference model. The TCP/IP architecture consists of four layers: transfer layer, network layer, application layer (including application layer, presentation layer, and session layer), and network interface layer (including data link layer and physical layer).

The TCP/IP is the foundation on which the current Internet is built \cite{9,10}, and most data of the Internet is based on the TCP/IP. The TCP/IP-based network environment is the main consideration in the IDS evaluation technology.

Data can be added to the model to enhance flexibility and timeliness of the evaluation. The IDS security can be evaluated by mixing data of multiple layers. The data results from attacks of a single layer or multiple layers. The layer-based attack data is generated against the vulnerability of the TCP/IP. As a result, the test on each segment is simplified. Different evaluation data is generated at different locations and stages. Thus, attacks that do not exist on some specific networks come into being, and the disturbance to normal networks is reduced.

The attack data in evaluation is manually generated through analysis of vulnerability of the TCP/IP. The TCP/IP architecture consists of four layers: link, network, transfer, and application layers.

- Link Layer
  - Typical attacks at the ARP layer:
The attacker sends a deceptive ARP request and reply, pretending that it is host A on the LAN. The attacker changes the address mapping in the ARP cache of host B, and obtains the use rights of host A over host B. In the DoS attack, host A cannot receive data packets.

- **Network Layer**

  Typical attacks at the IP layer result from segment disassembling and restructuring.
  
  - If there is an overlap between two consecutive segments, the RFC791 stipulates that the data in the latter segment covers the data duplication in the former segment. Obviously, it is possible that the two packets that contain no intrusion information will generate intrusion information after restructuring.
  
  - If the former segment contains the latter one or vice versa, the repeated computation during the restructuring leads to the buffer overflow.
  
  - If, after restructuring, the IP packet length exceeds the maximum length, that is, 64 KB, defined by the IP, disorders occur to the IP assembling module.

- **Transfer Layer**

  Typical attacks at the TCP layer:

  The TCP/IP is vulnerable to the SYN Flood and LAND attacks. Generally, before an application in one system communicates with that in another system, three-way handshaking is required. Afterwards, the two systems can start to send and receive data. The SYN Flood attack sends a series of SYN packets to the attacked system. The system responds to each packet with a SYNACK packet, and waits for the ACK packet to be sent from the other system. However, the other system does not send the ACK packet. The SYNACK packets in the queue are deleted when they time out or the ACK packets are received. In the end, the attacked system fails to process requests from other users because the queue is full of SYNACK packets.

  The LAND attack sends to a series of SYN packets to a system on the network, and employs the IP spoofing technology to make the system believe that those packets are sent by itself. When the system processes those packets, it fails to respond to itself. Thus, the system breaks down.

- **UDP Attack**

  Compared with the TCP, the UDP is not reliable. The common attack against the UDP is port scanning. When the UDP message is sent to a disabled port, the message that the port is inaccessible is returned through the ICMP. Therefore, whether the ICMP message is returned indicates the enabling state of the specified port. As a result, the DoS attack is formed.

- **Application Layer**

  The attacks against the application layer are reflected by the fact that the message contains sensitive data or lacks certain data. For instance, though remote login is prohibited by the TELNET, characters "USER root" still exist in the message, which indicates that the root user logs in. However, the characters "OA", namely the carriage return, do not appear within a period after the command is executed. As a result, the buffer overflow attack is formed.

  Due to the hierarchical structure of the protocol, the attacks against the application layer lie in the data segment of the data packet, and the attacks against other layers are embodied in the header segment. The attackers attack a single layer or launch complicated or comprehensive attacks against multiple layers.

5. **Test Schemes**

  The method of testing the IDS through only software can save on hardware and enhance flexibility. The entire architecture consists of four modules, namely attack data packet module, three-level evaluation environment module, data packet control module, and tested IDS module. The data packet control module controls the forwarded quantity, type, and combination mode of data packets (DoS attacks or attacks to be tested).

  Since the first paper on the research of the intrusion detection, a large number of IDSs have emerged. This paper focuses on three typical IDSs, namely Snort[6-7], BlackICE PC Protection (Black-ICE PCP), and eTrust Intrusion Detection(eTrust ID). Figure 1-55 shows the layout of the test environment.
Figure 1-5 Work flow

Figure 1-5 shows the architecture of a new IDS security evaluation system. The evaluation system is manipulated by the main control module. The evaluation procedure is based on requirements of the test process. The main control module dispatches the simulation attack module and multi-level control module. Each module independently records the evaluation data that serves as the standards for evaluating the IDS test results. The aim of the IDS security evaluation is to identify attack events among a great amount of multi-level simulation attack events. Each simulation attack event is marked by the occurrence time and forwarded quantity, which is of great importance to the IDS. The main control module dispatches each sub-module as required. For example, the main control module decides on the types of attacks (optional) launched by the simulation attack module, and the level of the DoS attack module under which performance indicators and ability of detecting attacks of the IDS are tested. The multi-level control module controls three levels of DoS attack modules to test the detection ability of the IDS on each level. The simulation attack module provides original data for the IDS test by simulating actual attack processes and generating attack data. The evaluation module calculates performance indicators of the IDS by comparing IDS test results and data recorded by the data recording module, and presents the evaluation report that includes the detection rate and error rate.

During the IDS test, the intruder may launch diverse and simultaneous attacks against one target through multiple terminals. In order to simulate one or more intrusions in an authentic manner, this paper classifies the simulation as follows:

- **Single Intruder Single Terminal (SIST):** A single intruder attacks a single terminal or multiple terminals that are considered as one terminal logically. The terminal connects to the target host directly or through the network or dial-up connection.
- **Single Intruder Multiple Terminal (SIMT):** The intruder attacks the target host through multiple terminals, establishes various network connections to attack the target host, or mixes up or hides the intrusion.
- **Multiple Intruders Multiple Terminals (MIMT):** Multiple intruders attack the target host, and one or more intruders attack the target host in SIMT mode. The target host can be one computer or a computer network. The intruder may attempt to hide authentic attack behaviors in suspicious connections.
6. Summary

This paper elaborates on the IDS security test on the basis of defects of original evaluations. This paper comes to the following conclusions:

- Through combination of the DFA method and typical test cases, this paper describes the evaluation process in fragments, and thus takes advantages of state and process in the IDS evaluation. As a result, the test process is vividly and intuitively described, which facilitates further researches on both horizontal (detection scope) and vertical (detection depth) aspects of the IDS evaluation.

- The DoS attack to be tested falls into three categories according to the forwarding rate of the attack data packet. As the test results indicate, the impact on Snort imposed by most DoS attacks is proportional to the forwarding rate of the attack data packet, which assigns credibility levels to measures taken to make products meet basic requirements on functions, thus helping users judge whether information products are safe to their applications.

- Compared with the original security evaluation systems, the IDS security evaluation system in this paper has a wider detection scope that includes the link, network, transfer, and application layers of the TCP/IP, thus improving the original invariable evaluation mode and simplifying the process of adding test cases. Thus, the evaluation data can be added to the model on the basis of different layers, which reduces workload of capacity expansion and reflects the performance of the IDS in real time through the evaluation results.

Reference


