



Prerana Educational & Social Trust (R)

PES INSTITUTE OF TECHNOLOGY & MANAGEMENT

NH 206, Sagar Road, Shivamogga - Karnataka www.pestrust.edu.in/pesitm/

(An ISO 9001:2015 Certified Institution)



ISTE Faculty Chapter


**NATIONAL CONFERENCE ON ADVANCED RESEARCH IN
SCIENCE, ENGINEERING AND MANAGEMENT**

Certificate

This is to certify that Dr./ Mr./ Ms. Prashanth Kumar R. has participated /
presented / published a research paper titled MAC Address Randomization Implemented by IDS
in the National Conference on Advanced Research in Science, Engineering and Management held at
PES Institute of Technology & Management, Shivamogga, on 26th May 2018.


Dr. M.N. Hiremath
Convenor


Dr. Ashok Kumar
Principal


Smt. Arunadevi S.Y.
Joint Secretary, PESITM

MAC address randomization implemented by intrusion detection system

Author1:

Ashwini.E.M

CSE Department

PESIAMS, Shimoga

Mail: ashwini.em@gmail.com

Author2:

Sunil M.E

CSE Department

PESITM, Shimoga

sunil.mghalli@gmail.com

Author3:

Prashanth kumar R

CSE Department

PESIAMS, Shimoga

prasha1988@gmail.com

Abstract : In computer networking, the Media Access Control (MAC) address is a unique value associated with a network adapter. They allow computers to uniquely identify themselves on a network at this relatively low level. Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses *vulnerability assessment* (sometimes referred to as *scanning*), which is a technology developed to assess the security of a computer system or network. In this paper, suggested data encryption technique is presented by using the MAC address as a key that is used to authenticate the receiver device like PC, mobile phone, laptop or any other devices that is connected to the network. Media Access Control (MAC) address randomization mechanism used to protect the users' privacy. An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Whenever the intruder occurs, admin can look after who all are the intruders occurred and at what time. Admin can see the user name and password from which the intruder is trying to access the system. Admin gets the IP and MAC address of the intruder

1 INTRODUCTION

Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks

from within the organization). MAC addresses are also known as hardware addresses or physical addresses. TCP/IP and other mainstream networking architectures generally adopt the OSI model. MAC addresses function at the data link layer (layer 2 in the OSI model).

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Tremendous growth and usage of internet raises concerns about how to protect and communicate the digital information in a safe manner. Nowadays, hackers use different types of attacks for getting the valuable information. Many intrusion detection techniques, methods and algorithms help to detect these attacks. Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources, and uses alarm filtering techniques to distinguish malicious activity from false alarms.

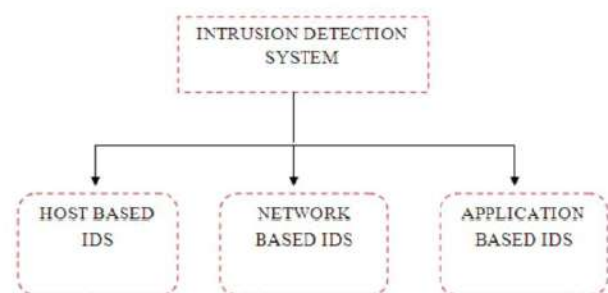


Figure 1.1 -TYPES OF INTRUSION DETECTION SYSTEM

There is a wide spectrum of IDS, varying from antivirus software to hierarchical systems that monitor the traffic of an entire backbone network. The most common classifications are network

intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS). A system that monitors important operating system files is an example of a HIDS, while a system that analyses incoming network traffic is an example of a NIDS. It is also possible to classify IDS by detection approach: the most well-known variants are signature-based detection (recognizing bad patterns, such as malware) and anomaly-based detection (detecting deviations from a model of "good" traffic, which often relies on machine learning). Some IDS have the ability to respond to detected intrusions. Systems with response capabilities are typically referred to as an intrusion prevention system.

1.1 Objective

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Whenever the intruder occurs, admin can look after who all are the intruders occurred and at what time .Admin can see the user name and password from which the intruder is trying to access the system. Admin gets the IP and MAC address of the intruder

1.2 Overview

Here we use several parameters to detect the intruder. The parameters are IP address, MAC address, username and password. If any unauthorized person try to access the data then his IP address and MAC address is fetched and it is informed to the admin. An intruder gets alert tone when he tries to access the data. The whole concept is divided into 3 modules.

First module is server module will be composed to handle many users at a time and also be able to store the data at their storage devices. This module will handle the requests of all the users of the system and response with the result. Second module is client module will be connected with the server and send request to the servers, the users of the system will communicate with other users of the system through the server.

Third module is database module , this module will be responsible for storing the data of all the

users and produces the data as the user's requirements.

Fourth module is virtual host, this module is a part of cloud virtual system here we will place our data using MySQL server which is maintained at virtual host. The security is give more to this system which is shielded by the local server which allows only authorized persons to access the database.

2. LITRATURE SURVEY

Intrusions in an information system are the activities that may be harmful to the security and functioning of the system, and intrusion detection is the process used to identify intrusions. Due to the limitations of information security and software engineering practice, computer systems and applications may have design flaws or bugs that could be used by an intruder to attack the systems or applications. So, in an effort to tackle these scenarios IDSs were developed as second line of defense. However, the ability to create solid rules based on clustering of packet signatures and their proper categorization is not much explored.

The need for intrusion detection systems began way back in 1980s when James P. Anderson published a study outlining ways to improve computer security auditing and surveillance at customer sites. The original idea behind automated ID is often credited to him for his paper on "How to use accounting audit files to detect unauthorized access". This ID study paved the way as a form of misuse detection for mainframe systems. Since then a lot of algorithms and frameworks have been proposed to tackle intrusion detection with each approach having its own advantages and disadvantages.

One of the classifications of TDSs is

1. Network-based IDS in which system is placed at an important endpoint in a network segment and

2. Mainframe-based IDS which is mainly used to analyse and determine the login file of a mainframe or a system.

There are two major methods to detect intrusions in computer networks;

1. Based on the network intrusion signatures, and
2. Based on the detection of anomalies on the network In this paper, we attempt to enhance the signature based intrusion detection by applying the concept of clustering and fuzziness by extracting features out of a network packet and test it against the generated signature database for the signs of intrusion. This gives a proper categorization of network packet as per its severity.

Several techniques are available in the literature for detecting the intrusion behaviour. In recent times, intrusion detection has received a lot of interest among the researchers since it is widely applied for preserving the security within a network. Here, we present some of the techniques used for intrusion detection.

Intrusion Detection System (IDS) researchers have been biased in constructing systems that are difficult to handle, lack insightful user interfaces and are inconvenient to use in real-life circumstances. The proposed adaptive expert system has utilized fuzzy sets to find out attacks. The expert system comparatively easy to implement when used with computer system networks has the capability of adjusting to the nature and/or degree of the threat. Experiments with Clips 6.10 have been used to prove the adjusting capability of the system. Alok Sharma have focused on the use of text processing techniques on the system call sequences for intrusion detection. Host-based intrusions have been detected by introducing a kernel based similarity measure. Processes have been classified either as normal or abnormal using the k-nearest neighbor (kNN) classifier. They have assessed the proposed method on the DARPA-

1998 database and compared its operation with other existing methods present in the literature.

2.1 EXISTING SYSTEM

In existing system the intruders are avoided by the using the applications by setting the password authentication and pattern matching etc. but these can be extracted using various methods. It is easy to use the application if they identify the password or the pattern. There is a lack of security in the network where the applications are used in sensitive areas.

LIMITATIONS OF EXISTING SYSTEM

1. The intruder can use the application in intruders system and can easily access the application and can hack the data.
2. No security locks for non-users of the application.

2.2 PROPOSED SYSTEM

The proposed system will use several parameters to detect the intruder. The parameters are IP address, MAC address, username and password. If any unauthorized person try to access the data then his IP address and MAC address is fetched and it is informed to the admin. An intruder gets alert tone when he tries to access the data.

ADVANTAGES OF PROPOSED SYSTEM

- Admin will get to know username and password which is tried to access the system.
- Admin can look when the intruder occurred.
- The IP and MAC address avoids the intruder from accessing the system.
- Intruder gets alert tone in his system when he tries to access.

3. SYSTEM DESIGN

It describes about the requirements of the system like functional, non-functional requirements,

software requirements, modules, use case diagram and activity diagram of the systems.

3.1 MODULES:

- **Server Module:**

Server Module will be composed to handle many users at a time and also be able to store the data at their storage devices. This module will handle the requests of all the users of the system and response with the result.

- **Client Module:**

Client module will be connected with the server and send request to the servers, the users of the system will communicate with other users of the system through the server.

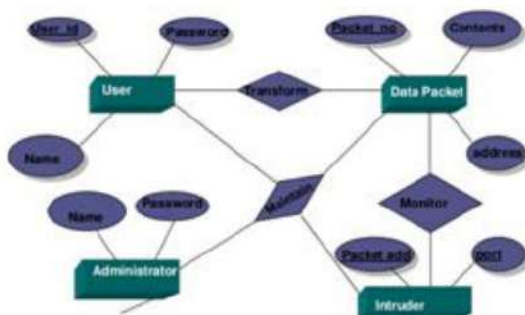
- **Database Module:**

This module will be responsible for storing the data of all the users and produces the data as the user's requirements.

- **Virtual Host Module:**

This module is a part of cloud virtual system here we will place our data using MySQL server which is maintained at virtual host. The security is give more to this system which is shielded by the local server which allows only authorized persons to access the database.

ENTITY RELATIONSHIP DIAGRAM



3.2 SYSTEM ARCHITECTURE : A system architecture or systems architecture is the conceptual model that defines the structure, behaviour, and more views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviours of the system.

A system architecture can comprise system components, the expand systems developed, that will work together to implement the overall

system. There have been efforts to formalize languages to describe system architecture, collectively these are called architecture description languages.

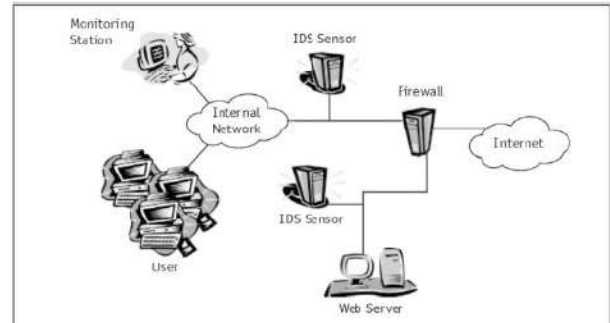


Figure 3.2- SYSTEM DESIGN OF IDS

The user's that is the admin and officer are connected through internet to access the data where a check for intruder is made before allowing the users to access the data. If user is identified as an intruder than he is not allowed to access the data.

3.3 DATAFLOW DIAGRAM:

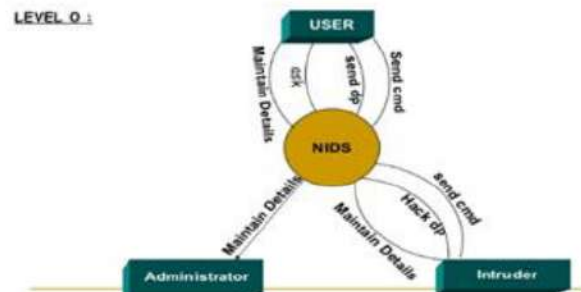


Figure 3.3 - level 0 data flow diagram

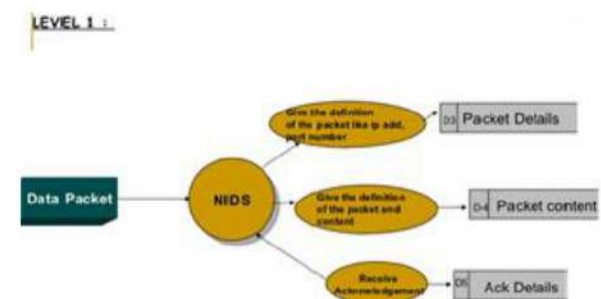


Figure 3.3.1- level 1 data flow diagram

3.4 Class Diagram for Interaction between Admin and Analytical Server

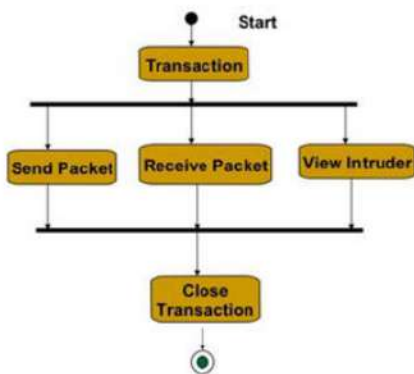
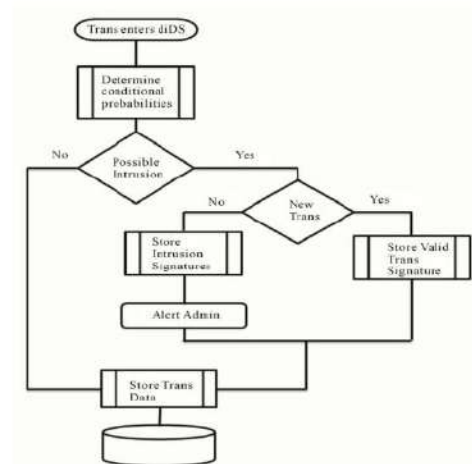


Figure 3.4- class diagram

3.5 FLOW CHART:



4. TYPES OF TESTING USED :

1. White box Testing
2. Black box Testing

4.1 White box testing

White Box Testing is testing in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is used to test areas that cannot be reached from a black box level.

4.2 Blackbox testing

Black Box Testing is the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definite source document, such as specification or requirements document. It is

testing in which the software under test is treated, as a black box, you cannot "see" into it. The test provides input and responds to outputs without considering how the software works.

4.2.1 Integration test

Integration tests are designed to test integrated software components to determine if they actually run as one program. Testing is event driven and is more concerned with the basic outcome of screens or fields. Integration tests demonstrate that although the components were individually satisfaction, as shown by successfully unit testing, the combination of components is correct and consistent. Integration testing is specifically aimed at exposing the problems that arise from the combination of components.

The task of the integration test is to check that components or software applications, e.g. components in a software system or - one step up - Software applications at the company level -- interact without error.

4.2.2 Function test:

Functional tests provide systematic demonstration that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

4.2.3 System Test:

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

4.3 TEST RESULTS

All the test cases mentioned above passed successfully. No defects encountered.

5. RESULTS AND DISCUSSION



Fig 5.1: Admin need to provide login credentials to get login into the system



Fig 5.2: The admin can view username, password, IP address with date and of an intruders who are trying to access the system.



Fig 5.3: Intruder Detected when the officer is not logged in form the respective IP address.

6. CONCLUSION

Intrusion Detection System we identified the intruder and alert the admin whenever an intruder occurs, it provides security for the data and avoids the intruder from accessing the data. Admin will get to know username and password which is tried to access the system and take protect the data. Admin can also see that when the intruder occurred. The IP and MAC address avoids the intruder from accessing the system. Intruder gets alert tone in his system when he tries to access.

7. FUTURE ENHANCEMENT

In this paper we have implemented a system which can detect the intruder who is trying to enter into our server. We have used only IP and MAC address of the client and the user credentials to identify the intruder.

But in future we can enhance by implementing more security issues such as face detection and figure print detections which will give more security for the server from the intruders. Anomaly based and misuse detection can be used for detecting the intruder in network traffic. And also send message to admin to his cell phone.

8. REFERENCES

1. Jonathan Cornabas, Formalisation de propriétés de sécurité pour la protection des systèmes d'exploitation, soutenue le : 02 Décembre 2010 pour obtenir le grade de : Docteur de l'université d'Orléans
2. TCSEC (1985). Trusted Computer System Evaluation Criteria. Technical Report DoD 5200.28-STD, Department of Defense.
3. Network Intrusion Detection System (NIDS), 978-0-7695-3267-7/08©2008 IEEE DOI 10.1109/ICETET.2008.252
4. https://en.wikipedia.org/wiki/Intrusion_detection_system
5. <https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids>
6. <https://www.sans.org/.../detection/intrusion-detection-systems-definition-challenges-34>
7. A New Vision for Intrusion Detection System in Information Systems, Science and Information Conference 2015 July 28-30, 2015 | London, UK
8. Classification of Intrusion Detection System (IDS) Based on Computer Network, 2017 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE).

9. NIDS: A network based approach to intrusion detection and prevention, 2009 International Association of Computer Science and Information Technology - Spring Conference.

10. A Novel Approach for the Design of Network Intrusion Detection System(NIDS), 2013 International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS).