International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 24 (2017) pp. 14108-14113


# Secure Communication Based On Authentication Techniques Using NIDS

**P.Thangavel**
*Research Scholar, Department of Computer Science,*
*Bharathiar University, Coimbatore, Tamil Nadu, India.*

*Orcid Id: 0000-0002-7401-788X*

**Dr. A. Senthil Kumar**
*Assistant Professor, Department of Computer Science,*
*Tamil University, Thanjavur, Tamil Nadu, India.*

*Orcid Id: 0000-0003-0707-016X*

**Abstract**

Network security plays a vital role as everything is being digitized and millions of people use the internet for personal and professional works. As the usage of internet has increased, several other threats have also risen drastically. Securing such network is essential because the data transferred over the network must be protected in this digital era. Authentication technique is the process of allowing users to communicate in the network after verifying who they are. Network Intrusion Detection System (NIDS) monitors the network traffic and detects the malicious activities. In this research, we have discussed how authentication techniques and Network Intrusion Detection System (NIDS) help to improve the security of information in the network.

**Keywords:** Authentication, Denial of service, Anomaly detection, Network Intrusion Detection System, SNORT tool

## INTRODUCTION

Network Intrusion detection system can be described as the process of identifying and taking necessary actions against malicious activities targeted to network and computing resources. A network intrusion detection system should continuously monitor the traffic crossing the network and compare with a previously known set of malicious activities or look for statistical deviation of the system under surveillance from its normal behavior. Aim of network security is to protect the device from unauthorized and potentially harmful activities such as denial of service attacks, port scans or attempt to crack into computers by monitoring network traffic. Network connected devices are very often susceptible to exploitation. The Intrusion detection system placed in the network should be able to sense the unusual activity and alert the administrators. A set of well defined rules E.g, Snort and Bro are used to identify network events that are other than expected.

In this digital era more and more people becoming active on the Internet for their personal and professional, because of this internet is growing rapidly. But, along with the evolution of Networking and Internet, several threats such as Denial-of-Service (DOS) attacks and Trojan Horses have also risen drastically. So the task of securing the Internet or even the Local Area Networks is now at the forefront of computer network related issues. Being on public network, serious security threats can be posed to individual‟s personal information and also to the resources of companies and government. Providing confidentiality, maintaining integrity and assuring the availability of correct information are the primary objectives. These threats are primarily present due to the ignorance shown by the users, weak technology and poor design of the network. Sometimes there are many network services that are enabled by default in a personal computer or a router. Out of which many services may not be necessary and may be used by an attacker for information gathering. So it is better to disable these unwanted services to protect them from hackers and crackers More importantly, not only need to be concerned regarding the security at each end of the network rather the focus should be on securing the entire network. Recently a financial transaction value which leads to the carrying Internet which uses Wipro networks is activated for the government, the security company and the bank, financial institution etc.

Network security plays a vital role as everything is being digitized and millions of people use the internet for personal and professional works. As the usage of internet has increased, several other threats have also risen drastically. Securing such network is essential because the data transferred over the network must be protected in this digital era. Authentication technique is the process of allowing users to communicate in the network after verifying who they are. Network Intrusion Detection System (NIDS) monitors the network traffic and detects the malicious activities. In this research, we have discussed how authentication techniques and Network Intrusion Detection System (NIDS) help to improve the security of information in the network.

While developing a secure network, the following need to be considered –

**1. Access** – Only authorized users are allowed to communicate to and from a particular network.

**2. Authentication** – This ensures that the users in the network are who they say they are. Actual flow of information can start only after the user has been authenticated and allowed to communicate to other systems in the network.

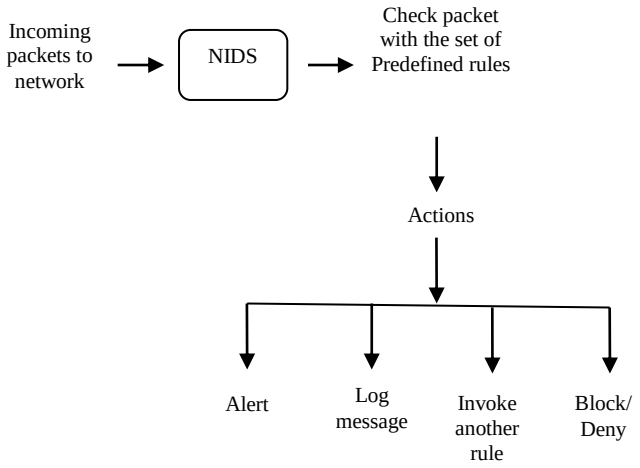
**3. Confidentiality** – Data in the network remains private. This is done to ensure that the information can be viewed only by authenticated systems and it can be achieved using various

**4. Integrity** – This ensures that the message has not been changed during transmission.

**Table 1:** Different types of attacks on Network/Data

| Attacks types | Description |
|---|---|
| Weak password recovery | Websites permit hackers to find a way to illegally obtain, modify or recover another user's password. |
| Brute force attacks | By trial and error, hackers can guess username, password, debit cards numbers, etc. This technique is highly popular |
| Insufficient authentication | Some websites don't authenticate much so hackers attack sensitive content |
| Shoulder surfing attacks | Hackers directly observe user while typing passwords or by some hidden cameras. |

## ARCHITECTURE




## DATA SECURITY AND AUTHENTICATION

Data Security is a challenging issue in the field of data communications. For securing information from hackers and crackers, authentication is the major phase in network security. It is a concept to protect network and data transmission over wired as well as wireless networks. Authentication is one of the primary techniques of ensuring that the person who is transmitting the information is whom he says he is. It is thus the process of determining the actual identity of users, systems or any other entity in network. To verify someone's identity, password is mostly used. To authenticate user or machines, different techniques can be used to perform authentication between user and machine or machine and another machine too.

## METHODS

Several techniques have been developed for building secure network. Many organizations around the world spend millions of revenue to safeguard their information. In the existing system where Network Intrusion Detection System (NIDS) as early warning system the disadvantage is that it detects those malicious activities that are blocked by firewall. Our proposal overcomes this disadvantage by adding the set of rules in firewall to NIDS rule set after removing the anomalies in firewall rule set. By doing so, we block and deny the packets in NIDS itself which saves us from the cost of adding firewall to the network. The time taken by NIDS to match the packet with its rule set is reduced as we are adding the rules only after removing the anomalies. Also we introduce one more action in SNORT rule set i.e. deny/block to drop the packet at NIDS itself. The aim of this research is to reduce the deployment cost and also the time taken for monitoring the traffic.

This research work initially manages the firewall policies which is a challenging task due to the complex nature of rules. After resolving anomalies in firewall rule set we can add these rules to the NIDS rule set. The following is the nature of work involved in this research.

### A) Authentication Phase

Anyone of the authentication techniques among the Password based, Token based and Biometric based or a combination of those techniques can be used for authentication.

#### i) Login

User must login using their credentials before they can continue to use the network.

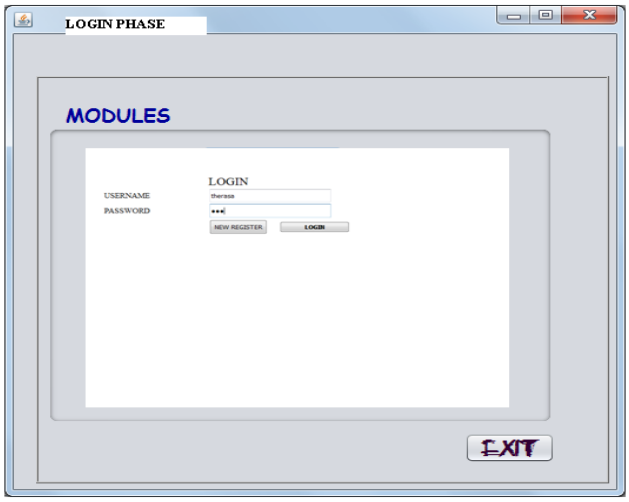



**Figure 4.1** Login Phase

### ii) Registration

If the user is not already registered, they must register themselves so that they will be allowed in the network.

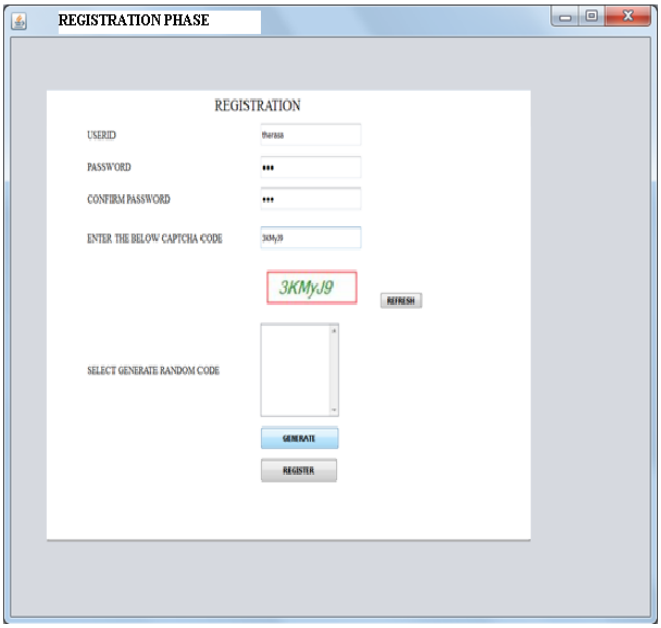



**Figure 4.2** Registration Phase

## B) Anomaly Detection Phase

### i) Conflicting rules

A conflict occurs when two rules overlap with each other. Using Rule Based Segmentation the packets are classified as overlapping segments, non overlapping segments. Overlapping segments is again classified into conflicting and non-conflicting segments.

Non overlapping segments contain the unique rules and overlapping segments contains the rules which are intersecting. Under that the conflicting segments contain the intersecting rules which perform different actions and non-conflicting segments (CS) contain the rules which perform the same action.

**Algorithm 1:** Rule based segmentation technique

Input: R – Set of rules

Output: S – Set of segments

For each ‘r’ in R do,

If ‘IP’ of r equals r.next then

If ‘action’ of r equals r.next then

$S_{CS}$ ← r, r.next

Else

$S_{NCS}$ ← r, r.next

Else

$S_{NOS}$ ← r, r.next

End

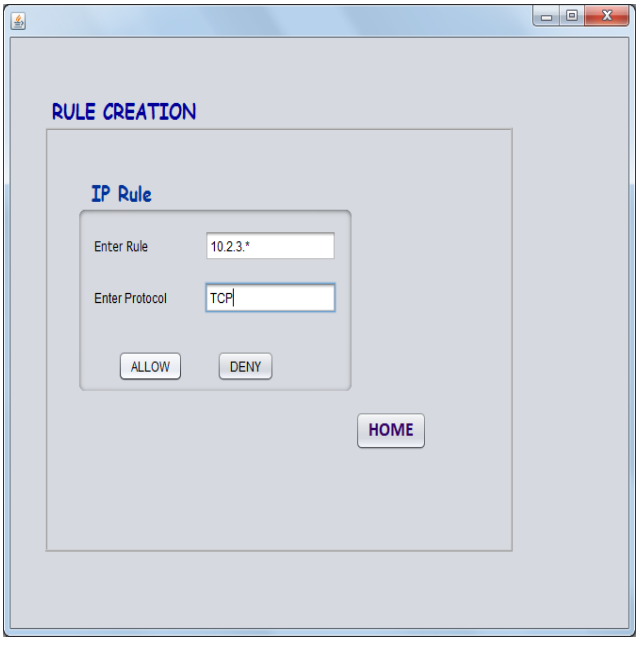



**Figure 4.3** Rule Creation Phase

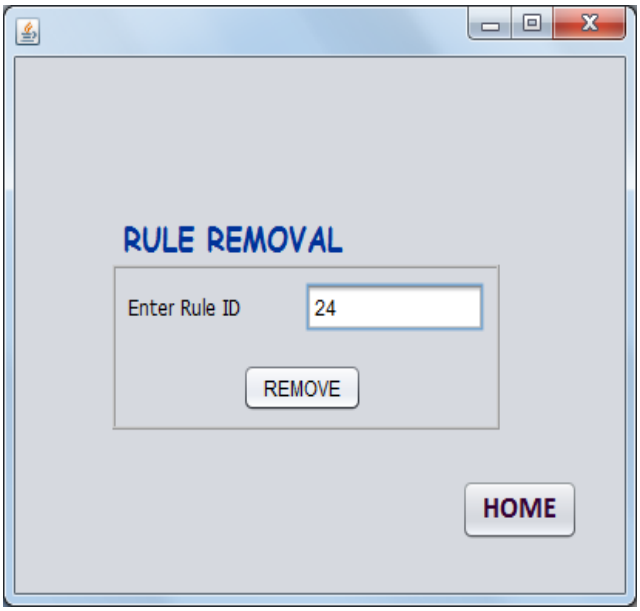



**Figure 4.4** Rule Removal Phase

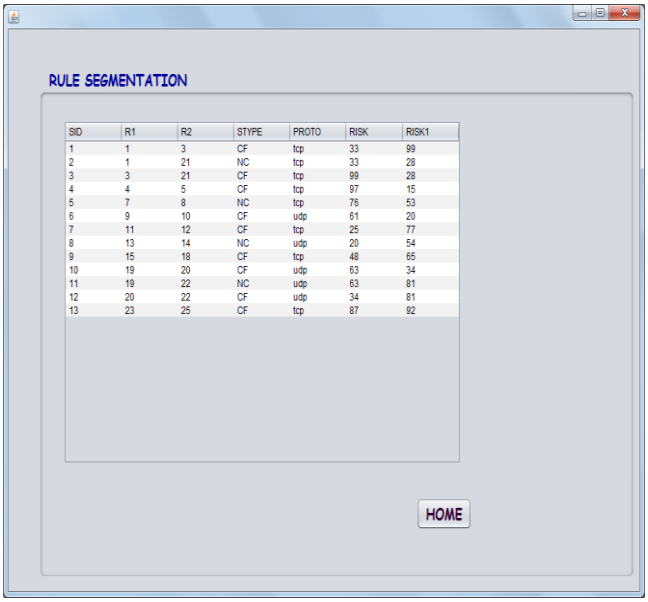



**Figure 4.5** Rule Segmentation Phase

### ii) Risk value

After the anomalies are detected among the multiple rules we then calculate the risk values of those rules. Then the administrator can decide whether to allow or deny the rule.

**Risk Value = CVSS Base Score * Importance Value**

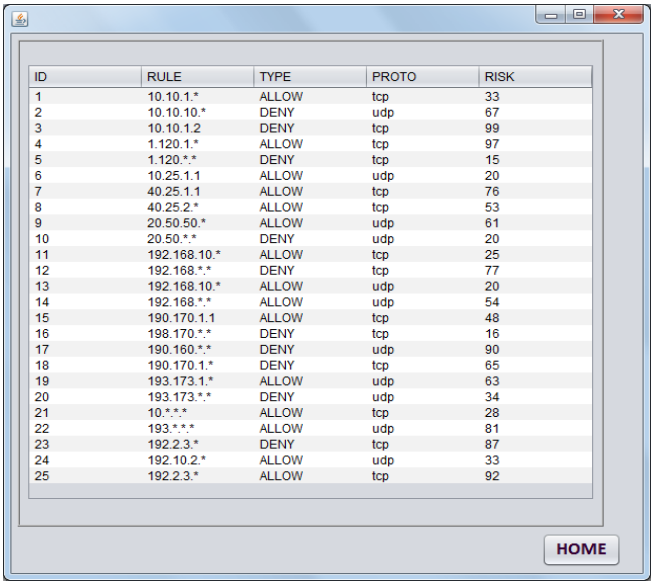



**Figure 4.6** Rules with Risk Value Phase

### iii) Rule reordering

The rules can be reordered by considering which rule should take precedence over other rules. Reordering rules is done based on a combination of greedy and permutation algorithm.

**Algorithm 2**: Greedy and Permutation

Input: CS – Set of conflicting segments
Output: G – Set of groups, S – Set of reordered conflicting segments

For each s in CS,
  If s is a subset of Gs then
    Gs ← s
End

For each g in G,
If no_of_segments(g) < 100
  P ← no_of_rules(g)!
  For each p in P,
    Reorder the position of rules in 'g'
    Find the Resolved Conflicts (RC)
  End
  Select permutation with max(RC)
 Else
  Find RC for each rule in 'g'
  Select rule with greatest RC
  Move rule to new position
  Repeat this for all rules in 'g'
End

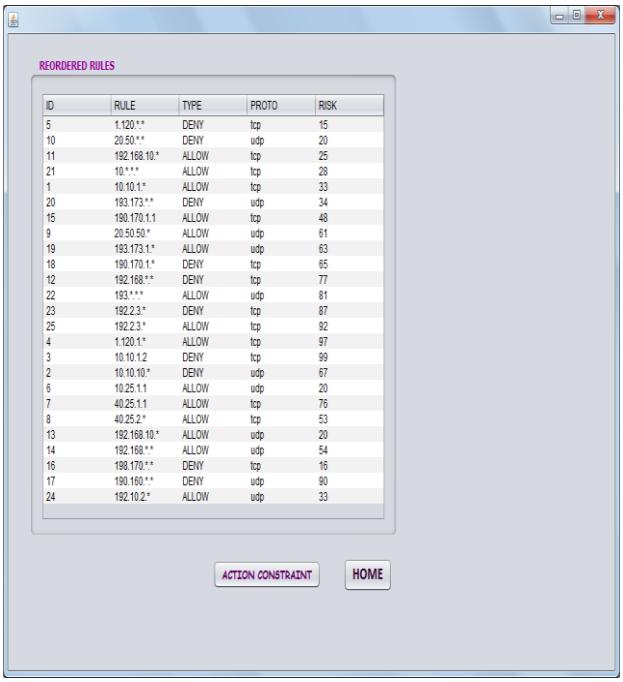



**Figure 4.7** Rules Reordering Phase

### C) NIDS Rule Phase

We are using the software based NIDS approach which relies on Snort rule set. SNORT is a cross platform, light weight network intrusion detection tool that can be deployed to monitor small TCP/IP networks and detect a wide variety of suspicious network traffic as well as attacks.

The basic structure of SNORT rule is as follows

| Rule Header | Rule Options |
|---|---|

Rule Header – Consists of information for matching a rule against packets

Rule Options – Consists of information about alert message

The structure of SNORT Rule Header is as follows

| Action | Protocol | Address | Port | Direction | Address | Port |
|---|---|---|---|---|---|---|

**Action** – alert, log message and invoking other rule. We add one more action in our research i.e. deny/block

**Protocol** – IP, TCP, UDP, ICMP

**Address** – Source and destination address

**Port** – Source and destination ports for TCP, UDP

**Direction** – Specifies which one is source or destination port and address

#### i) Adding rules

After resolving all the anomalies, we add each rule to SNORT rule set. There won't be any conflicts since it has all been handled earlier.

#### ii) Blocking packets

In action part of SNORT Rule Header, we add one more action deny/block. By doing so, the packets can get denied there itself which reduces the work or eliminates presence of firewall in the network.

When packet enters the network, compare it with the SNORT rule set. If there is no match, packet enters the network. When match occurs and the action of the rule states 'Alert', the alarm starts to ring to alert the user. When action states 'Log message', the message is just logged in file/terminal. If action is 'Invoke another rule', it calls another rule and if action is 'deny/block' the packet gets dropped.

### RESULT

The following table shows the time taken and Resolved Conflicts (RC) for permutation, greedy algorithm and the result when a combination of both is used to detect packet conflicts with respect to time.

**Table 2:** Algorithm Analysis

| Group | CS | Permutation | | Greedy | | Permutation and Greedy | |
|---|---|---|---|---|---|---|---|
| | | RC | Time (s) | RC | Time (s) | RC | Time (s) |
| 1 | 4 | 4 | 0.759 | 3 | 0.498 | 4 | 0.743 |
| 2 | 5 | 4 | 0.789 | 3 | 0.528 | 4 | 0.789 |
| 3 | 8 | 7 | 0.923 | 6 | 0.758 | 7 | 0.897 |
| 4 | 14 | 12 | 1.976 | 9 | 1.257 | 11 | 1.754 |
| 5 | 20 | 18 | 3.734 | 15 | 1.538 | 17 | 2.897 |

The performance analyses used in this research are the time, cost and maintenance features by comparing it with the existing approach.

**Table 3:** Performance Analysis

| Performance characteristics | Existing System | Proposed System |
|---|---|---|
| Time | Less | Very Less |
| Cost | Deployment cost is less | Cost is reduced as NIDS takes care of the work of firewall |
| Maintenance | Easy to update | Very easy to update as there is no need to maintain firewall |
| Advantage | Single point of deployment | Malicious activities can be blocked by NIDS itself eliminating need of firewall |

The following graph captured using SNORT tool shows the captured and dropped packets with respect to time.

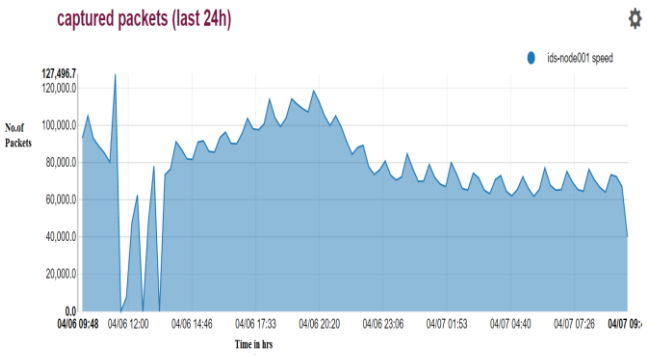



**Figure 5.1** Captured Packets (Last 24 hrs)

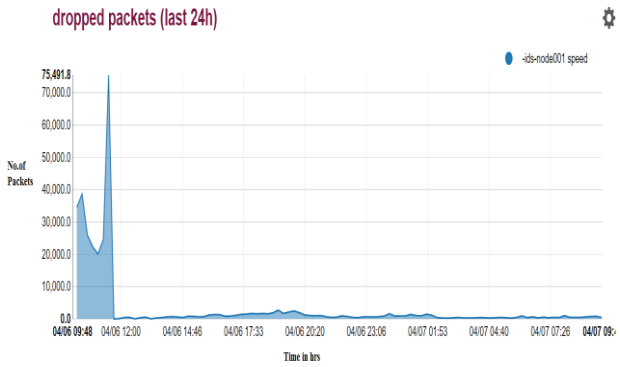



**Figure 5.2 Dropped Packets (Last 24 hrs)**

## CONCLUSION AND FUTURE WORK

Network security can be maintained by making use of various authentication techniques. The demand for a secure network is ever increasing. One central challenge with network security is the determination of the difference between normal and potentially harmful activity. The ultimate aim of a Network Intrusion Detection System (NIDS) is to develop an automated and adaptive tool for network security.

In future, still more techniques can be combined together with NIDS to provide a more secure network as the usage grows day by day. Every system has its own pros and cons; it depends totally on how the technique is used to get maximum efficiency.

## REFERENCES

[1] Lawrence O"Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", Vol. 91, No. 12, Dec. 2003, pp. 2019-2040 ã 2003 IEEE.

[2] Hafiz Zahid Ullah Khan, "Comparative Study of Authentication Techniques", IJVIPNS-IJENS Vol: 10 No: 04.

[3] [Online]Available:http://www.authenticationworld.com/Token-Authentication.

[4] [Online]Available:http://www.authenticationworld.com/Authentication-Biometrics.

[5] Jae-Jung Kim and Seng-Phil Hong, "A Method of Risk Assessment for Multi-Factor Authentication", Journal of Information Processing Systems, Vol.7, No.1, March 2011.

[6] Qinghua Li, Student Member, IEEE, and Guohong Cao, Fellow, IEEE "Multicast Authentication in the Smart Grid with One Time Signature", IEEE TRANSACTIONS ON SMART GRID, VOL. 2, NO. 4, DECEMBER 2011.

[7] [Online]Available: http://www.duosecurity.com.

[8] [Online]Available:http://ids.nic.in/technical_letter/TNL_JCES_JUL_2013/Advance%20Authentication%20Technique.pdf.

[9] Stamati Gkarafli, Anastasios A. Economides, "Comparing the Proof by Knowledge Authentication Techniques", international Journal of Computer Science and Security (IJCSS), Volume (4): Issue (2).

[10] Roger Meyer, "Secure authentication on the internet"As the part of security reading room, SANS institute 2007.