IMPROVISATION OF SECURITY AND ENERGY OVER A NETWORKING SYSTEM

R. Meena[1], V. Perumal[2]
[1]Department of Computer Science and Engineering, Saveetha Engineering College, Chennai, India
[2]Department of Computer Science and Engineering, Research scholar at Anna University, Working as an Associate Professor in Saveetha Engineering College, Chennai, India

Abstract— **Denial of Service attacks remain a major security problem in the networks and its difficult to detect malware activities where the attacks can send the virus data alone with original data which is to be Encrypted in turn leads to system crush. Intrusion Detection methodologies are used to reduce the malware activities. In Networking, protection against the above lines of attacks consume energy and increases the traffic, the need for the intrusion detection grows in step to reduce the intrusion detection and diagnosis. Homo Blowfish is derived from the combination of the Advance Encryption Standard and blowfish for increasing performance encryption and security. A Network Anomaly Detection Algorithm is proposed to overcome the traffic flow in a network.**

Index Terms— **Network Sniffer, Security, Encryption, Homo blowfish algorithm, Traffic Flow Identification.**

I. INTRODUCTION

A Network is the inter-connection of communications media and electronic devices for sharing data and resources. Security means safety or safekeeping, protection or well-being. Network Security refers to any undertaking designed to protect the network. Users will assign an ID and password to access the information and programs within their authority. Unwanted intrusions can be protected from computer system and network. A specialized field in computer networking that involves caring a computer network infrastructure. Specifically, these activities protect the usability, reliability, integrity, network and data. The main goal of the Network security to stops the variety of threads from entering and spreading on network. [1] Network security is handled by a network administrator and system administrator and implements the security policy. A well good software and hardware is required to protect a network and the resources can access from unauthorized access and ensure that employees have adequate access to the network and resources to work. [8] Cyber-physical systems it's used to operate reliably in the face of unforeseen failures and external malicious attacks. In this, mathematical framework is designed for identification monitors and distributed attack detection, [6] when the data is transferred between the source and sink, it undergoes certain security checks before reaching the sink .The data format is analyzed and encrypted, and this data in turn is checked by the security checker for any malware attack. The rate of false alarm is very high, [9] Deep Packet Inspection it is a key component in network intrusion detection systems and deployed to detect attacks and viruses in Internet traffic based on patterns stored in a database. [4] All packets in the incoming data stream are compared with patterns in an attack database, byte-by-byte, using string matching and regular expression matching. [2] Sensor failure could degrade the systems performance and possibly lead to total system failure. The impact of the failure depends on the application domain. In safety critical applications, any failure could result in damage to property and environment, result in loss of life, [5] Peer-to-peer networking has the potential of providing wide channels for file exchange. At the same time, Peer-to-Peer is prone to the proliferation of viruses. Peer trust reputation can be used to prevent virus dissemination, [3] Non-interactive zero-knowledge proof scheme is proposed for secure identification in wireless networks, and it uses a timed transfer technique to enable a single verifier to identify multiple provers. The verifier and the synchronization are not needed for prover.

This paper is proposed to find the malware activities and classifies the category according to level. Traffic flow is controlled by using Network Anomaly Detection Algorithm.

II. HOMO BLOWFISH

Homo blowfish is a variable-length key, 64-bit block cipher. The algorithm consists of two parts: a key-expansion part and a data encryption part. Key is used to convert a key of 448 bits into 4168 bytes.

Data encryption occurs through a Feistel network 16-round. Each round will have a key-dependent permutation, and a key- and data-dependent substitution. Every operation will be XORs and 32-bit words on additions. The only additional operations are four indexed array data lookups per round.

Subkeys:

HomoBlowfish uses a large number of subkeys. These keys must be precompiled before any data encryption or decryption.

1. The X-array consists of 18,32-bit subkeys:
   X1,X2,X3,….,X18.

2. There are four 32-bit Z-boxes with 256 entries each:
   Z1,0, Z1,1,..., Z1,255;
   Z2,0, Z2,1,..,, Z2,255;

ISSN: 2278 – 1323

All Rights Reserved © 2016 IJARCET

Z3,0, Z3,1,..., Z3,255;
Z4,0, Z4,1,..,, Z4,255.

These method used to calculate these subkeys in future will be described.

A. Data Encryption and Decryption using Homoblowish

Encryption:

- Homo blowfish is a Feistel network consisting of 16 rounds. The input is a 64-bit data element, x.

```
x can be divided into two 32-bit halves, i.e xL, xR
For i = 1 to 16:
xL = xL XOR Pi
xR = F(xL) XOR xR
Swap xL and xR
Next i
Exchange  xL and xR
xR = xR XOR P17
xL = xL XOR P18
Recombine xL and xR
Function F
```

xL can be divided into four eight-bit quarters, i.e a, b, c, and d

F(xL) = ((S1,a + S2,b mod 2^{32}) XOR S3,c) + S4,d mod 2^{32}

- Decryption is exactly the same as encryption, except that X1, X2,X3,..., X18 are used in the reverse order.
- Implementations of Homo blowfish it needs the speeds to unroll the loop and assuring that all subkeys are stored in cache.
- Generating the Subkeys:

The subkeys are calculated using the Homo blowfish algorithm. The exact method is as follows:

1. P-array is initialized first and it takes the four S-boxes with a fixed string. String has hexadecimal digits with pi and it should be less the initial 3.

```
P1 = 0x243f6a88
P2 = 0x85a308d3
P3 = 0x13198a2e
P4 = 0x03707344
```

2. XOR as P1 and having the first 32 bits of the key, XOR as P2 and the second 32-bits of the key, and so on for all bits of the key. Cycle should repeat through the key bits until the entire P-array has been XOR with key bits.
3. All-zero string can be encrypted with the Homo blowfish algorithm.
4. P1 and P2 can be replaced by using the output of step (3).
5. Encrypt the output of step (3) using the Homo blowfish algorithm with the modified subkeys.
6. Replace P3 and P4 with the output of step (5).
7. Continue the process, P- array can replace all entries and four S-boxes in order, with the output of the continuously-changing Homo blowfish algorithm.

- In total, 521 iterations are required to generate all required subkeys. Subkeys are stored in the applications rather than execute the derivation process multiple times.

B. Network Anomaly Detection Algorithm

This algorithm is used to detect the traffic flow while the document is transferred from source to destination. Network Anomaly will direct the traffic flow during the encryption of the document. It does not allow the more documents at a time so that traffic will not occur. The purpose this algorithm is used to detect and classify the traffic anomalies.

III. PROPOSED ARCHITECTURE DESGIN

In this section, we introducing the architecture design to handle the malware activities and to control the traffic flow. In the System Architecture Client/Intruder can send files either with or without virus are sniffed by Network Sniffer and routes the packets to Router for filtration. Later router sends the packet for classifying types of attack to the Attack Classifier. Here based on the behavior of the Client/Intruder, it creates dynamic list of attacks. Using Proxy techniques, it blacklists the IP address of intruder to block them reaching server. If it founds the files without virus, allows client for grant access to server otherwise show access denied to the intruder. Access Granted will allow the data to the Server.

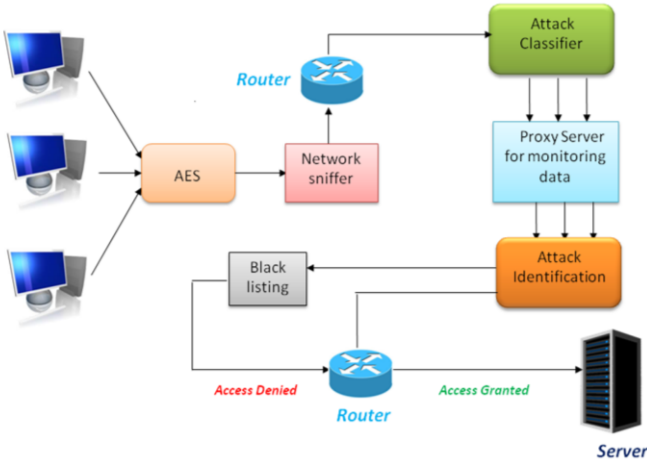

Fig. 1. Architecture of Intrusion Detection Methodology

Steps involved in the Architecture

1: First authentication process done by an user at the source side.

1.1 No fields should not ϕ.

1.2 *Verify ←username and password.*

2: Setting the system IP address for both the source and destination node.

3: Select file from a system storage and send from source to destination.

Selected file ←Encrypt and send.

4: Store the encrypted file to a server.

```
    Check for malware activities
    If exist,
        Classify the virus level, then
        Access will be denied and go to step 2.
        else
            Access will be granted and go to step 4.
5: Encrypted file will be received from a sever to a destination
   node.
   Decrypt received file ← View the original file.
```

IV.CONCLUSION

In this research work we have proposed a network administrator for analyzing the various types of attack and observe malware from the network. The process basically understands the pattern and behavior of the hostile circumstances over the network. Profile of the attackers can be created by using pattern analysis and it is used to blacklisting the malware from the network system. In future work the malware should be classified according to their levels. Proxy server is used to monitor all information in the networking system.

REFERENCES

[1]. Florian Dör fler,StudentMember,IEEE,and Francesco Bullo,Fellow, (2013) "Attack Detection and Identification in Cyber-Physical, Pasqualetti,StudentMember," IEEE.

[2]. Husain, M. Mokhtar, and J.M. Howe,(2013) "Sensor failure detection, identification, and accommodation using fully connected cascade neural network". IEEE Transactions on Industrial Electronics.

[3]. J. Mark off, (2013) "A silent attack, but not a subtle one." New York Times.

[4]. J.D. Gibson, A. Servetti, H. Dong, A. Gersho, T. Lookabaugh, and J.C. De Martin, (2013) "Selective encryption and scalable speech coding for voice communications over multi-hop wireless links."

[5]. L. Repele, R. Muradore, D. Quaglia, and P. Fiorini, (2013) "Improving performance of networked control systems by virus proliferation in peer to peer networks."

[6]. Ncaimu Tang, (2013) "Distance-Bounding Based Defense Against Relay Attacks in Wireless Networks."IEEE.

[7]. P. Prasithsangaree and P. Krishnamurthy, (2013) "Analysis of energy consump- tion of RC4 and AES algorithms in wireless LANs." In IEEE Global Telecommunications Conference (GLOBECOM).

[8]. Riccardo Muradore, Member, IEEE, and Davide Quaglia, (2015) "Energy-Efficient Intrusion Detection and Mitigation for Networked Control Systems Security."

[9]. Xiaofei Wang, Yang Xu, (2013), Member, IEEE, "Stride Finite Automata for High-Speed Regular Expression Matching in Network Intrusion Detection Systems."

[10]. Y. Mo, T.H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, (2012) "Cyber–physical security of a smart grid infrastructure." Proceedings of the IEEE.