ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 5, May 2016

Optimizing the Firewalls from different Domains and Improvising the Security through Hybrid Cryptographic Algorithms

Trupti V. Inamdar, R. M. Goudar

Abstract— Internet has been widely using the firewalls for protecting the private networks. Security checks all incoming and outgoing packets and takes decision according to its policy. Privacy is not being considered in this case and the number of rules in firewall policy files also exceeds in respective domains. Proposed work includes optimization using anomaly detection and removal algorithm and the security is enhanced by protecting the firewall files using the cryptographic algorithms. The hybrid cryptographic algorithm is implemented which performs symmetric AES-DES encryption with 128-bit key. This algorithm uses multiple ciphers of different types together. Security system tends to use a hybrid solution to increase the security and speed of the policy file which is to be encrypted. This security is provided to the firewalls from different domains which reduces the processing time and improves the network performance.

Index Terms- Optimization, privacy, encryption.

I. INTRODUCTIONs

A firewall is defined as any device (or software) used to filter or control the flow of traffic. The implementation of firewall is typically on the network perimeter and it operates by defining trusted and untrusted region. Most firewalls will allow traffic from the trusted region to the untrusted region, without any explicit configuration. However, traffic from the untrusted region to the trusted region must be explicitly allowed. Thus, any traffic that is not explicitly allowed from the untrusted to trusted region will be implicitly denied by default. The basic aim of a firewall is to keep unauthorized users from browsing your network. A firewall can be defined as any software or hardware, it is usually placed at the edge of the network to perform as a gatekeeper for all incoming and outgoing traffic flow. Firewall uses the different techniques to restrict traffic. Device or application may use the combination of these techniques to provide more protection. The four techniques are packet filtering, circuit-level gateway, proxy server and application gateway. Packet filtering is one of the core services provided by firewalls. Packets can be filtered (permitted or denied) based on a wide range of criteria:

- Source IP
- Destination IP
- Type of protocol
- Source Port
- Destination Port

Packet filtering implementation is based on list of rules. These rules are considered critically. The list of rules is always passed from top to bottom manner. Thus, more exact rules should always be placed near the top of the rule-list; otherwise they may be cancelled by a previous, more surrounding rule. Also, an implicit 'deny any' rule usually exists at the bottom of a rule-list, which often can't be removed. Thus, rule-lists that contain only deny statements will prevent all traffic. For increasing the security of firewalls, advanced encryption mechanism should be used.

II.PREVIOUS RELATED WORK

The firewall analysis in previous work focuses on conflict detection. The basic clue of firewall conflict detection is to first detect all rule pairs that conflict with each other, and then the designer of firewall manually observes every pair of rules that are conflicting to check whether those two rules are essential to be swapped or a new rule must to be included. Observing every conflict or anomaly is beneficial to reduce errors. Two ways to approach towards the goal:

[1] How to reduce errors when a firewall configuration is being designed.

[2] How to detect errors after a firewall configuration has been designed.

A. Cross-Domain Firewall(CDF)

Firewall operates on intra-firewall and Inter-firewall domains both. Consider 2 domains and we want to detect inter-firewall redundant rules for these 2 domains. Since

Manuscript received May, 2016.

Trupti V. Inamdar*. Computer Engineering, MIT Academy of Engineering Alandi(D), Pune, Pune, India*

R. M. Goudar*, Department of Computer Engineering, MIT Academy of Engineering Alandi(D), Pune, Pune, India*

firewall rule holds confidential and remote(private) information, the security is needed to provide. The security is provided through the RSA encryption algorithm. The policy files in the firewalls from separate domains are encrypted for security purpose. But this algorithm has a key distribution problem and hence it is less secured. It uses both private and public keys which takes more time for encryption and decryption. Speed of RSA is also quadratic in key length, So the performance of the system is not good enough with the RSA security.

The Cross Domain Firewall permits the network traffic to enforce each other through multiple domains and controls the traffic. For improving the performance of network optimizing the firewall is important. Similar way, Privacy and security are two main worries in supporting users through organizational domains.

B. Contributions

The proposed work focuses on Interfirewall anomaly (redundancy) detection firstly and Second is the Encryption/Decryption algorithm performed on policy files for the purpose of security. The protocol implementation is on both real and synthetic policies of firewall. The results on real firewall policies show that this protocol can remove as many as 98% of rules. Hybrid cryptographic algorithm is used in proposed system for encryption the rule file which is the combination of AES and DES.

III ARCHITECTURE AND METHODOLOGY

A. Architecture

In the Fig 1, the user goes through the registration process and enters into the system through login. Multiple users can be included in this system. Every user should have userid and Password. After authenticating the userid and password from the database, then the user is allowed into the System and search for specific domain. Admin also have userid and password, hence the information searched by the user is viewed by them ,if admin puts the correct userid and password. “An information access system that allows access to all the information on the web that is relevant to a particular domain”.

The user goes through the registration process and enters into the system through login. Multiple users can be included in this system. Every user should have userid and Password. After authenticating the userid and password from the database, then the user is allowed into the System and search for specific domain. Admin also have userid and password, hence the information searched by the user is in the database, then the user is allowed into the System and search for specific domain. Admin also have userid and password, hence the information searched by the user is viewed by them ,if admin puts the correct userid and password. “An information access system that allows access to all the information on the web that is relevant to a particular domain”.

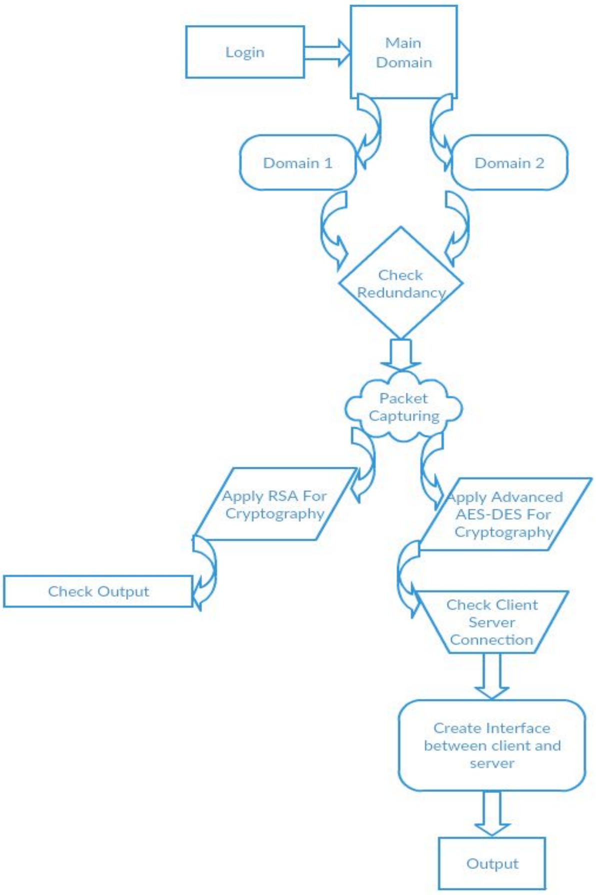
Login
Main Domain
Domain 1
Domain 2
Check Redundancy
Packet Capturing
Apply RSA For Cryptography
Apply Advanced AES-DES For Cryptography
Check Output
Check Client Server Connection
Create Interface between client and server
Output

Fig 1 Architecture of Proposed System

User enters into the specific domain. Then the anomaly detection algorithm is performed to remove the redundancy from different domains in the system. The process of packet capturing is included whose output is generated as train_log file. This file contains information about all the packets flowing through the network. The users should not be allowed to access these private information of network. Hence for maintaining the security, Encryption algorithms are used to protect the policy file(train_log).

A Cross-Domain Firewall that permits two networks to apply each other’s firewall rules in an insensible manner. Redundant or same rules from these different firewalls are removed by the system. . This system is efficient and better as compared to others. CDF is used to allow the security and purifying the rules without revealing the common messages. Matching rule will allow all the packets and rule mismatch means to discard the packet. It eliminates the rules in effective manner.

A. METHODOLOGIES

1. *Anomaly detectition and removal algorithm*

```
old _rules_list ← read rules of config data file
rulelist_new ← empty_ list
for all r ∈ rulelist_old do
    Insert(r, rulelist_new)
for all r ∈ rulelist_new do
    for all s ∈ rulelist_new after r do
        if r ⊂ s then
            if r_action = s_action then
                Remove r from rulelist_new
                break
```

Insert the rule r in rulelist_new

```
if rulelist_new is empty then
    insert r into rulelist_new
else
    inserted ← false
    for all s ∈ rulelist_new do
        if r and s are not disjoint then
            inserted ← resolve(r, s)
            if inserted = true then
                break
    if inserted = false then
        Insert r into rulelist_new
```

2. AES AND DES

Advanced Encryption Standard (AES)[12] is the encryption algorithm established on a principle of design called as a substitution-permutation network. It's speed is high for software and hardware. Dissimilar to its predecessor, DES, AES do not use a Feistel structure. AES is having a fixed size block of 128 bit and size of key is 128, 192, or 256 bit, while Rijndael has specified with key and block sizes in multiples of 32 bit, with a minimum of 128 bit. The maximum block size is 256 bit but the key size is the same. [11]. AES operates on a 4×4 matrix of bytes, termed the state. Most AES calculations are drawn in a distinct finite field. The steps of AES involves Substitute bytes — Uses an S-BOX to perform a byte-by- byte block substitution.

DES is the archetypical block of cipher, In this algorithm plaintext is taken as a fixed-length string and it is then transformed into complicated operations series and then into another cipher text string of the same length. Of DES [12] transformation is customized by the key, so that decryption can be performed only by those who know that particular key used for encryption. In case of DES, the size of block is 64 bits [13], but from that only 56 bits are used and the rest of 8 bits are used for performing the parity operation, and then eliminated in the algorithm. So that, the efficient length of key in DES is 56 bit. There are 16 identical processes, called as rounds. There is also an starting and final permutation, known as IP and FP. Before the main rounds, the block is divided into two 32 bit half blocks and processed at same times, this crossing process is known as the Feistel scheme. Feistel scheme is used to guarantee the matching of both the encryption and decryption processes. The only difference is the sub-key, which is inverted and used in the process of decryption and rest part it is the same. This design defines the algorithm implementation, especially for difficult implementation. XOR operation is performed

3. DESIGN OF HYBRID CRYPTOGRAPHIC ALGORITHM

It is a designed for transfering data with better security. At present, various types of cryptographic algorithms provide high security to information on networks, but there are also has some drawbacks. This hybrid algorithm is designed for better security by combinations of AES and DES.

4. CONCEPT OF HYBRID AES DES

Mathematically, the idea behind the hybrid based AES-DESis that it is construed with reference to basic DES Feistel equations. The replication of these equations is based on the number of rounds as improved by the Feistel structure network, which in the case of DES was standardized. However, by incorporating the AES within this yield the following results.

L1 =f (R0) -------------------------------- (1)
R1 =AES (f (L0) XOR f (R0)) --------- (2)

The plaintext given by user is divided into two halves L0 and R0 each of 128 bits. Each of half is again divided into two halves that is we got LL0 and LR0 from L0 and RL0 and RR0 from R0 of size 64 bits each respectively. DES algorithm is applied on all these halves thar are generated by dividing plaintext, that is LL0, LR0, RL0 and RR0 by using the key given by the user itself. We can also use the two different keys. At the time of encryption if the user decides that two different keys are used that is one key for DES encryption and second key for AES encryption. Same key is used for AES and DES encryption if the user selects only one key at the beginning. The output size of DES encryption text is of 192 bits each. As DES encryption is applied on four quarters every quarter produces an output of size 192 bits. The output of LL0 and LR0 is smashed together to form f (L0) and the output of RL0 and RR0 is smashed together to form f (R0). The length of f (L0) and f (R0) is 384 bits each. Once the f (L0) and f (R0) are obtained, they both are then XORed with each other i.e. f (L0) XOR f (R0). The size of output issame as the size of the input that is The result is 384 bits. After that it is given to AES algorithm where the result is encrypted by using the key given by the user. The key can be same or different. The length of output of the AES encrypted text is of size 704 bits. The f (R0) can be named as L1 and the AES encrypted text can be named as R1. Both L1 and R1 are then smashed together to give the cipher text of 1088 bits. The Decryption process is exactly opposite of the encryption process.

B. Security Analysis

Public-key cryptography, also defined as asymmetric cryptography, refers to a cryptographic algorithm which takes two different keys one is private and the other is public. Two parts of these keys are linked together mathematically. The public key is used for encrypting the plaintext or it can be said like for verifying the signature; whereas the private key is used for decrypting the cipher text or for generating the digital signature. The term "asymmetric" stops from the use of different keys to perform these different functions, each function is the inverse of the other – as compared with predictable symmetric cryptography which depends on the same single key to perform both the operations. Public-key algorithms are centered on mathematical problems which has no effective solution that are essential in certain integer factorization, discrete logarithm, and elliptic curve relationships. It is easy for a user for computations to generate their own public and private key-pair and use those for encryption and decryption. It is computationally infeasible for a private key which is properly generated to be determined from its corresponding public key.

II. RESULT ANALYSIS

By using the proposed method security is increased and privacy is also maintained. The concept of Combined AES and DES is used for encrypting the policy files that are shared among the networks. As the network is growing these days, use of a powerful encryption algorithm for security purpose is very necessary. Previously the RSA algorithm was used for security within firewalls which was having key distribution problem that's why taking more time for encryption and decryption. The Hybrid cryptographic algorithm in the proposed system is more flexible, it uses multiple ciphers of different types together. Convectional encryption system uses only one key, if this key is disclosed then complete encryption and decryption process become Vulnerable. Security system tends to use a hybrid solution to increase the security and speed of firewall policy file.

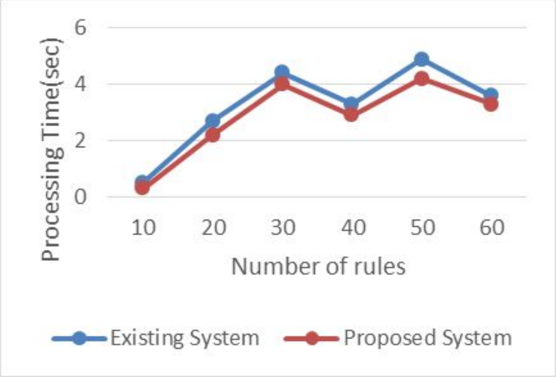

Fig 2. Processing Time

Above Fig. 2 shows the graph of results based on the number of rules. In Proposed system rules are optimized, so the processing time required for accessing the firewall policy files by the user is minimized.

III. CONCLUSION

Firewalls are designed to provide access control. The proposed method is Efficient and secured approach for cross domain firewalls to improve their performance by reducing the processing time. By using this method the security will be increased and controlled and also we can able to provide privacy and security. If the rule exists, this protocol is proposed to optimize the network. If the rule does not exist, the network performance collapse and discards due to the entry of third party. Thereby privacy and security fails. Security is maintained through the hybrid cryptographic algorithm. This algorithm uses many computations for obtaining the keys, Hence the security is unbreakable. Firewall policy file is protected by this algorithm.

ACKNOWLEDGMENT

I thank Prof. R. M. Goudar for providing guidance and giving suggestions on the project. She gave me directions and helped me to find the solutions. I have further more to thank Prof. Sunita. S. Brave, M.E. Coordinator, Department of Computer Engineering, to encouraged me to go ahead and for continuous guidance. I also want to thank Prof. S. A. Jain for all his assistance and valuable guidance.

REFERENCES

[1] R. A. Devi and P. Arivanantham, "Interfirewall optimization across administrative domains for enabling privacy preserving and security," *Information Communication and Embedded Systems (ICICES), 2014 International Conference on*, Chennai, 2014, pp. 1-5.

[2] Hong-ryeol Gil1, Joon Yoo1 and Jong-won Lee2 ,'An On-demand Energy-efficient Routing Algorithm for Wireless Ad hoc Networks', Proceedings of the 2nd International Conference on Human. Society and Internet HSI'03, pp. 302-311, 2003.

[3] S.K. Dhurandher, S. Misra, M.S. Obaidat, V. Basal, P. Singh and V. Punia,'An Energy-Efficient On Demand Routing algorithm for Mobile Ad-Hoc Networks', 15 th International conference on Electronics, Circuits and Systems, pp. 958-9618, 2008.

[4] DilipKumar S. M. and Vijaya Kumar B. P. ,'Energy-Aware Multicast Routing in MANETs: A Genetic Algorithm Approach', *International Journal of* Computer *Science and Information Security* (IJCSIS), Vol. 2, 2009.

[5]AlGabri Malek, Chunlin LI, Z. Yang, Naji Hasan.A.H and X.Zhang ,' Improved the Energy of Ad hoc On- Demand Distance Vector Routing Protocol', International Conference on Future Computer Supported Education, Published by Elsevier, IERI, pp. 355-361, 2012.

[6]D.Shama and A.kush,'GPS Enabled E Energy Efficient Routing for Manet', International Journal of Computer Networks (IJCN), Vol.3, Issue 3, pp. 159-166, 2011.

[7]Shilpa jain and Sourabh jain ,'Energy Efficient Maximum Lifetime Ad-Hoc Routing (EEMLAR)', international Journal of Computer Networks and Wireless Communications, Vol.2, Issue 4, pp. 450-455, 2012.

[8] Vadivel, R and V. Murali Bhaskaran,'Energy Efficient with Secured Reliable Routing Protocol (EESRRP) for Mobile Ad-Hoc Networks', Procedia Technology 4,pp. 703- 707, 2012.

[9] A. X. Liu, E. Torng, and C. Meiners. Firewall compressor: An algorithm for minimizing firewall policies. In *IEEE INFOCOM*, 2008.

[10] M. G. Gouda and A. X. Liu. Structured firewall design. Computer Networks Journal (Elsevier), 51(4):1106–1120, March 2007.

[11] Advance Encryption Standard, [Online], Available: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

[12] Deven N. Shah:"Information Security: Principles and Practice".J.Orlin Grabbe:"The DES Algorithm Illustrated",

Trupti V. Inamdar Student Studying Post Graduation M.E.(Computer) at MIT AOE, Alandi(D), Pune Interest in Computer Network.

R. M. Goudar Is Associate Professor in Department of computer engineering at MIT AOE, Alandi(D), Pune. Her Area of Research is Cognitive Radio Network.