© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 05 , Issue : 01 | January – March 2018

BOOSTING SECURITY OF NETWORK USING PICTURE KEY ENCRYPTION

Nancy, nancymalik339@gmail.com

ISSN : 2348-5612 © URR
9 770234 856124

Abstract: Networking is a process of information & ideas among individuals or groups that share common interests. Networking has been two categories: social or business. In this paper we have discussed threats to security of network & different security mechanisms. research is that if there is secure transmission then speed of data transfer gets degraded. But if packet size is reduced then speed of data transmission could be improved in contrast of secure traditional work. Here we have discussed how to improve security of networks using picture key encryption.

Keywords: Network security, Encryption, decryption, DES, RES, AES, Picture key Encryption

[1] NETWORK SECURITY

Data security is an essential aspect of IT for organizations of every size & type. The security of Data means to protecting digital privacy measures that are useful to prevent illegal access to computers, websites & databases. Data security also protects data from corruption. This is means as data or computer security. These security technologies include data masking backups & data erasure,.

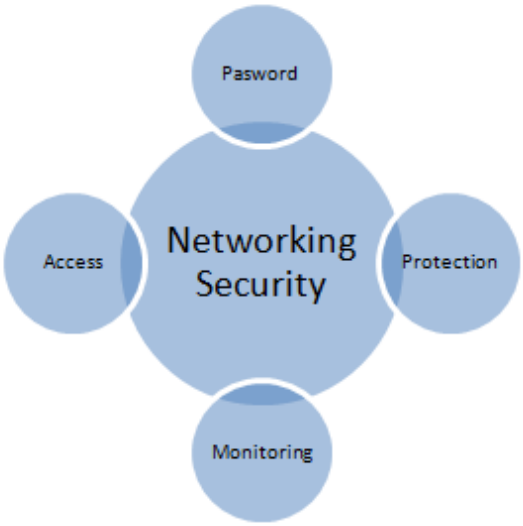

Fig 1 Security

The key of data security measure is encrypt that software/hardware, digital information, hard drives are encrypted & rendered deadly to illegible users & hackers. One of most commonly encountered methods of practicing data security is use of authentication. Within authentication, users must provide a password, code, biometric data, or some other form of data to verify identity before access to a system or data is granted.

Network security would be any activity considered to secure reliability & usability of computer network & data. It involve both hardware & software technologies. Effective network security manages access to network. It objective a diversity of attacks & stops them from entering or spreading on your network. Network security combines multiple layers[1] of defenses at edge & in network. security layers of network enhance documents & controls. users received entry to network resources, but malicious actors are blocked from carrying out exploits & threats. Digitization has transformed our world.

Types of network security[2]

Access control

Not some client would have access to their data network. To stay out possible hacker we require to recognize each user & each device

Application security

This security to include procedure software & hardware to use to close those holes.

Behavioral analytics

Behavioral analytics tools automatically discern activities that deviate from norm.

Data loss prevention

This technologies could stop people from uploading, forwarding, or even printing critical information in an unsafe manner.

Firewalls

A firewall could be hardware, software, or both. Cisco offers unified threat management devices & threat-focused next-generation firewalls.

[3] CRYPTOGRAPHY

It had been discipline of information security had been called Cryptography. Meaning of Cryptography had been hidden imitative from Greek crypto's. The Cryptography are cover data within space or transfer including methods like as integration of words with image.

Cryptography had been process of altering plaintext using process encryption into cipher text using procedure decryption. This procedure had been used to secure communication between two parties within occurrence of third party. There are four goals for Modern cryptography:

Confidentiality

It identifies that only participants should be able to access message.

Integrity

Content of message should not be changed. If it had been altered, then it had been called type of modification attack.

Non-repudiation

There had been situation where sender converts content of message & after that he refuses that he had not sent message.

Authentication

Both sender & receiver had to prove credentials to each other. cryptography had been basic requirement of computer experts for security purposes so that two parties could send data to each other without any modification & confidently. So both sender & receiver could validate to each other for secure communication so that material could be safely send to each other.

[4] ENCRYPTION TECHNIQUES

In this section we have discussed encryption techniques.

Data Encryption Standard - Symmetric Key Cryptography

1. In first step, 64-bit plain text block is handed over to an Initial permutation function.
2. The Initial Permutation is performed on plain text.
3. Next, Initial Permutation produces two halves of permuted block; say Left plain text (LPT) & Right Plain Text (RPT).
4. Now, each of LPT & RPT goes through 16 rounds of encryption process.
5. In end, LPT & RPT are rejoiced & a FINAL Permutation (FP) is performed on combined block.

6. The result of this process produces 64-bit cipher text.

RSA (Rivest, Shamir, Adleman) Asymmetric Key Cryptography

1. Choose two large prime numbers P & Q.
2. Calculate N = P * Q.
3. Select public key (i.e. Encryption key) E such that it is not a factor of (P-1) & (Q-1).
4. Select private key (i.e. decryption key) D such that following equation is true:

i. (D * E) mod (P-1) * (Q-1) = 1

5. Work out for cipher text from plain text as follows: CT = PTE mod N.
6. Send CT as cipher text to receiver.
7. For decryption, calculate plain text PT from cipher text CT as follows: PT = CT^D mod N

[5] PROPOSED WORK

Several experiments have been conducted with this Procedure on several images. There are some steps of our proposed technique are given below:

Phase 1: Firstly we develop a particular GUI for this implementation. After that we develop a code for loading picture file in Matlab database.

Phase 2: Develop a code for encryption algorithm using wavelet with suitable key in proposed work. This code is explain then implementer on image.

Phase 3: Develop a code for compression technique using Prediction Error Clustering & Random Permutation.

Phase 4: After that we develop code for decompression & decryption process.

[6] IMPLEMENTATION

Snapshots of Key exchange problem

The various snapshots for key exchange problem are given below:-

Fig 2 Snapshot of Symmetric Cryptosystem

Above figure 2 would be first view of simulation. In this figure both approach are shown i.e. Symmetric key & Picture key.

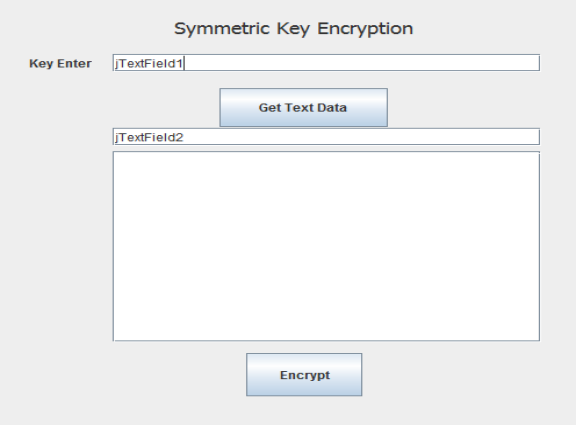

Fig 3 Snapshot of Symmetric Key Encryption

In above figure 3 we would perform symmetric key encryption i.e. traditional approach which would be performed on text message with help of key.

Fig 4 Snapshot of Message Encrypted

In above figure 4 we have taken a message **"hello how r u?"** as our plain text & then encrypted message with a key **"123456"**.

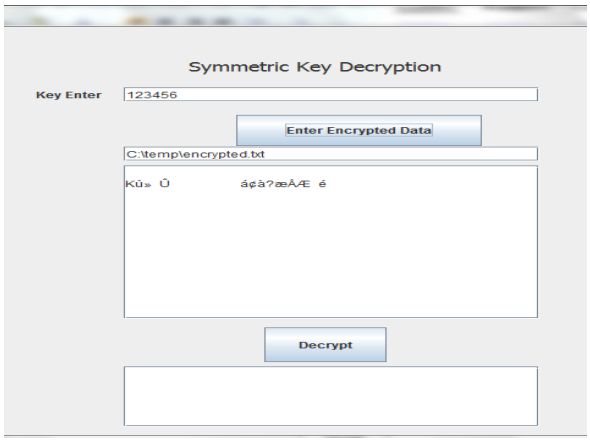

Fig 5 Snapshot of Symmetric Key Decryption

In above figure 5 we are performing decryption process. For that we are taking same key as used for encryption. Here key exchange is a big issue more over intruder could easily attack on key.

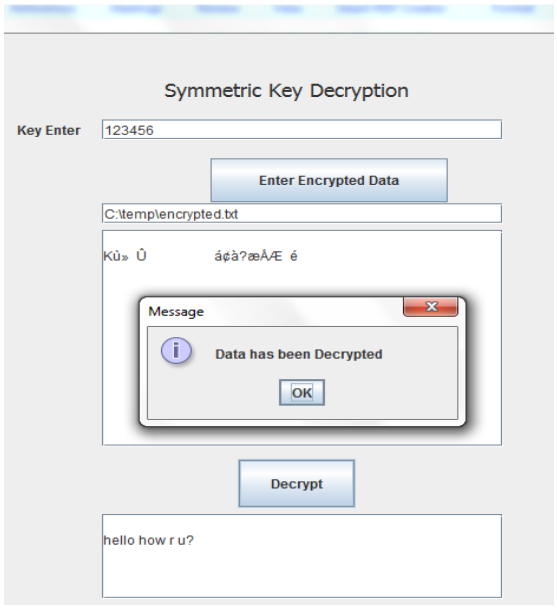

Fig 6 Snapshot of Message Decrypted

In above figure 6 we performed decryption process on encrypted data using same key & we got same plain text.

Proposed Protocol

Sender side:-

Fig 7 Snapshot of Picture Key Cryptosystem

For proposed protocol key picture & data picture are shared between sender & receiver.

© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 05 , Issue : 01 | January – March 2018

Fig 8 Snapshot of Message Encrypted with Shared Picture

In above figure 8 we have taken same message "hell how r u?" as our plain text. Plain text is encrypted using Key picture with DES.

Fig 9 Snapshot of Browsing of Cover Picture for Encryption

[7] CONCLUSION

The Picture based encryption has been found far better approach in order to enhance security of network. However DES, AES standard algorithms are providing security. But they have certain limitations. This work would reduce probability of data hacking from hackers end.

REFERENCE

1. Shahriar Mohammadi, Reza Ebrahimi Atani, Hossein Jadidoleslamy (2011) A Comparison of Link Layer Attacks on Wireless Sensor Networks *Journal of Information Security*, 2011
2. Wajeb Gharibi & Maha Shaabi (2012) Cyber threats in social networking websites, International Journal of Distributed & Parallel Systems (IJDPS) Vol.3, No.1, January 2012
3. Tongguang Ni, Xiaoqing Gu, Hongyuan Wang, & Yu Li (2013) Real-Time Detection of Application-Layer DDoS Attack Using Time Series Analysis, Journal of Control Science & Engineering Volume 2013,
4. Hong-Ning Dai, QiuWang, Dong Li, & Raymond Chi-Wing Wong (2013) On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas, International Journal of Distributed Sensor Networks Volume 2013,
5. Rupam, Atul Verma, Ankita Singh (2013) An Approach to Detect Packets Using Packet Sniffing, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.3, June 2013

6. Md. Waliullah, (2014) Wireless LAN Security Threats & Vulnerabilities, International Journal of Advanced Computer Science & Applications, Vol. 5, No. 1, 2014
7. Jhilam Biswas, Ashutosh (2014) An Insight in to Network Traffic Analysis using Packet Sniffer, International Journal of Computer Applications (0975 – 8887) Volume 94 – No 11, might 2014
8. Sharmin Rashid, Subhra Prosun Paul (2013) Proposed Methods of IP Spoofing Detection & Prevention, International Journal of Science & Research (IJSR), Volume 2 Issue 8, August 2013
9. Mukesh Barapatre, Prof. Vikrant Chole, Prof. L. Patil (2013) A Review on Spoofing Attack Detection in Wireless Adhoc Network, International Journal of Emerging Trends & Technology in Computer Science, Volume 2, Issue 6, November – December 2013
10. D. R. Cheriton & C. L. Williamson, 'VMTP as Transport Layer for High-Performance Distributed Systems,' IEEE Commun. Mag., vol. 27, no. 6, June 1989.
11. D. D. Clark, M. L. Lambert, & L. Zhang, "NETBLT: A High Throughput Transport Protocol," Proc. SIGCOMM '87and Commun. Rev., vol. 17, no. 5,' 1987.
12. Mr. Sachin Taluja Survey on Network Security, Threats & Firewalls International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 1, Issue 7, September 2012
13. Kuldeep Tomar ENHANCING Network Security & Performance Using Optimized Acls International Journal in Foundations of Computer Science & Technology (IJFCST), Vol.4, No.6, November 2014
14. Dhanalakshmi. R Enhancing Network Security by Implementing Preventive Mechanism Using GNS3 International Journal of Innovative Research in Science, Engineering & Technology Volume 6, Special Issue 3, March 2017
15. Udaya Wijesinghe An Enhanced Model for Network Flow Based Botnet Detection Proceedings of 38th Australasian Computer Science Conference (ACSC 2015), Sydney, Australia, 27 - 30 January 2015
16. Johannes Landstorfe Weaving a Carpet from Log Entries A Network Security Visualization Built within Co-Creation We created a pixel map for multivariate data based on an analysis of needs of network security engineers.