An Innovative Angle in the Application of Cryptography to Network Security

H.MOHAMMED KHAN M.C.A.,
Lecturer,
Department of Computer Science,
Shaqra University,Shaqra,K.S.A

DR.J.GEORGE CHELLIN CHANDRAN.,M.E.,Ph.D.,
Principal,
C.S.I College of Engineering,
Ooty, Tamilnadu, India

C.SAHAYA KINGSLY.,M.E
Research Scholar,
Manonmanium Sundaranar University
Tirunelveli, India

Abstract— **Network Security is protecting data transmitted over a network and privacy is of utmost importance. Rapid developments in information technology makes Data Security a challenging issue of data communications in the global networked world. Vital information of offices and organizations has to be guarded from unauthorized persons who may tamper with the information. Sensitive information is exposed to threats like masquerades, corruption or denial of services [1, 2]. Secure systems need to maintain integrity and privacy of data [3]. Designing an appropriate security system to protect proprietary information requires developing a set of appropriate solutions for specific risk scenarios. One important tool to protect information is the use of cryptography for hiding contents of a message and Confidentiality of network communications. The applications of cryptography go beyond networks, business and customers. This paper suggests a new direction in using cryptography for network security.**

Keywords- Cryptographic Algorithm, Network Security, Communication security

I. INTRODUCTION

Information exchanges and collaborations on the public networks is at an unprecedented level. The open nature of these exchanges makes it more difficult to protect valuable information, identifying a strong need for security on intranets and Internet. Internet Protocol (IP) networks which provide for open communication between users and computers are vulnerable to attacks. Intruders can steal proprietary information or eavesdrop on private communications by impersonating users on the network. Both the software industry and the Internet community need to address these problems and improve security of information on open networks. Cryptography which is a viable solution to network security has a long history. It has been used as a means of secure communication between any two parties. Modern day cryptography is more complex and has an expanded domain. It is designed to be a cost-effective means of protecting electronic data that is stored and communicated across networks. Cryptography has advanced after having emerged in the 1970s. The National Bureau of Standards (NBS) data encryption standard called the Data Encryption Standard (DES), in January, 1977 was a milestone in launching cryptography research and development into the modern age of computing technology,. Commercial cryptography began in December, 1980, when American National Standards Institute (ANSI), adopted DES. Cryptography is not only considered both, a branch of mathematics and a branch of computer science. Cryptosystems have two forms namely symmetric and asymmetric. Symmetric cryptosystems use a single key, the secret key to encrypt and decrypt information. Asymmetric cryptosystems use a public key to encrypt messages and a secret key to decipher or decrypt encrypted messages, called public key cryptosystems. Public Key Cryptography (PKC), is still undergoing research development [4]. RSA algorithm is a popular public key cryptosystem developed by Ron Rivest, Leonard Adleman and Adi Shamir in 1977 [5]. The RSA algorithm generates the public key by multiplying two large digits and a randomly chosen large number, called the encryption key. RSA is considered a strong algorithm since mathematics is involved. Pretty Good Privacy (PGP) of Phil Zimmerman is another popular public crypto system. The strength of the keys is directly dependent on the length of the keys. Modern cryptosystems use complex mathematical algorithms and techniques to provide network and information security. Cryptography-based security commonly use Encryption algorithms, Message digest functions, Hashed Message Authentication Code (HMAC) functions, Secret key exchange algorithms and Digital signatures. Cryptography is based on secrets and secretive, hence, it may not be good for security [6]. The techniques involved in cryptography parallels software applications hiding details from users, making cryptography a useful tool in providing network and data security [5]. Companies have incorporated data loss preventions by incorporating cryptographic techniques, into their network programs. Information security is needed but is often difficult to achieve. Cryptography serves as the base for IT security solutions including Digital signatures. Web-based applications rely on Secure Sockets Layer (SSL) and Transport Layer Security (TLS). Cryptography and information security are needed in the defense of almost every nation and enterprise worldwide [7]. The nature of the Internet makes it difficult to trace or identify intruders of corporate

networks and businesses nvolved in the public domain. The overall security of a system depends upon its ability to keep the cipher keys a secret. Security is an important aspect of wireless ad-hoc networks also where mobile applications perform network specific tasks. Mobile Application Security System (MASS) utilizing a layered security approach and strong cryptographic techniques is a viable low-cost solution for protecting application-based wireless networks [8]. The concept of data hiding technologies aims to solve modern network security and secure communications. These technologies are a cost-effective, do not require protocol modifications and is compatible with existing standards of compression and communications [9]. This paper suggests new directions for secured communication over an unsecure channel.

II. TYPES OF ATTACKS ON NETWORKS

Network attacks analyse the network and gain information, eventually crashes or corrupts the network. Attackers also exploit unmonitored network devices which are the main source of information leakage, since Emails, web requests, transmittable files are handled by network devices. When a network device is controlled the attacker cuts across all categories of software's and platforms. There are a variety of network attacks like Spoofing, Sniffing, Mapping, Hijacking, DoS and many more. There are also many types of code-breaking attacks. Brute-force is an attack on encrypted information in which all possible keys combinations are tested until the correct one is encountered [10]. All internet connected devices send IP datagrams with the sender's IP address and application-layer data. The attacker controls by modifying protocols and placing an arbitrary IP address into the data packet's source address field called IP spoofing. It is difficult to find the source when spoofed. Packet sniffing is intercepting data packets on the network at the Ethernet layer in combination with network interface cards (NIC). Sniffers capture all traffic communication packets and monitor the traffic. Packet sniffers are generally passive and clear their tracks or logs. Eavesdropping or Mapping is obtaining the IP addresses of machines, operating system and services offered. This monitoring is the biggest security problem faced by network administrators. The man-in-the-middle attack takes advantage of weakness in the TCP/IP protocol stack and Hijacks an active communication and re-routes the data exchanges. Denial-of-Service attack (DoS) is attack where the network is flooded with unwanted requests. Yahoo! and e-bay were victims of DOS attacks in the past. DOS attacks result in unusually slow network performance and ultimately unavailability of the web site. Figure 1 illustrates the DOS attacks based on different protocols. Though spoofing can be countered with ingress filtering at the router level, Cryptography remains the main line of defence against network threats. End user-to-user encryption counters spoofing. Counter measures for eavesdropping again are strong encryption services based on cryptography.

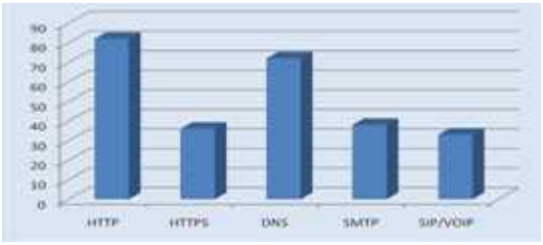

Figure 1. DOS attacks on Protocols

III. PROPOSED CRYPTOGRAPHIC DESIGN

Cryptography is an important component of secure communications systems where there is a growing need for protection of information [11]. Cryptography is an alternative to protect Networks, since Crypto techniques balance communication capabilities with security. Crypto techniques mark, transform and reformat the message to protect them from disclosure, change or both, making information transit safer. Cryptography can also protect transmitted information from being intercepted as a passive attack or modified as an active attack by an intruder. Cryptography secures communications on networks by Authentication, Confidentiality and Integrity. In cryptography, a string of bits to be encrypted is called the plaintext, often denoted by a P or an M for message. The plaintext is transformed by an encryption process to an encrypted text known as the cipher text, commonly denoted by the letter C. The receiver transforms the cipher text to the original plaintext using a cryptographic algorithm, called decryption [12], as depicted in Figure 2. The transformation between plaintext and cipher text can be described using formal notations. We write, D(K,E(K,P)=C)=P where C = cipher text, M = plain text, E = encryption rule and D = decryption rule.

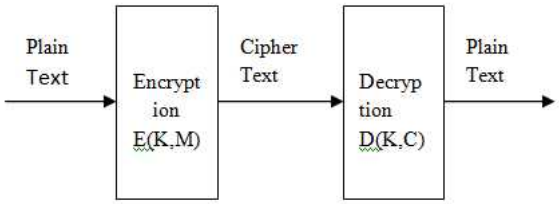

Figure 2. Basic Encryption and Decryption

IV. SECURING TRANSMISSIONS WITH ACCESS CONTROL LISTS

Access control lists commonly referred to as ACL's are the primary element in securing networks. They are filters utilized by routers and switches to permit and restrict data inflows. A configured ACL, analyses data passing through the interface and

permits the flow or prohibits it. ACLs are not complex like firewalls, but provide protection on high speed interfaces. ACLs are also used to restrict updates and define flow control for network traffic. ACLs can filter traffic from less desirable networks and known vulnerable protocols. ACLs have a similar profile for defining an access control list. The lists generally have an Access control list name (numeric or combination of letters and numbers), A sequence number for each entry, a permission or denial status, network protocols and ports, Destination and Source targets where addresses are defined as a single discrete address, a range or subnet, and additional flags or identifiers. There are many types of access control lists but defined for a distinct purpose. ACLs can be reflexive ACLs or dynamic ACLs. Dynamic ACLs or lock-and-key ACLs allow user access to a specific source/destination host through a user authentication process. One of the most common methods is setting up a de-militarized buffer zone DMZ, in the network as depicted in Figure 3. In a DMZ, the most exterior router provides access to other network connections. This router provides larger protection access blocks to areas of the global routing tables. IT professionals place systems which need access from outside in a DMZ like web servers or DNS servers. The internal router is more restrictive and designed to protect from defined threats. They are configured with explicit permissions. ACL file Lines have the following syntax <permit | deny> <ip-address[/mask]> [tracelevel] [# comment]. For Example permit 10.1.2.0/24 # permit client network, permit 192.168.7.0/24 # permit server network, deny 0.0.0.0/0 # deny the rest.

A. *Encrypting the ACLs*

Understanding traffic flow and placement is important in configuring an ACL on a router. Mistakes in ACL placement are common in security implementations. ACLs start with a source address first in their configuration and destination second and it is important to recognize all network hosts. The implementation in explained below. Initially, Making the File Entries encrypted with a common key, increases the security level. For Example applying the network id to the source and destination and increasing the length of the network key to 128 bits. Only the hosts who know the common generated key would have access to the network. Spoofs or attackers would have to know the key in advance before getting access. The encrypted key which includes the hosts id and name will have to broken by the attacker to have access. This new encrypted id of the hosts will have less danger in being hacked in transit. The file would also be accessible only on producing the common key. Since the common key is generated by the network administrator, all accesses can be monitored and configured accordingly. The common key and the encrypted ACL entry are depicted in Figures 3 and 4

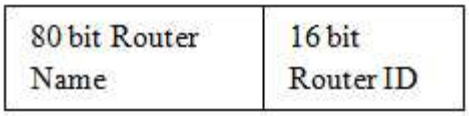

Figure 3. 96 bit Common Encrypted Key of the Router

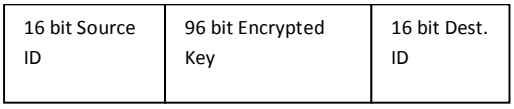

Figure 4. The 128 bit Encrypted ACL Entry

B. *Encryption Algorithm*

Let N be the router name and Nid be the network id. The name is clubbed with the corresponding Nid in an exclusive OR operation to form the Encrypted common key. The resultant Cipher text is rotated right twice to generate the final output of the Encrypted key C.

Algorithm EK(N)

{

N . . .N ← Nid

C EKN← Nid

C ⊕ (RARC)2

return C

}

C. *Decryption Algorithm*

Let C be the given Encrypted key of length m (90). The key is rotated left twice and an exclusive OR operation done with Nid to retrieve the original Name.

Algorithm DK(C)

{

C . . .C[n] C

K . . ←. K[n] K

C ← (RALC)2

N ⋯ E−1 (C) Nid

return N

}

V. ANALYSIS OF THE ENCRYPTED NETWORK KEY

Cryptanalysis finds weaknesses or insecurity in a cryptographic scheme though it is a common misconception that every encryption method can be broken. There are many cryptanalytic attacks classified in several ways. The cryptanalyst has access to a ciphertext and its corresponding plaintext. A brute-force attack tries every possible key until the

translation of the ciphertext into plaintext is obtained after half of the possible keys are tried to achieve success. Table 1 shows time involved for various key spaces with the results for four binary key sizes. The 56-bit key size is used with the Data Encryption Standard (DES) algorithm, and the 168-bit key size is used for triple DES. The minimum key size specified for Advanced Encryption Standard (AES) is 128 bits. For each key size, the results are shown assuming that it takes 1 μs to perform a single decryption and with the use of parallel microprocessors, it may be possible to achieve higher order processing rates. The final column of Table 1 considers the results for a system that can process 1 million keys per microsecond. A simple brute force attack against DES requires one known plaintext and approximately half of the possible keys, to find the keys. Since the key length of 128 (96+32) is large, it is difficult to trace this key in exhaustive key searches and secure against known cryptanalytic techniques, namely differential and linear cryptanalysis.

TABLE I. EXHAUSTIVE KEY SEARCH TIME TAKEN TO BREAK A KEY

Key Size Bits	Alternate Keys	Time Required for Decryption
32	$2^{32}= 4.3 \times 10^{9}$	2.15 milliseconds
56	$2^{56}= 7.2 \times 10^{16}$	10.01 Hours
128	$2^{128}= 3.4 \times 10^{38}$	5.4×10^{30} Years

VI. CONCLUSION

Information and communications technologies do not always work perfectly and human errors can also play a role. Strongest cryptography becomes ineffective if the keys are compromised. Moreover, the process of revoking keys and key certificates can be complicated Sources of motivation differ from hacker to hacker. They may hack for a variety of reasons like, financial, political, desire for recognition and a desire to do harm. It is important to understand the risks, threats and vulnerabilities currently existing in the environment. Encrypted Data with Algorithms take a longer time to decrypt in terms of choices or permutations. This paper has provided a new angle towards network security and on transmissions via insecure communication channels. The proposed algorithm has also discussed that an encrypted ACL entry can withstand any type of the attack.

REFERENCES

[1] B. Figg. (2004). Cryptography and Network Security. Internet: http:/www.homepages.dsu.edu/figgw/CryptographyNetworkSecurity.ppt. [March 16, 2010].

[2] A. Kahate, Cryptography and Network Security (2nd ed.). New Delhi: Tata McGraw Hill, 2008.

[3] M. Milenkovic. Operating System: Concepts and Design, New York: McGrew-Hill, Inc., 1992.

[4] Levy, S. (2001). Crypto: How the code rebels beat the Government – Saving privacy in the digital age. New York: Viking Penguin Publishing.

[5] Robinson, S. (2008, June). Safe and secure: data encryption for embedded systems. EDN Europe, 53(6), 24-33.

[6] Schneier, B. (2004, October). The Nonsecurity of Secrecy. Communications of the ACM, 47(10), 120-120.

[7] Fagin, B., Baird, L., Humphries, J., & Schweitzer, D. (2008, January). Skepticism and Cryptography. Knowledge, Technology & Policy, 20(4), 231-242.

[8] Floyd, D. (2006, Fall2006). Mobile application security system (MASS). Bell Labs Technical Journal, 11(3), 191-198.

[9] Lovoshynovskiy, S., Deguillaume, F., Koval, O., & Pun, T. (2005, January). INFORMATION-THEORETIC DATA-HIDING:: RECENT ACHIEVEMENTS AND OPEN PROBLEMS. International Journal of Image & Graphics, 5(1), 5-35.

[10] K.M. Alallayah, W.F.M. Abd El-Wahed, and A.H. Alhamani."Attack Of Against Simplified Data Encryption Standard Cipher System Using Neural Networks". Journal of Computer Science,2010, 6(1), pp. 29-35.

[11] William Stallings, "Cryptography and Network Security Principles and Practices, Fourth Edition", Prentice Hall, 2005.

[12] B. Schneier. Applied Cryptography. John Wiley & Sons Inc., 2nd edition, 1996.

