ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

Crypt Analysis Of DES Cryptosystem Over Man In The Middle Attack

[1] Chandrashekar T, [2]R.Viswanathan,[3]Punitharaja.K
[1][3] Assistant Professor, [2]Associate Professor
[2][3] Galgotias University [1]Sr,VIT, University

Abstract: In this paper, we are developing the DES (Data Encryption Standard) algorithm to minimize the possibility of getting attacked from the hacker to break the crypto code. Moreover, this will result in increase over security level to protect data over the network attacks. This design also shows the strength of encryption and decryption process with reference to the reasonable overhead. Here the paper objective is to show the tuned DES to the common mathematical attack especially man-in-the-middle attack.For the security issues in the internet, cryptography is one of the most important nowadays. Designing a cipher for data exchange between one node to other node deals with one of the troubleshooting job. In our algorithm we try to bring in a new system in the field of cryptography. We are hopeful that this new system will sure minimizes the overhead of data or key exchange between nodes.

Keywords - DES, Man-in-the-middle attack, Encryption, Decryption, Cryptography.

INTRODUCTION

Cryptographic attacks are designed to weaken the security of cryptographic algorithms, and they are used to try to decrypt data without prior access to a key. Cryptanalysis, which is defined as the art of deciphering encrypted data. Also known as the art of creating secreted writing, shape the science of Cryptology. Cryptosystem is defined as the set of transformations that are required to translate an unencrypted message into an encrypted message.

In Cryptography key exchange is one of the most significant aspects. While transmitting data between two nodes we need to use some keys to encrypt data from cipher text to plain text or the original text. The process where same key is used to encrypt or decrypt data in cryptography is called symmetric key cryptography presented in Bellare et al. [1]. Whereas using symmetric key in cryptography the sender and receiver may use the similar by some previous conformity or they may send the key one after the other. While sending key one another the security part might be maintained.

Cryptography is the study of techniques for safe and sound communication in the existence of third parties. It is about constructing and analyzes the protocols that rise above the influence. Cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography consist of ATM cards, computer passwords, and electronic commerce and so on proposed in Liddell et al. [3].

RELATED WORKS

Major technology companies not only tampering web traffic to deliver advertising. Security researchers newly discovered that consumer-grade Lenovo computers ship with software called Superfish Visual Discovery that injects advertising into websites on browsers such as Google Chrome and Internet Explorer presented in I. Paul [5]. G. N. Nayak et al. [6] emphasizes on different types of MITM attacks, their consequences and feasible solutions under different situations. MITM attack of each kind has lot of consequences such as, stealing online account userid, stealing of local ftp id, telnet session, password, ssh.

Mauro Conti et al. [7] analyze and classify the possibility of MITM attacks considering open systems interconnection (OSI) model, as well as two network technologies, GSM and UMTS. Categorize Man in the Middle attacks based on several factors, like location of an attacker in the network, impersonation techniques and nature of a communication channel.

HTTPS protocol avoids illegal viewing of their personal, financial, and confidential information over the Web. Man in the Middle attack to HTTPS protocol described in F. Callegati et al. [8]. K. M. Haataja et al. [10] proposed a Bluetooth MITM attack against Bluetooth-enabled

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

printers that support SSP (Secure Simple Pairing). A. Ornaghi et al. [11] describes different types of MITM attacks. They are Command injection, malicious code injection, Key exchanging, Parameters and banners substitution, IPsec Failure, ARP poison, DNS Spoofing.

R.Wagner [12] proposed and explain ARP Spoofing and its role in Man-in-the middle attacks. Enrique de la Hoz et al. [13] have proposed insecure key exchange lead to a man-in-the-middle attack (MITM). Trust in certificates is usually attained using Public Key Infrastructures (PKIs), which employ trusted certificate authorities (CAs) to create certificate validity chains. N. Karapanos et al. [14] presented a TLS Man-In-The-Middle (MITM) attacks in the context of web applications, where the attacker is capable to effectively impersonate the legitimate server to the user, with the goal of impersonating the user to the server and thus compromising the user's online account and data.

X. Bai et al. [15] introduces one type of defense technique established on the main features of DNS response packets. The technique employs Artificial Neural Networks (ANN), which produces excellent performance. Y. Yang et al. [16] describe a SCADA (Supervisory Control and Data Acquisition) specific cyber-security test-bed which comprises SCADA software and communication infrastructure. This test-bed is used to examine an Address Resolution Protocol (ARP) spoofing based man-in-the-middle attack. F. Fayyaz et al. [17] explore JPCAP (a Java library for capturing and sending network packets) must be used to capture ARP replies. JPCAP is open source and is licensed under GNU LGPL. It can seizure Ethernet, IPv4, IPv6, ARP/RARP, TCP, UDP, and ICMPv4 packets.

J. Belenguer et al. [18] present a low-cost embedded IDS which, when plugged into a switch or hub, is capable to identify and avoid MitM attacks automatically and efficiently. Z. Trabelsi [19] proposed a practical and efficient mechanisms for identifying such malicious attacks in a switched LAN environment. M.-H. Chiu et al. [20] demonstrated a form of active attacks, called Man-in-the-middle (MITM) attack, in which the entire communication between the victims is controlled by the attacker. A detailed description of setting up the system for MITM is included.

Man-In-The-Middle Attack:

Man-in-the-middle attack means the hacker illegally demanding to access the communication between users whereas we designed to catch the transmission of a key which is to insert a known key structure in place of the requested public key. From the view of the victims of such attacks, their encrypted communication appears to be taking place normally in fact the hacker is receiving every encrypted message and decoding it and then encrypting and sending it to the originally intended recipient.

In Figure 1, it is shown that when Ramesh and Suresh giving out their communication they are trying to establish their connection with secret key. But at the same the hacker or the intruder sits in the middle of Ramesh and Suresh and trying to access the communication between them. When Ramesh sends secret key to Suresh then Suresh should reply the suitable secret key to Ramesh for the communication. But here the hacker has the possibility to send any random key to both Ramesh and Suresh. So when both Ramesh and Suresh were receiving their key from hacker they will think that approval reply from their corresponding communicator.

So to reduce the possibility of Man-In-The-Middle attack the secret keys recognized with digital signatures can reduce and also prevent the traditional man-in-the-middle attack, as the attacker cannot replica the signatures proposed in Liddell et al. [3] and Rivest et al. [4].

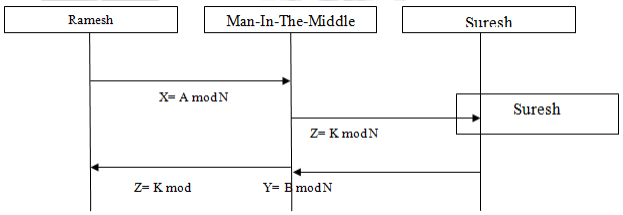

Figure 1. Connection establishments with secret key

DES:

DES is the Data Encryption Standard, a United States government standard encryption algorithm for encrypting and decrypting unclassified data. DES is described by Federal Information Processing Standards (FIPS). DES is a block cipher that takes a plaintext string as an input and creates a cipher text string of the same length. It uses a symmetric key, which means that the same key is used to convert cipher text back into plaintext. The DES block size is 64 bits. The key size is also 64 bits, although 8 bits of the key are used for similarity (error detection), which makes the effective DES key size 56 bits. A 56-bit key length is now considered to be weak due to advances in computer processing power.

The term Data Encryption Algorithm (DEA) is occasionally used, which describes the tangible algorithm

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

(as disparate to the standard). In this situation, TDEA is an acronym for Triple DES. Triple Data Encryption Algorithm Modes of operation presented in Coppersmith D [2]. For the sake of steadiness, we use this concept in our paper.

PROPOSED SYSTEM:

In the proposed system it has the digital signature in the secret key with the mathematical concept, i.e., perfect square. In Perfect square concept, the both sender and receiver have to send only the perfect square number as the secret key for communication. When Sender send any perfect square value with secret key , then the receiver should also send any perfect square value to sender, then only the communication will be established between both sender and receiver. If sender receives any other value and not perfect square value then the sender will receive the notification like "Communication blocked with the Man-In-The-Middle-Attack". Here the man-in-the-middle doesn't know anything about what the key and what the model they are handling for communication. So he might send any random key to both sender and receiver and it'll leads the user to get the man-in-the-middle attack notification. Most probably it will reduce the possibility of man-in-the-middle attack.

In Figure 2, it shows that Ramesh send the key with perfect square value to Suresh for communication, the man-in-the-middle also trying to access their communication by randomly sending his keys to both Ramesh and Suresh. But when Suresh receive his key from the hacker he knows to reply for only the secret key with perfect square values. So that the hacker did not get any reply from Suresh and also Ramesh will receive the notification that "The Hacker Found."

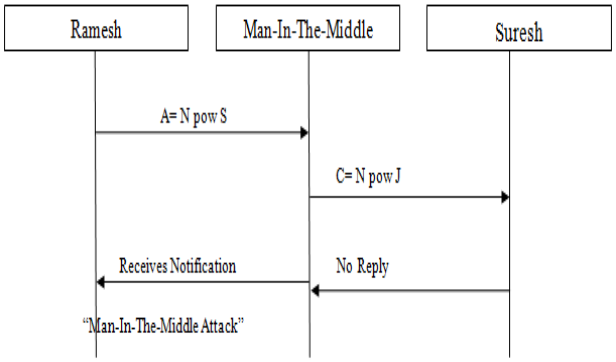

Figure. 2. Communicating from one node to another in the presence of Man-In-The-Middle.

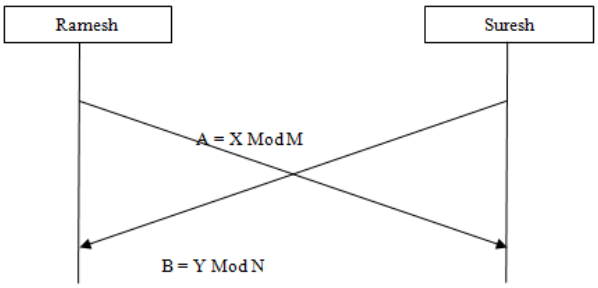

Figure 3. Checking whether Man-In-The-Middle is attacked or not.

To verify whether the received value is perfect square or not, the process will multiply the received value with sent perfect square value then divide those values with the sent perfect square value. If the result will be perfect

Implementation:

For the implementation of secret key with the digital signature, it follows the perfect square implementation algorithm for both sides of users. In our proposed process we try to eliminate the man-in-the-middle attack, so our approach would be such that the middle man could not change the key. The proposed technique is as follows: Suppose user1 wants to exchange key with user2. Both user1 and user2 use e as a secret number as the base of log.

Step 1: User 1 chooses a perfect square number M and calculates K1= log e (M).

Step 2: User 2 chooses a perfect square number M and calculates K2= log e (N).

Step 3: User 1 sends K1 to user 2, note that N is not known to user 1.

Step 4: User 2 sends K2 to user 1, note that M is not known to user 2.

Step 5: User 1 calculates Key= K1 + K2= log e (M) + log e (N) = log e (MN).

Step 6: User 2 calculates Key= K1 + K2= log e (N) + log e (M) = log e (NM) =log e (MN).

Step 7: Both user 1 and user 2 can check whether the key is being attacked or not by calculating as follows:

$$\text{elog e(MN)} = MN$$

Elimination of Man-in-the-Middle attack

Both user1 and user2 use a secret number e as the base of the log. If in the middle the key is attacked and the key is changed not necessarily the base will be e. As we can calculate K1=MN/M and K2=MN/N so we can easily catch the error. Here in the above figure 3, when Ramesh

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 4, April 2018

sends the secret key with perfect square like A= X mod M and if he receive B= Y mod N from Suresh then both of them will check whether their received value is perfect square or not as follows:

Ramesh calculates with the calculation K1=MN/M, if K1 is a perfect square number then key is not attacked by any intruder. Suresh calculates by computing K2=NM/N, if K2 is a perfect square number then key is not attacked else there is an intruder in the middle.

Algorithms

This algorithm iterates the encryption and decryption of data based on its requirements.

User 1

```
1.  ServerSocket ss=new ServerSocket(9500)
2.  Socket s=ss.accept()
3.  double key1, key2
4.  key1=Math.log10(m)
5.  key2=Math.log10(n)
6.  double key=key1+key2
7.  double key_check=Math.pow(10.00, Math.log10(m*n))
8.  double check=Math.round(key_check/m)
9.  if((Math.sqrt(check)*10)%10==0.0)
10. byte[] b=s1.getBytes()
11. int len=b.length
12. int arr1[]=new int[len]
13. char[] c=new char[len]
14. for(int i=0;i<len;i++)
15. arr1[i]=b[i]-(int)Math.round(key)
16. c[i]=(char)arr1[i]
17. end for
18. end if
```

User 2

```
1.  Socket s=new Socket (InetAddress.getLocalHost(),9500)
2.  Scanner ip=new Scannner(System.in)
3.  Double key1,key2
4.  key1=Math.log10(m)
5.  key2=Math.log10(n)
6.  double key=key1+key2
7.  byte[] b=s1.getBytes()
8.  int len=b.length
9.  int arr1[]=new int[len]
10. char[] c=new char[len]
11. for(int i=0;i<len;i++)
12. arr1[i]=b[i]+(int)Math.round(key)
13. c[i]=(char)arr1[i]
14. end for
```

CONCLUSION

Aim of this algorithm on the cryptographic field is one of the majorities challenging aspects. In reality exchanging it on internet without vulnerable is such a big deal. Whereas designing this algorithm we keep man-in-the-middle attack in mind while implementing. In this cipher we tried our finest to preserve that security side. On the other hand we can't say that man-in-the-middle attack can be fully eliminated because the base e selected by the middle man can be same as the secret key unfortunately. We use perfect square number to be the key were possibility is less when compared to prime number or the other methods that exist.

REFERENCES

1) Introduction to Modern Cryptography. Bellare, Mihir, Rogaway, Phillip 21 September 2005.
2) The Data Encryption Standard (DES) and its strength against attacks. Coppersmith D.
3) Liddell and Scott's Greek-English Lexicon. Oxford University Press. (1984)
4) Rivest, Ronald L. (1990). "Cryptology". In J. Van Leeuwen. Handbook of Theoretical Computer Science. 1. Elsevier.
5) I. Paul, Lenovo preinstalls man-in-the-middle adware that hijacks HTTPS traffic on new PCs. PC World, Feb 19, 2015.
6) G. N. Nayak and S. G. Samaddar, Different flavors of man-in-the-middle attack, consequences and feasible solutions, Chengdu, 3rd IEEE International Conference Volume 5, pp 491-495, 2010.
7) Mauro Conti, Nicola Dragoni, Viktor Lesyk, "A Survey of Man In The Middle Attacks", Communications Surveys & Tutorials IEEE, vol. 18, pp. 2027-2051, 2016, ISSN 1553-877X.
8) F. Callegati, W. Cerroni, M. Ramilli, "Man-In-The-Middle Attacks to https protocol", IEEE Security and Privacy, vol. 7, no. 1, pp. 78-81, Jan. -Feb. 2009.
9) Capec-94: Man in the Middle Attack, 2014
10) K. M. Haataja, K. Hypponen, "Man-in-the-middle attacks on Bluetooth: A comparative analysis a novel attack and countermeasures", Proc. 3rd Int. Symp. Commun. Control Signal (ISCCSP), pp. 1096-1102, 2008.
11) A. Ornaghi, M. Valleri, "Man in the middle attacks", Proc. Blackhat Conf. Eur., 2003.
12) R. Wagner, "Address resolution protocol spoofing and man-in-the-middle attacks" SANS Institute Reading Room site, Bethesda, Maryland, USA:, 2001.

13) Enrique de la Hoz, Gary Cochrane, Jose Manuel Moreira-Lemus, Rafael Paez-Reyes, Ivan Marsa-Maestre, Bernardo Alarcos, Detecting and Defeating Advanced Man-in-the-Middle Attacks Against TLS, 2014.
14) N. Karapanos, S. Capkun, "On the effective prevention of TLS man-in-the-middle attacks in web applications", IACR Cryptol. ePrint Arch., pp. 150, 2014.
15) X. Bai, L. Hu, Z. Song, F. Chen, K. Zhao, "Defense against DNS man-in-the-middle spoofing" in Web Information Systems and Mining, New York, NY, USA:Springer, pp. 312-319, 2011.
Cross Ref
16) Y. Yang et al., "Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid SCADA systems", Proc. Int. Conf. Sustain. Power Gener. Supply, vol. 7, pp. 1-8, 2012.
17) F. Fayyaz, H. Rasheed, "Using JPCAP to prevent man-in-the-middle attacks in a local area network environment", IEEE Potentials, vol. 31, no. 4, pp. 35-37, Jul./Aug. 2012.
18) J. Belenguer, C. T. Calafate, "A low-cost embedded IDS to monitor and prevent man-in-the-middle attacks on wired LAN environments", Proc. Int. Conf. SecureWare Emerging Secur. Inf. Syst. Technol., pp. 122-127, 2007.
19) Z. Trabelsi, K. Shuaib, "NIS04-4: Man in the middle intrusion detection", Proc. Global Telecommun. Conf. (GLOBECOM'06), pp. 1-6, 2006.
20) M.-H. Chiu, K.-P. Yang, R. Meyer, T. Kidder, "Analysis of a man-in-the-middle experiment with Wireshark", Proc. Int. Conf. Secur. Manage. (SAM'11), pp. 461-464, 2011.
21) H. Xia, J. C. Brustoloni, "Hardening Web Browsers against Man-in-the-Middle and Eavesdropping Attacks", Proc. 14th Int'l Conf. World Wide Web (IW3C2), pp. 489-498, 2005.
22) Yu Huang, Liang Jin, Na Li, Zhou Zhong, Xiaoming Xu, "Secret key generation based on private pilot under man-in-the-middle attack", Science China Information Sciences, vol. 60, pp. , 2017, ISSN 1674-733X.
[17]. Gowtham, M., and S. Sobitha Ahila. "Privacy enhanced data communication protocol for wireless body area network." In Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on, pp. 1-5. IEEE, 2017.