Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 17 Issue 5 Version 1.0 Year 2017
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Survey on Network Security

By C. Sridevi
NPR Arts And Science College

Abstract- Computer security is one of the most expected factor in the current & future industry. Nowadays computers are available in all places from home to big organization where they are all connected to networks. Hence the risk of data security is high whereas many algorithms are emerging according to the needs of various categories of people. Still we can see the security threats. In this paper I am going to present the threat attacks and the mechanisms that were used to secure data.

Keywords: security attacks, intrusion detection, hackers.

GJCST-E Classification: C.2.0, D.4.6

A Survey on Network Security

C. Sridevi

Abstract- Computer security is one of the most expected factor in the current & future industry. Nowadays computers are available in all places from home to big organization where they are all connected to networks. Hence the risk of data security is high whereas many algorithms are emerging according to the needs of various categories of people. Still we can see the security threats. In this paper I am going to present the threat attacks and the mechanisms that were used to secure data.

Keywords: security attacks, intrusion detection, hackers.

I. Introduction

There are many kinds of attacks in networking. Whereas we can classify into wired and wireless attacks. Here we are going to see about various attacks and attackers and defenders in this paper.

A *network* is basically all of the components (hardware and software) involved in connecting computers across small and large distances [2]. Networks are used to provide easy access to information, thus increasing productivity for users. There are following main types of networks:[1]

Personal area network (PAN): It is a network that is used for the communication among the personal system ad its connecting devices like printer, modem, telephone, etc. in close proximity limited to one person only.

Local area network (LAN): It is a network used for connecting two or more than two persons in a small geographical area like campus, office building, etc.

Wide area network (WAN): It is a network used for connecting people at large geographical area. Large numbers of LAN are connected with each other creating a WAN so as to connect almost whole world.

Metropolitan area network (MAN): It is a hybrid network ranging between LAN and WAN where the connecting devices lies within the city. It is mainly used by the co-operate companies who want to share data from its one branch to another in the same city.

Global area network (GAN): This network is used for supporting mobile across arbitrary number satellite coverage areas and wireless LANs etc. The key challenge in mobile communications is handing off user communications from one local coverage area to the next.

Virtual private network (VPN): It is a network which is maintained by companies who wants to do the private communication over the public network. The path between the two companies in VPN is encrypted and forming a tunnel for the safe communication.

II. Classification of Attackers

Hackers: He is a person who gains unauthorized access to data classified into inside and outside attacks.

Cracker: Detects vulnerability and take advantage over it To develop a secure system we consider the following:

Hacker Types:

Black hats
White hats
Grey hats
Blue hats

a) Various Types of Attacks

Vulnerability – Weak point used as entry point
Threat -
Attacks
Controls

4 Types of Attacks

1) Interception : Watches packets
2) Interruption : Steals or disturbs the data
3) Modification : Changes the data
4) Fabrication : Sends another message apart from original but having the same sender name.

b) Attacks on Password

Loose Lipped Systems: When System asks for password and username to typed in the system accepts username before the password is typed in where unrevealing the user name.

Exhaustive Attack: Tries all types of passwords

Probable likely for the user: Thinks of user familiarities and guesses what the password the user could might have choosen.

Plain text system password list: Accesses the password database directly.

c) Defending mechanisms

Password selection criteria: Carefully selecting password where one cannot guess so.

One time passwords: On every access changes password by giving a function and the user solves.

Encrypted password File: Even when the database is accessed the passwords cannot be accessed when it is stored in an encrypted form.

Author: Assistant Professor, Department of SW, BCA, NPR Arts & Science College, Natham. e-mail: c.sridevi1983@gmail.com

d) Other Attacks

i. *Phishing*

Unsuspecting user submits sensitive information in to a fraud system believing it is a trustworthy one.

ii. *Pharming*

Also called as DNS Spoofing. It changes DNS address of the original website. Redirects to fake website.

iii. *Packet Sniffing*

Hacker observes conversation between 2 conversation.

iv. *Packet Spoofing*

Hacker obverses conversation and also sends false packet with false address.

v. *Spreading Viruses*

Viruses spreads itself through networks and through all medias.

Virus Types:

Parasitic Virus: Attach itself and spread

Memory resident virus: Stored in main memory and then spread to all executable files.

Stealth Virus: Remains undetected from antivirus.

Boot sector viruses: Starts whenever the system gets booted.

Polymorphic Virus: Changes code every time it copies to other.

Metamorphic Virus: Keeps rewriting itself every time.

e) Other Attacks

Packet Sniffing: In networks attacker observes packets between two conversation.

Packet Spoofing: Attacker receives the message of the sender and in turn sends another message with false address.

Phishing: Creates duplicate website with simple modification to the original website , if user access this page their secret data like online bank passwords and security questions and answers will be accessed through the website. This will be used to steal and transfer their money.

Pharming (DNS Spoofing): This will create a website duplicating the DNS address itself where whenever the website is tried to access this website will be loaded.

III. Various Algorithms

a) Data Encryption Standard (DES)

DES was the result of a research project set up by International Business Machines (IBM) Corporation in the late 1960‟ s which resulted in a cipher known as LUCIFER. DES is based on a cipher known as the Feistel block cipher. It consists of a number of rounds where each round contains bit-shuffling, nonlinear substitutions (S-boxes) and exclusive OR operations. Once a plain-text message is received to be encrypted, it is arranged into 64 bit blocks required for input. If the number of bits in the message is not evenly divisible by 64, then the last block will be padded. DES performs an initial permutation on the entire 64 bit block of data. It is then split into 2, 32 bit sub-blocks, Li and R I which are then passed into 16 rounds. The output of this final permutation is the 64 bits ciphertext.

b) AES (Advanced Encryption Standard)

AES is also known as the Rijndael's algorithm, is a symmetric block cipher. It was recognized that DES was not secure because of advancement in computer processing power. It encrypts data blocks of 128 bits using symmetric keys. It has a variable key length of 128, 192 or 256 bits : by default 256 is used. AES encrypts 128 bit data block into 10, 12 and 14 rounds according to the key size. AES can be implemented on various platforms such as small device encryption of AES is fast and flexible. AES has been tested for many security applications. The purpose of NIST was to define a replacement for DES that can be used in non-military information security applications by US government agencies.

c) Blowfish

It is one of the most public domain encryption algorithms. Blowfish was designed in 1993 by Bruce Schneider as a fast alternative to existing encryption algorithms. Blowfish is a symmetric key block cipher that uses a 64 bit block size and variable key length from 32 bits to 448 bits. Blowfish has 16 rounds or less. Blowfish is a very secure cipher and to use encryption free of patents and copyrights. No attack is successful against Blowfish, although it suffers from weak key problem.

d) IDEA(International Data Encryption Algorithm)

IDEA is a block cipher algorithm and it operates on 64-bit plaintext blocks. The key size is 128 bits long. The design of algorithms is one of mixing operations from different algebraic groups. Three algebraic groups are mixed, and they are easily implemented in both hardware and software: XOR, Addition modulo 216, Multiplication modulo 216 + 1. All these operations operate on 16-bit subblocks. This algorithm is efficient on 16-bit processors. IDEA is symmetric key algorithm based on the concept of Substitution- Permutation Structure, is a block cipher that uses a 64 bit plain text with 8 rounds and a Key Length of 128-bit permuted into 52 subkeys each of 128- bits. It does not contain Sboxes and same algorithm is used in reversed for decryption.

e) RC4

RC4 is a stream cipher symmetric key algorithm. as the data stream is simply XOR with generated key sequence. It uses a variable length key 256 bits to initialize a 256- bit state table. A state table is used for generation of pseudo-random bits which is XOR with the plaintext to generate the cipher text.

f) RC6

RC6 is a derivative of RC5. RC6 is designed by Matt Robshaw, Ron Rivest Ray Sidney and is a symmetric key algorithm that is used to congregate the requirements of AES contest. RC6 was also presented to the CRYPTREC and NESSIE projects. It is patented by RSA Security . RC6 offers good performance in terms of security and compatibility. RC6 is a Feistel Structured private key algorithm that makes use a 128 bit plain text with 20 rounds and a variable Key Length of 128, 192, and 256 bit. As RC6 works on the principle of RC that can sustain an extensive range of key sizes, word-lengths and number of rounds, RC6 does not contain S-boxes and same algorithm is used in reversed for decryption.[4]

g) Serpent

Serpent is an Advanced Encryption Standard (AES) competition, stood 2nd to Rijndael, is a symmetric key block cipher, designed by Eli Biham, Ross Anderson, and Lars Knudsen. Serpent is a symmetric key algorithm that is based on substitution permutation network Structure. It consists of a 128 bit plain text with 32 rounds and a variable Key Length of 128, 192 and 256 bit. It also contains 8 S- boxes and same algorithm is used in reversed for decryption. Security presented by Serpent was based on more conventional approaches than the other AES finalists. The Serpent is open in the public sphere and not yet patented.[4]

h) Twofish

Twofish is also a symmetric key algorithm based on the Feistel Structure and was designed by Bruce Schneier along with Doug Whiting, John Kelsey, David Wagner, Niels Ferguson and Chris Hall,. The AES is a block cipher that uses a 128 bit plain text with 16 rounds and a variable Key Length of 128, 192, 256 bit. It makes use of 4 S-boxes (depending on Key) and same algorithm is used in reversed for decryption. The inventors extends the Blowfish team to enhance the earlier block cipher Blowfish to its modified version named Twofish to met the standards of AES for algorithm designing. It was one of the finalists of the AES, but was not selected for standardization. The Twofish is an open to public sphere and not yet patented. [4]

i) TEA

TEA is also a Feistel Structured symmetric key algorithm. TEA is a block cipher that uses a 64 bit plain text with 64 rounds and a Key Length of 128-bit with variable rounds having 32 cycles. It does not contain S-boxes and same algorithm is used in reversed for decryption. TEA is designed to maximize speed and minimize memory footprint. Cryptographers have discovered three related-key attacks on TEA. Each TEA key can be found to have three equal keys, thus it can be used as a hash function. David Wheeler and Roger Needham have proposed extensions of TEA that counter the above attacks.[4]

j) CAST

CAST is symmetric key algorithm based on the backbone concept of Feistel Structure. It is designed by Stafford Taveres and Carlisle Adams, is considered to be a solid algorithm. The CAST is a block cipher that uses a 64 bit plain text with 12 or 16 rounds and a variable Key Length of 40 to128-bit. It also contains 4 S-boxes and same algorithm is used in reversed for decryption. Bruce Schneier, John Kelsey, and David Wagner have discovered a related-key attack on the 64 bit of CAST that requires 217 chosen plaintexts, one related query, and 248offline computations. CAST is patented, which was generously released it for free use.[4]

IV. Security Protocols

a) Secure Socket Layer

It is used in secure exchange of information between web browser and web server. It gives 2 security services.

1. Authentication
2. Confidentiality

It has five layers

Application Layer
Secure Socket Layer
Transport Layer
Internet Layer
Data Link Layer
Physical Layer

SSL layer perform encryption on the data received and supports an algorithm called Fortezza.

b) Transport Layer uses HMAC

SSL have 3 sub protocol

Handshake protocol– Connection Establishment.

Record protocol –Actual message protocol.

Alert Protocol - If client/ server detects error other party discloses the connection and the secret key is deleted.

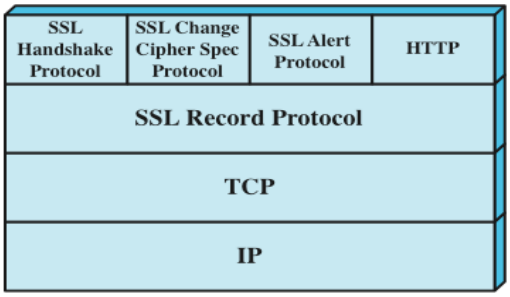


Fig.1

SSL is attacked by Buffer Overflow.

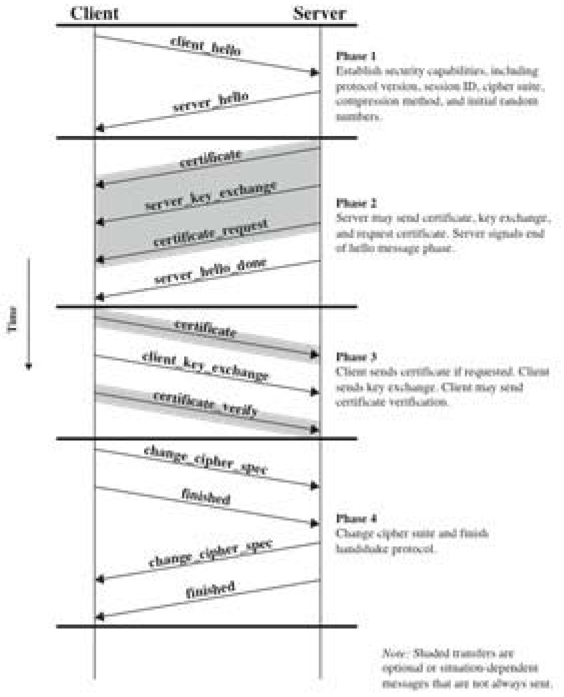

Client
Server
client_hello
server_hello
Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.
certificate
server_key_exchange
certificate_request
server_hello_done
Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.
Time
certificate
client_key_exchange
certificate_verify
Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.
change_cipher_spec
finished
change_cipher_spec
finished
Phase 4
Change cipher suite and finish handshake protocol.
Note: Shaded transfers are optional or situation-dependent messages that are not always sent.

Fig. 2: Handshake protocol action

c) *SHTTP- Secure HTTP*

Combination of HTTP and SSL to implement secure communication between a Web browser and a Web server SSL don't differentiate different messages. SHTTP is similar to SSL but work on individual messages.

d) *Internet Protocol Security (IPSec)*

Although it was designed to run in the new version of the Internet Protocol, IP Version 6 (IPv6), it has also successfully run in the older IPv4 as well.

IPSec sets out to offer protection by providing the following services at the network layer:

Access Control: To prevent an unauthorized access to the resource.

Connectionless Integrity: To give an assurance that the traffic received has not been modified in any way.

Confidentiality: To ensure that Internet traffic is not examined by non-authorized parties. This requires all IP datagrams to have their data field, TCP, UDP, ICMP or any other datagram data field segment, encrypted.

Authentication: Particularly source authentication so that when a destination host receives an IP datagram, with a particular IP source address, it is possible to be sure that the IP datagram was indeed generated by the host with the source IP address. This prevents spoofed IP addresses.

Replay protection: To guarantee that each packet exchanged between two parties is different.

IPSec protocol achieves these objectives by dividing the protocol suite into two main protocols:

1. Authentication Header (AH) protocol
2. Encapsulation Security Payload (ESP) protocol.

The AH protocol provides source authentication and data integrity but no confidentiality.

The ESP protocol provides authentication, data integrity, and confidentiality. [5]

IPSec operates in two modes: transport and tunnel:

i. *Transport Mode*

The Transport mode provides host-to-host protection to higher layer protocols in the communication between two hosts in both IPv4 and IPv6.

ii. *Tunnel Mode*

Tunnel mode offers protection to the entire IP datagram both in AH and ESP between two IPSec gateways. This is possible because of the added new IP header in both IPv4 and IPv6. Between the two gateways, the datagram is secure and the original IP address is also secure.

e) *SET - Secure Electronic Transactions*

SET[6] is a protocol specifically designed to secure payment-card transactions over the Internet. It was originally developed by Visa International and MasterCard International in February 1996 with participation from leading technology companies around the world.

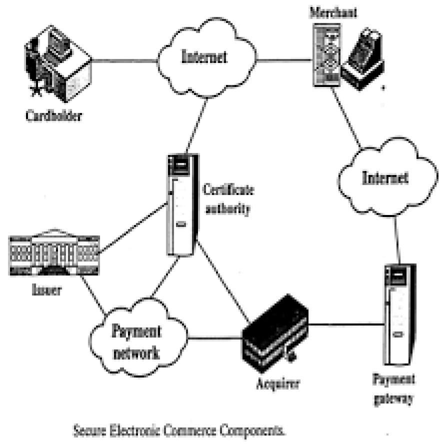
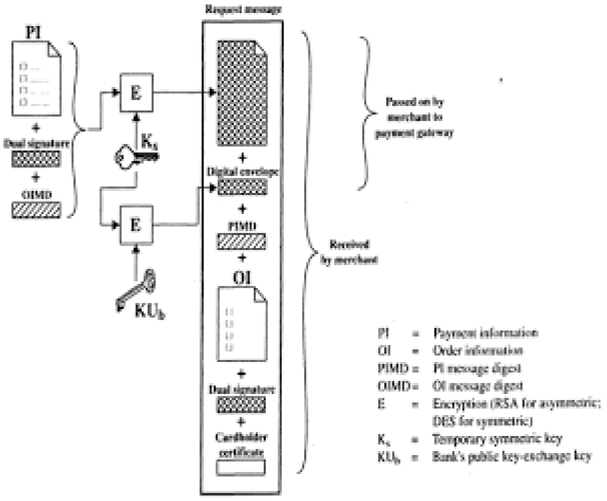


Fig. 3

1. Bob indicates to Alice that he is interested in making a credit card purchase.
2. Alice sends the customer an invoice and a unique transaction identifier.
3. Alice sends Bob the merchant's certificate which includes the merchant's public key. Alice also sends the certificate for her bank, which includes the

bank's public key. Both of these certificates are encrypted with the private key of a certifying authority.

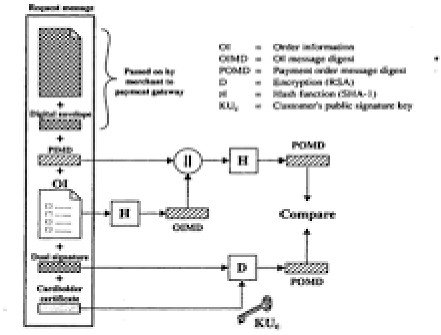
4. Bob uses the certifying authority's public key to decrypt the two certificates. Bob now has Alice's public key and the bank's public key.
5. Bob generates two packages of information: the order information (OI) package and the purchase instructions (PI) package. The OI, destined for Alice, contains the transaction identifier and brand of card being used; it does not include Bob's card number. The PI, destined for Alice's bank, contains the transaction identifier, the card number and the purchase amount agreed to Bob. The OI and PI are dual encrypted: the OI is encrypted with Alice's public key; the PI is encrypted with Alice's bank's public key. (We are bending the truth here in order to see the big picture. In reality, the OI and PI are encrypted with a customer-merchant session key and a customer-bank session key.) Bob sends the OI and the PI to Alice.



Cardholder Sends Purchase Request.

Fig. 4

6. Alice generates an authorization request for the card payment request, which includes the transaction identifier.
7. Alice sends to her bank a message encrypted with the bank's public key. (Actually, a session key is used.) This message includes the authorization request, the PI package received from Bob, and Alice's certificate.
8. Alice's bank receives the message and unravels it. The bank checks for tampering. It also make ssure that the transaction identifier in the authorization request matches the one in Bob's PI package.
9. Alice's bank then sends a request for payment authorization to Bob's payment-card bank through traditional bank-card channels -- just as Alice's bank would request authorization for any normal payment-card transaction.



Merchant Verifies Customer Purchase Request.

Fig. 5

One of the key features of SET is the non-exposure of the credit number to the merchant. This feature is provided in Step 5, in which the customer encrypts the credit card number with the bank's key.

Encrypting the number with the bank's key prevents the merchant from seeing the credit card. Note that the SET protocol closely parallels the steps taken in a standard payment-card transaction. To handle all the SET tasks, the customer will have a so-called digital wallet that runs the client-side of the SET protocol and stores customer payment-card information (card number, expiration date, etc.)

V. Conclusion

This papers dealt with various attacks on networks and the defencing mechanisms present. Many algorithms have been developed as an measure to secure the system. All the algorithms are useful based on the requirement as and when needed. Various security mechanisms and security protocols are available.

References Références Referencias

1. Dr. Parminder Singh Assistant Professor (Department of Information Technology) Chandigarh Group of Colleges, Landran, Mohali, Punjab, India. “A Survey on Different aspects of Network Security in Wired and Wireless Networks” in International Journal of Latest Trends in Engineering and Technology (IJLTET)
2. http://computernetworkingnotes.com/network-technologies/basic-networking.html
3. “Cryptography and Network Security” – Behrouz A. Forouzon.
4. “A Survey On Various Encryption And Decryption Algorithms M.Chanda Mona et al.,” International Journal of Security (IJS) Singaporean Journal of Scientific Research(SJSR) Vol.6.No.6 2014 Pp. 289-300.

5. Kizza Guide to Network Security.
6. Creative World 9 – Website.
7. ”Cryptography and Network Security” – Atul Kahate
8. Gurjeevan Singh, Ashwani Kumar Singla,K.S. Sandha, ”Through Put Analysis Of Various Encryption Algorithms”, IJCST Vol. 2, Issue 3, September 2011.
9. Deepak Kumar Dakate, Pawan Dubey,“ Performance Comparison of Symmetric Data Encryption Techniques “, International Journal of Advanced Research in Computer Engineering & Technology, Volume 3, No. 8, August 2012, pp . 163-166.
10. Shashi Mehrotra Seth, Rajan Mishra,” Comparative Analysis Of Encryption Algorithms For Data Communication”, IJCST Vol. 2, Issue 2, pp.192- 192 *June 2011.*
11. Agarwal, R., Dafouti, D., Tyagi, S. “Peformance analysis of data encryption algorithms “, Electronics Computer Technology (ICECT), 2011 3rd International Conference, vol.5, April 2011, pp. 399 – 403.