

Introduction to Network Security

Dr. Rahul Banerjee

Computer Science & Information Systems Group

Self-Instructional Material (SIM): Module 01

Course Number: SS ZG 513

Course Title: Network Security

Second Semester: 2005-2006



Birla Institute of Technology & Science, Pilani (India)

Dedication

This work is dedicated to my past and present students who have been a source of joy and who have provided me a reason to take up this small enterprise.

-Rahul Banerjee

Objectives & Scope of This Course

- Introduction to the fundamental aspects of security in a modern networked environment
- Focus on system design aspects and cryptography in the specific context of network / internetwork security
- Study of elements of cryptographic techniques, algorithms and protocols
- Study of system/application design issues in building secure networked systems
- Designing effective Internetwork Security Systems
- Analyzing these designs from viewpoints of real-life security needs vis-à-vis current best practices and evolving trends

© Dr. Rahul Banerjee, BITS-Pilani, India <1998-2006>

No part of this work can be published, copied, edited, re-distributed or used in any other way not explicitly permitted herein without the written permission of the Author.

CONTENTS

<i>Preface</i>	<i>i</i>
Chapters	
1. Introduction	4
<i>Learning Objectives</i>	
1.1. Introduction	
1.2. Need for Security of Computer Networks	
1.3. Elements of Network Security	
1.4. Cryptography as an Instrument of Network Security	
1.5. Symmetric-Key Cryptography	
1.6. Safety of Cryptographic Schemes	
1.7. Types of Cryptographic Attacks	
1.8. Substitution Ciphers	
1.9. Transposition Ciphers	
1.10. Principles of Design of Good Cryptographic Mechanisms	
1.11. The Data Encryption Standard (DES)	
1.12. The International Data Encryption Algorithm (IDEA)	
1.13. The Advanced Encryption Standard (AES)	
1.14. Select Elements of Network Security Systems	
1.15. Current Trends	
1.16. Concluding Remarks	
<i>Summary</i>	
<i>Recommended Readings</i>	
<i>Self-Test Questions</i>	
<i>Exercises</i>	
Appendices	
A. Mathematical Concepts of Relevance	16
B. Relevant on-line resources at author's website	18

Chapter-1 Introduction

Learning Objectives:

- Understanding the concepts of security as applicable to computer networks and internetworks of any kind
- Recognizing elements of network and security
- Realizing the significance of cryptographic mechanisms in the context of network security
- Understanding the scope of security schemes and their consequent design limitations

1.1 Introduction

A Computer Network is an interconnected group of autonomous computing nodes which use a well-defined, mutually-agreed set of rules and conventions known as Protocols, interact with one-another meaningfully and allow resource-sharing preferably in a predictable and controllable manner. Study of methods of analysis of security requirements and needs of such systems and consequent design, implementation and deployment is the primary scope of the discipline named as Network Security. Although named as network security, the principles and mechanisms involved herein do apply to internetworks as well.

1.2 Need for Security of Computer Networks

Security is often viewed as the need to protect one or more aspects of network's operation and permitted use (access, behaviour, performance, privacy and confidentiality included). Security requirements may be Local or Global in their scope, depending upon the network's or internetwork's purpose of design and deployment.

Criteria for evaluating security solutions include ability to meet the specified needs / requirements, effectiveness of approach across networks, computing resources needed vis-à-vis the value of the protection offered, quality and scalability, availability of monitoring mechanisms, adaptability, flexibility, practicability from sociological or political perspective economic considerations and sustainability.

Security Attacks compromises the information-system security. Active attacks involve *active attempts on security leading to modification, redirection, blockage or destruction of data, devices or links. Passive attacks involve simply getting access to link or device and consequently data.*

Security Threats are those having potential for security violation. Security Mechanism is a mechanism that detects / locates / identifies / prevents / recovers from "security attacks". Security Service is a service that enhances security, makes use of the security mechanisms.

Importance of identification of sources cannot be underestimated. Strategic importance applies to planning, preventing and / or countering whereas other variety of importance is with respect to Sensitivity-analysis and Economic -impact-analysis and pro-active protection.

Network Security-specific monitoring approaches can be either Log-based or Agent-based type; whereas Non-monitoring approaches can be either Model-based or Experimental Replication-based.

1.3 Elements of Network Security

Primary elements of security of any computer network include security provisioning at the Sending Node, Intermediate Forwarding Node, Receiving Node, interconnection links and mechanism of transmission / reception at physical and logical levels. Extraneous factors that these elements may be influenced by may include various kinds of external and internal attacks, unintentional leakages and location of devices involved in communication. Apart from the obvious networking elements, network security is also influenced by the System and Application Software security provisioning or lack of it on individual nodes.

1.4 Cryptography as an Instrument of Network Security

It aims to handle network-specific or internetwork-specific issues and problems involving authentication, integrity and secrecy / confidentiality / privacy. Cryptography can exist with or without networks but Network Cryptography / Internet Cryptography specifically addresses the needs / requirements of networks / internetworks and is thus a subset of general cryptography.

Cryptography is broadly classified into two types: Symmetric-Key Cryptography (conventional) and Asymmetric-Key Cryptography.

1.5 Symmetric-Key Cryptography

Symmetric-Key cryptography is called so since in this class of cryptographic algorithms, encryption as well as decryption processes are performed using the same (i.e. symmetric) key. The algorithms / schemes / programs that use this paradigm are often termed as Symmetric-Key Ciphers / Private-Key Ciphers / Secret-Key Ciphers / Conventional Ciphers etc. In such cases, Plaintext, Encryption-Decryption Algorithm, Key and Ciphertext form four basic components of the Symmetric Cipher Model. Such schemes *should* exhibit security of Key Distribution to the legal recipients and adequate strength of encryption.

Characterizing the Symmetric Key Ciphers is often done by Choice of key-space, Key-derivation / identification within the key-space, number of cycles involved in encryption / decryption process, choice of operations (or choice of type of operators) that are used in the process of encryption / decryption, number of internal algorithms that form the final scheme of enciphering / deciphering, role, if any, of the compression algorithms / schemes in adding the security value etc.

Terms like Conventional / Private-Key / Secret-Key / Symmetric-Key cryptography are interchangeably used in literature.

1.6 Safety of Cryptographic Schemes

Any cryptographic scheme is safe if and only if it is unbreakable in reasonable time using feasible resources in spite of the intruder's being aware of the encryption and decryption algorithm and size of the key. Strength of the algorithm and the size of key remain two important factors in Cryptography. Unconditionally secure and Computationally secure schemes of cryptography do exist; but in practice involving computers, only the latter is popular.

1.6.1 Unconditionally Secure Encryption schemes

Here, the generated *Ciphertext* simply *does not have adequate information* to allow *discovery of the unique plaintext irrespective of the amount of Ciphertext available (as well as irrespective of the computational resource available)* to the attacker.

1.6.2 Computationally Secure Encryption schemes

Here, the *cost of deciphering exceeds the value of enciphered information and the time needed to decipher exceeds the lifetime of the enciphered information.*

1.6.3 Kerckhoff's Principle

Security of conventional encryption depends only upon the Secrecy of the Key, and not on the Secrecy of the Algorithm.

Therefore, requirements for secure deployment of conventional cryptography are availability of a strong Encryption Algorithm and secure distribution of the Secret Key to the intended recipients. *Kerckhoff's Principle remains a guiding line for the research on conventional cryptography and its real-life use in internetworks.*

1.7 Types of Cryptographic Attacks

Classification of such attacks may be of several types such as: classification based on the approach of mounting attacks that involves *Brute-force Attacks* and *Cryptanalytic Attacks (Differential cryptanalytic attacks and Linear cryptanalytic attacks included)*, classification based on the attacks that try to recover Keys including the *Ciphertext-only attacks (here, the attacker has only the Ciphertext, Known Plaintext attacks (the attacker has the Ciphertext of some known plaintext), Chosen Plaintext attacks (the attacker has the Ciphertext of some chosen plaintext) and Chosen Ciphertext attacks (here, Ciphertext and corresponding plaintext are chosen); and finally, classification based on the attacks that focus upon discovering the difference between the actual and expected (ideal) cipher like the *Distinguishing attacks (exploit imperfections of encrypting functions).**

1.8 Substitution Ciphers

These use *substitution* of symbols, sets of symbols, groups of sets by one or more symbols, sets of symbols or group of symbols. For instance, one such scheme, *Caesar Cipher uses letter-by-letter substitution*. Current letter is replaced in this scheme by the letter standing three places after. It has, thus for the English language, only 25 keys. Its basic weakness is the small key-space, cannot survive frequency analysis.

In *Monoalphabetic Substitution Ciphers* instead of 'n-1' keys, the cipher could be made using 'n!' permutations. This increases the Key-Space and provides greater security. Its primary weakness is that it cannot survive frequency analysis.

Basic idea of *Playfair Cipher* is to Treat 'Digrams' in the input plaintext as a single unit and map these units into corresponding ciphertext 'Digrams' using a 5x5 matrix and applying a set of four rules to it.

Steps involved:

- Select a keyword
- Fill the rest of the matrix with non-repeating letters
- Use four rules:
 - Consecutive paired repeated letters to be separated by a filler letter.
 - Letter in the same row to be replaced by the letter to the right with the first element found circularly
 - Ditto for same column letter!
 - Otherwise plain one-to-one replacement

Hill Cipher's basic idea is to take 'n' successive plaintext letters and substitute this set by another set of 'm' ciphertext letters using 'm' linear equations and a set of associated rules.

Polyalphabetic Substitution Ciphers' basic idea is to use multiple different monoalphabetic substitutions through the process of encryption using a set of governing rules and a key that is used to fire a particular rule.

1.9 Transposition ciphers

These ciphers attempt to exploit the power of permutation on the plaintext symbols / letters. In real-life these ciphers *complement* the Substitution ciphers. Example of Transposition ciphers includes the simple *Rail-fence cipher*. Here letters of plaintext are organized as a sequence of diagonal elements *of depth 'k'* while writing; and, the ciphertext gets generated when these elements are read out as the resultant rows. However, it is very easy to break unless the encoding scheme is used with any other scheme for the final effect. Cannot withstand frequency analysis in its purest form.

1.10 Design Principles of Modern Cryptographic Algorithms

Keep the design-complexity to the minimum and remember greater the complexity, higher are the risks that the security analysis would be difficult or imperfect. This may, therefore, result in lower security in real practice. *Design must ensure that each part of the solution works correctly irrespective of the external elements' failure.* In other words, correctness of the design should be treated as a local property.

1.10.1 Principles of Modern Block Cipher Design

The design-complexity must be kept to the minimum in order to minimize the risks arising out of possibly inadequate cryptanalysis of complex design. Design must ensure that each part of the solution works correctly irrespective of the external elements' failure. Number of rounds should be decided based on minimum acceptable security that allows the required degree of computational security. The Cipher function should be designed to be preferably directly reversible for decryption. Key-scheduling algorithm must be carefully crafted to maximize the combined effect of Rounds, Cipher function and itself. The choices of these design parameters should be such that Cryptanalytic attacks to search keys should require more intensive effort than its brute force counterpart. A good scheme should also consider the computing power and efficiency aspects keeping the targeted class of applications in view.

1.10.2 Design criteria for the Cipher function:

It should be difficult to unscramble the substitutions (confusion) performed by the Cipher function. This, in turn, requires the Cipher function to be non-linear as the difficulty-level increases with the non-linearity of this function. Algorithm must have good 'Avalanche properties', i.e. a one-bit change in input must produce change in many bits of the output. Strict Avalanche Criterion (AVC) requires that any output bit 'm' of a substitution-box should change with the probability of 0.5 when any single input bit 'n' is inverted for all 'n, m'. Bit-Independence Criterion' (BIC) suggests the requirement of change of output bits 'x' and 'y' to be changed independent of the inversion of single input bit 'z'.

1.11 The Data Encryption Standard (DES)

Better known as *DES*, this conventional cryptographic scheme has been standardized and has run into some revisions ever since IBM decided to open the DES to the outside world. The NIST of the USA has published the DES standard, in 1999, as *FIPS PUB 46-3*. The *FIPS PUB 46-3* works in accordance to another NIST recommendation: *FIPS 140-1*. A related document that completes the entire set is the *ANSI X 9.52* standard published by the ANSI of the USA.

A *DES* key-space consists of *64 bits* of which *56 bits* are randomly generated and used directly by the algorithm. The remaining *8 bits*, which are not used by the algorithm, *may* be used for *error detection*. The *8 error detecting bits* are set to make the *parity of each octet* of the key *odd*.

Keys can also be generated in an encrypted form. In this case, a random 64-bit number is generated and defined to be the ciphertext formed by the encryption of a key using a key encrypting key (KEK). Here, obviously, the parity bits of the encrypted key cannot be set prior to key's decryption.

Steps involved:

- A block to be encrypted is subjected to an *initial permutation IP*.
- Next, this permuted plaintext is subjected to a complex *key-dependent computation using two functions called cipher function and key schedule function respectively*.
- Finally, the resultant data is subjected to a *final permutation* which is the inverse of the initial permutation *IP-1*.
- The key-dependent computation is defined in terms of a function *f*, called the cipher function, and a function *KS*, known as the key schedule.
- Cipher function *f* is defined in terms of primitive functions which are called the *selection function Si* and the *permutation function P*.

Primitive Functions for the DES

The choice of the primitive functions *KS, S1,...,S8* and *P* is critical to the strength of encryption.

The primitive functions *S1,...,S8* are:

S1

14 4 13 1 2 15 11 8 3 10 6 12 5 9 0 7
 0 15 7 4 14 2 13 1 10 6 12 11 9 5 3 8
 4 1 14 8 13 6 2 11 15 12 9 7 3 10 5 0
 15 12 8 2 4 9 1 7 5 11 3 14 10 0 6 13

S2

15 1 8 14 6 11 3 4 9 7 2 13 12 0 5 10
 3 13 4 7 15 2 8 14 12 0 1 10 6 9 11 5
 0 14 7 11 10 4 13 1 5 8 12 6 9 3 2 15
 13 8 10 1 3 15 4 2 11 6 7 12 0 5 14 9

S3

10 0 9 14 6 3 15 5 1 13 12 7 11 4 2 8
 13 7 0 9 3 4 6 10 2 8 5 14 12 11 15 1
 13 6 4 9 8 15 3 0 11 1 2 12 5 10 14 7
 1 10 13 0 6 9 8 7 4 15 14 3 11 5 2 12

S4

7 13 14 3 0 6 9 10 1 2 8 5 11 12 4 15
 13 8 11 5 6 15 0 3 4 7 2 12 1 10 14 9
 10 6 9 0 12 11 7 13 15 1 3 14 5 2 8 4
 3 15 0 6 10 1 13 8 9 4 5 11 12 7 2 14

S5

2 12 4 1 7 10 11 6 8 5 3 15 13 0 14 9
 14 11 2 12 4 7 13 1 5 0 15 10 3 9 8 6
 4 2 1 11 10 13 7 8 15 9 12 5 6 3 0 14
 11 8 12 7 1 14 2 13 6 15 0 9 10 4 5 3

S6

12 1 10 15 9 2 6 8 0 13 3 4 14 7 5 11
 10 15 4 2 7 12 9 5 6 1 13 14 0 11 3 8
 9 14 15 5 2 8 12 3 7 0 4 10 1 13 11 6
 4 3 2 12 9 5 15 10 11 14 1 7 6 0 8 13

S7

4 11 2 14 15 0 8 13 3 12 9 7 5 10 6 1
 13 0 11 7 4 9 1 10 14 3 5 12 2 15 8 6
 1 4 11 13 12 3 7 14 10 15 6 8 0 5 9 2
 6 11 13 8 1 4 10 7 9 5 0 15 14 2 3 12

S8

13 2 8 4 6 15 11 1 10 9 3 14 5 0 12 7
 1 15 13 8 10 3 7 4 12 5 6 11 0 14 9 2

7 11 4 1 9 12 14 2 0 6 10 13 15 3 5 8
 2 1 14 7 4 10 8 13 15 12 9 0 3 5 6 11

The primitive function P is:

16 7 20 21
 29 12 28 17
 1 15 23 26
 5 18 31 10
 2 8 24 14
 32 27 3 9
 19 13 30 6
 22 11 4 25

In a nut shell, the process involves Initial Permutation (IP) as performed on the 64-bit plaintext block, partitioning of IP output, Key transformation (56-bit key is taken and partitioned in two parts 28-bit (for Rounds 1,2,9,16) or 28-bit (for all other rounds) circular left shifting is performed on each part using Compression Permutation (a 48-bit sub-key is generated in each round), Expansion Permutation (it is performed on the right 32-bit part of the plaintext to generate 48-bit output). Now, the 48-bit sub-key and 48-bit 'Right part of plaintext' are used for the defined operation, as discussed. The procedure in each round involves steps 3, 4 and 5. At the end of Round 16, 'L' and 'R' blocks are recombined and IP-1 is performed.

DES Strengths: key transformation, rounds, expansion permutation, cipher function, difficulty in efficient software implementation

DES Weaknesses: Single DES is breakable in reasonable time, IP and IP-1 do not add to security value, has weak keys (4), semi-weak key-pairs (6) and possibly weak keys (48) .

1.12 The International Data Encryption Algorithm (IDEA)

Its origin lies in the Proposed Encryption Standard (PES) that appeared in 1990. This led to the Improved PES (IPES) one year later. In 1992, IPES was renamed and slightly fine tuned as the International Data Encryption Algorithm (IDEA). In a way, after DES and before AES, the IDEA has been one of the most analyzed algorithms. It is a patented algorithm and needs to be licensed specifically for commercial use.

This scheme operates on 64-bit blocks of plaintext, uses a 128-bit key for encryption, mixes operations from different algebraic groups for added security value (XOR, Addition Modulo 2^{16} , Multiplication Modulo $2^{16} + 1$), operations are performed on 16-bit sub-blocks and does not involve any bit-level manipulation (unlike the DES). IDEA uses the same algorithm for encryption and decryption.

Steps involved:

- Take a 64-bit block of plaintext 'X' and divide it into 4 sub-blocks of 16-bit each: 'X1', 'X2', 'X3' and 'X4'.
- Take the 128-bit Key, expand it and generate 52 sub-keys of 16-bit length.

(Here, each Round shall use only 6 sub-keys <4+2> of the 8 sub-keys generated using the '16-bit-chop & 25-bit-circular-left-shift' scheme. In other words, simply take eight 16-bit blocks in each Round, then perform circular left-shifting of the original 128-bit Key by 25 bits after every round until all 52 sub-keys have been generated in total.)

1.13 The Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is based on the winning entry out of several proposals submitted by cryptographers to the NIST during 1997-2000. NIST required all the entries to support block sizes of 128-bit length (at least) and key-sizes of 128, 192 and 256

bits. In October 2000, the NIST brought out the first version of the AES which was basically the *Rijndael Cipher* (pronounced as "*Reign Dahl*" -- a block cipher, designed by Vincent Rijmen and Joan Daemen). Rijndael's combination of security, performance, efficiency, ease of implementation and flexibility made it an appropriate choice. It became an official standard in 2001 through *FIPS-176*.

AES is based on the principle of *Iterative Block Ciphers*. It uses *arithmetic operations* in the *finite field* F_{2^8} . AES provides for 128, 192 and 256-bit *block* and *key sizes* and *allows any independent combination* of these. The *basic unit for cryptographic processing* in the AES scheme is a *byte* (an octet). The Input, Key and Output bit sequences are *processed as arrays of bytes* that are formed by dividing these sequences into *octets* so as to form *arrays of bytes*.

For an Input, Output or Key denoted by a , the bytes in the resulting array will be referenced using one of the two forms, a or $a[n]$, where n will be in one of the following ranges:

- Key length = 128 bits, $0 \leq n < 16$; Block length = 128 bits, $0 \leq n < 16$;
- Key length = 192 bits, $0 \leq n < 24$;
- Key length = 256 bits, $0 \leq n < 32$.

All *byte values* in the AES algorithm are presented as the *concatenation of its individual bit values* (0 or 1) between braces *in the order* $\{b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0\}$. These bytes are interpreted as *finite field elements* using a *polynomial representation*: $b_7x^7 + b_6x^6 + \dots + b_1x + b_0 = S \text{ bix}_i$ for $i=0..7$. Some finite field operations involve one *additional bit* (bit 8) to the left of an octet. Where this extra bit is present, it will appear as '{01}' immediately preceding the octet.

Arrays of bytes are represented in the form: $a_1 a_2 \dots a_{15}$. Internally, the AES operations are performed on a *two-dimensional array of bytes* called the *State*. The State consists of four rows of bytes, each containing N_b bytes, where N_b is the block length divided by 32. In the State array denoted by the symbol s , each individual byte has two indices, with its row number r in the range $0 \leq r < 4$ and its column number c in the range $0 \leq c < N_b$. This allows an individual byte of the State to be referred to as either s_r, c or $s[r, c]$. (For AES, $N_b=4$, i.e., $0 \leq c < 4$).

Therefore, at the beginning of the *Cipher* or *Inverse Cipher*, the *input array*, in , is copied to the *State array* according to the scheme: $s[r, c] = in[r + 4c]$ for $0 \leq r < 4$ and $0 \leq c < N_b$. At the end of the *Cipher* and *Inverse Cipher*, the *State* is copied to the output array out as: $out[r + 4c] = s[r, c]$ for $0 \leq r < 4$ and $0 \leq c < N_b$. The four bytes in each column of the State array form 32-bit words, where the row number r provides an index for the four bytes within each word. The state can hence be interpreted as a one-dimensional array of 32 bit words (columns).

1.14 Select Elements of Network Security Systems

In this section, we will briefly introduce a few terms of significance that we shall encounter quite often in the realm of system-level security of networked systems.

1.14.1 The Network Perimeter

A Network / Internetwork Perimeter is a secure boundary of a network that may include some or all of the Firewalls, Routers, IDS, VPN mechanisms, DMZ and Screened subnets. DMZ is outside the Firewall. Screened subnet is an isolated sub-network connected to a dedicated firewall interface.

1.14.2 Intrusion Detection System

Intrusion Detection System (IDS) is a system that comprises of mechanisms / devices involving one or more Intrusion Detection Sensors (traffic monitoring devices / mechanisms)

placed at security-wise strategic locations; and, has been designed to detect any known or likely intrusion into the protected network. Sensor reporting may involve several forms like logs, database updates, Email alerts etc.

Types of IDS:

- Network-based IDS (NIDS) : Subnet-resident
- Host-based IDS (HIDS) : Host resident

1.14.3 Firewall

Firewall is an internetwork security device that serves on the only access route that connects the internal network / internetwork (i.e. the segment to be protected) to the external network (s) / internetwork (s); and, decides about physically allowing / denying entry / exit to / from the protected segment using a set of policies (often manifested in terms of rules) is called a Firewall. A Firewall may be implemented in hardware / software / firmware or a combination of these.

Characteristically, an Internet Firewall exhibits security measures and internetwork-control-mechanisms related to but not necessarily limited to:

- Internet services as separated from the intranet services
- Service-based directional traffic
- User-specific / Class-specific / Group-specific service access
- Service-usage / deployment-behaviour
- Origin-specific / Destination-specific service / traffic / monitoring / QoS-security bindings
- Relaying / blocking / redirection of encapsulated and / or encrypted traffic

A common assumption (though debatable) made is that the Firewall itself is incorruptible / impenetrable. A firewall works under the assumption that it is solely responsible for blockade / allowance of any traffic between two or more than two networks / internetworks separated by it.

As part of an Internetwork Security System, a firewall:

- Allows defining exit and entry points for traffic from and to the internal protected network / intranet
- Offers a set of mechanisms and a set of locations / points for supervising security-sensitive activities / events / behaviour
- Provides network-level encapsulation, encryption, decryption, decapsulation, tunnelling services
- Permits a variable-security facility-zone's creation that may also offer some functionalities not necessarily related to the security function that is the primary function of the firewall
- Supports creation and interpretation of structured logging mechanisms and files for a variety of purposes.

A Firewall is not meant for:

- Virus / Worm / Trojan Horse / Logic bomb detection
- Virus / Worm / Trojan Horse / Logic bomb removal
- Semantic analysis of the application-to-application messages with certain exceptions
- Protecting a network / internetwork from a trusted entity (client / server / user) or an internal authorized user with adequate privileges
- Protecting from power, link or protocol failure

- Monitoring processes at individual workstations / servers / switches that are of local significance to that machine or network segment except for certain explicitly registered classes of processes / systems / users / patterns
- Guarding against traffic that bypasses the Firewall itself

Firewall Constituents: (some of these can serve as firewalls as well)

- Application-level Gateways and Proxies
- Transport-level / Circuit-level Gateways and Proxies
- Network-level Gateways / Routers
- Packet filters (also known as Static Packet Filtering Firewalls)
- Bastion Host
- Screened Host

Types of Firewalls may include Stateless Firewalls, Stateful Inspection-based Firewalls, Perimeter Firewalls, Screened Host Firewalls, Intranet Firewalls, Internet Firewalls and Extranet Firewalls.

1.14.4 Virtual Private Networks (VPNs)

A *Virtual Private Network* (VPN) is a mechanism that allows establishment of a *protected session* between *two network nodes / services* located in / on *two different protected networks / internetworks* separated by unprotected / untrusted / insecure (often public) networks / channels / infrastructure.

Another perspective: SSH, TLS, SSL, IPSec, L2TP, PPTP are choices providing different types of security at different layers. *Although, all of these could be reused in an appropriately designed VPN mechanism, often the L3 and L2 mechanisms are preferred by many VPN designers.* Often, people refer to a VPN as a security device / mechanism on the perimeter of the protected network / internetwork that allows encrypted sessions.

Advantages of VPNs include capability to access remote network as if there exists a private channel to that network, several security options available to provide a range of security, adequacy of lower-strength encryption schemes on certain occasions, cost-effectiveness if well-designed, well-implemented and well-configured in addition to the fact that these can be quickly implemented.

However, not all is rosy with the VPNs! Disadvantages include the high overheads (requirement of encryption, decryption, encapsulation and decapsulation induce a sizeable processing overhead, packet overhead and storage overheads) and latency as well as increase cost of service. In some cases, if designed ad-hoc, certain network installations may pose additional challenges in adding the VPN functionality due to the added overhead in packet processing. Intricate design issues, unless handled carefully, may actually serve to lower the network performance without really bring corresponding increase in the security level of the network. Implementation issues include VPN pass through issues, NAT-specific issues and MTU-size related issues. Also, troubleshooting of networks employing these devices becomes tricky.

1.15 Current Trends

Current trends in cryptographic security solutions to network and internetwork security problems use a clever combination of both the symmetric and asymmetric key cryptography. Quantum Key Exchange aspects of what is sometimes called Quantum Cryptography is being seen as a promising solution to the key exchange issues faced by the conventional cryptography.

1.16 Concluding Remarks

Network security requires a multi-pronged approach for a reasonably secure, easy to use and cost-effective solution. There are two important perspectives of analysis and design of secure networked systems: mathematical perspective (including cryptography) and system-level perspective (including device-level security aspects).

Summary

Although named as network security, the principles and mechanisms involved herein do apply to internetworks as well. Security Attacks compromises the information-system security. Security Threats are those having potential for security violation. Security Mechanism is a mechanism that detects / locates / identifies / prevents / recovers from “security attacks”. Security Service is a service that enhances security, makes use of the security mechanisms.

Cryptography can exist with or without networks but Network Cryptography / Internet Cryptography specifically addresses the needs / requirements of networks / internetworks and is thus a subset of general cryptography. The algorithms / schemes / programs that use this paradigm are often termed as Symmetric-Key Ciphers / Private-Key Ciphers / Secret-Key Ciphers / Conventional Ciphers etc. In such cases, Plaintext, Encryption-Decryption Algorithm, Key and Ciphertext form four basic components of the Symmetric Cipher Model. Such schemes should exhibit security of Key Distribution to the legal recipients and adequate strength of encryption.

Characterizing the Symmetric Key Ciphers is often done by Choice of key-space, Key-derivation / identification within the key-space, number of cycles involved in encryption / decryption process, choice of operations (or choice of type of operators) that are used in the process of encryption / decryption, number of internal algorithms that form the final scheme of enciphering / deciphering, role, if any, of the compression algorithms / schemes in adding the security value etc. Terms like Conventional / Private-Key / Secret-Key / Symmetric-Key cryptography are interchangeably used in literature. In real-life Transposition ciphers complement the Substitution ciphers.

A DES key-space consists of 64 bits of which 56 bits are randomly generated and used directly by the algorithm. Keys can also be generated in an encrypted form. In this case, a random 64-bit number is generated and defined to be the ciphertext formed by the encryption of a key using a key encrypting key (KEK). Here, obviously, the parity bits of the encrypted key cannot be set prior to key's decryption. Next, this permuted plaintext is subjected to a complex key-dependent computation using two functions called cipher function and key schedule function respectively. The key-dependent computation is defined in terms of a function f , called the cipher function, and a function KS , known as the key schedule. The process involves Initial Permutation (IP) as performed on the 64-bit plaintext block, partitioning of IP output, Key transformation (56-bit key is taken and partitioned in two parts 28-bit (for Rounds 1,2,9,16) or 24-bit (for all other rounds) circular left shifting is performed on each part using Compression Permutation (a 48-bit sub-key is generated in each round), Expansion Permutation (it is performed on the right 32-bit part of the plaintext to generate 48-bit output). Now, the 48-bit sub-key and 48-bit 'Right part of plaintext' are used for the defined operation, as discussed. DES Strengths: key transformation, rounds, expansion permutation, cipher function, difficulty in efficient software implementation Single DES is breakable in reasonable time, IP and IP-1 do not add to security value, has weak keys (4), semi-weak key-pairs (6) and possibly weak keys (48) .

The International Data Encryption Algorithm (IDEA) operates on 64-bit blocks of plaintext, uses a 128-bit key for encryption, mixes operations from different algebraic groups for added security value (XOR, Addition Modulo 2^6 , Multiplication Modulo $2^{16} + 1$), operations are performed on 16-bit sub-blocks and does not involve any bit-level manipulation (unlike the

DES). Take a 64-bit block of plaintext 'X' and divide it into 4 sub-blocks of 16-bit each: 'X1', 'X2', 'X3' and 'X4'. Here, the 128-bit Key is expanded and generate 52 sub-keys of 16-bit length. Here, each Round shall use only 6 sub-keys <4+2> of the 8 sub-keys generated using the '16-bit-chop & 25-bit-circular-left-shift' scheme.

The Advanced Encryption Standard (AES) provides for 128, 192 and 256-bit block and key sizes and allows any independent combination of these.

Current trends in cryptographic security solutions to network and internetwork security problems use a clever combination of both the symmetric and asymmetric key cryptography.

Recommended Readings

1. Bruce Schneier: Applied Cryptography, Wiley Student Edition, Second Edition, Singapore, 1996.
2. Alfred Menezes, Paul van Oorschot, and Scott Vanstone: Handbook of Applied Cryptography. CRC Press, NY.
3. William Stallings: Cryptography and Network Security. Fourth Edition. Prentice-Hall, Englewood Cliffs, 2006.
4. C.Kauffman, R.Pearlman and M.Spenser: Network Security, Second Edition, Prentice Hall, Englewood Cliffs, 2002.
5. S.Bellovin and W.Chesvick: Internet Security and Firewalls, Second Edition, Addison-Wesley, Reading, 1998.
6. Rahul Banerjee: Internetworking Technologies, Prentice-Hall of India, New Delhi, 2003.

Self-Test Questions

1. What is the primary motivation behind the study of Network Security?
2. Compare the DES, IDEA and AES in terms of their complexity vis-à-vis their cryptographic strengths.
3. Define the following terms and briefly compare both members of a pair of terms in terms of possible classes of their applications, if any:
 - Provably Secure and Computationally Secure Cryptographic Algorithms
 - Stream Ciphers and Block Ciphers
 - Symmetric-key-cryptography and Asymmetric-key-cryptography
 - Key-exchange and Key-management
 - Authentication and Authorization
4. Prove that IP and IP^{-1} operations do not add to the security of the plain DES algorithm.
5. What are the situations in which Stream Ciphers are used and which situations warrant use of Block Ciphers and why?
6. What is the reason that many real-life applications (Internet-based) use a combination of public-key as well as symmetric-key cryptographic schemes even though the former does not suffer from the problems of the latter?

Exercises

1. Analyze the security requirements of your organization and identify the variety of security mechanisms currently in place in your organization's network / intranet. Do you find some interesting patterns and practices? Discuss.

2. Visit the NIST website at www.nist.gov and identify the major FIPS recommendations relevant to the cryptographic algorithms you have briefly learnt so far.

Appendix: A

Mathematical Concepts of Relevance

Groups

'Symmetry' is key to formation of any group. Group theory provides a set of tools that allow construction of algebraic abstractions of familiar phenomena. Several applications may exist of this theory including Error-Correcting Codes. Group Theory, in its current form, evolved out of the algebraicisation of the notion of 'Symmetry'. A 'Group' may be seen as a set of elements (e.g. set of numbers). A group is cyclic if every element is a power of some fixed element.

Rings

Notionally, a 'Ring' is an algebraic structure designed to axiomatise a non-empty set with inter-related 'addition' and 'multiplication' operations:

$$+ : R \times R \rightarrow R$$

$$(-) : R \times R \rightarrow R$$

A 'Ring', is thus, a set of 'numbers' with these two operations those form an 'abelian group' with addition operation. A ring is a set in which we can do +, - (since, $[a - b = a + (-b)]$), and * without leaving the set. AES uses two rings including the polynomial interpretation of $GF(2^8)$, with coefficients over $GF(2)$ and irreducible polynomial $x^8 + x^4 + x^3 + x + 1$, and the ring of polynomials mod x^4+1 over $GF(2^8)$.

Fields

It may be defined as a set of numbers with two operations, namely, 'abelian group' for addition (+) and abelian group for multiplication (*) excluding zero). In case of 'Field', we can compute with +, -, *, and / without leaving the set.

Galois Field: Cryptographic mechanisms of many kinds involve a sub type of 'Field' called 'Finite Field'. Number of elements in a 'finite field'. must be a power of a prime pn. Galois Field is such a finite field. It is denoted as $GF(pn)$. $GF(p)$ represents a set of integers $\{0,1,.., p-1\}$ with arithmetic operations modulo prime p. In cryptography, popular types of GFs are $GF(p)$ and $GF(2n)$.

Modulo Arithmetic

Modulo operator is defined as $a \text{ mod } n = \text{remainder}$ and Congruence: $a = b \pmod{n} \Rightarrow n \mid (a-b)$. Greatest Common Divisor is defined as: $GCD(a,b) = \text{the largest number that divides evenly into both } a \text{ and } b$ If we do not want any common factor (barring 1) and we use numbers which are relatively prime.

$$\text{Example: } GCD(7,13) = 1$$

A relevant theorem is: $GCD(a,b) = GCD(b, a \text{ mod } b)$. Euclid' GCD Algorithm for finding GCD (a,b) is given below:

$$A=a, B=b$$

$$\text{while } B > 0$$

$$R = A \text{ mod } B$$

$$A = B, B = R$$

$$\text{return } A$$

Modulo Arithmetic

Any polynomial may be expressed as: $f(x) = q(x)g(x) + r(x)$ where, $r(x) \Rightarrow$ remainder and $r(x) = f(x) \text{ mod } g(x)$. If $r(x) = 0$ and if $g(x)$ has no divisor other than itself & 1, it is said to be an irreducible polynomial (prime polynomial). Polynomial GCD can be determined by extending the Euclid's GCD Algorithm.

Joint & Conditional Probability

If P, C and K denote random variables representing plaintext, ciphertext and key with probability distributions $PP(P)$, $PC(C)$ and $PK(K)$ respectively.

Conditional Probability: $Pr(P=P_0/C=C_0)$ provides the probability that the plaintext P_0 is sent when the ciphertext C_0 is received.

Joint Probability: $Pr(P=P_0, C=C_0)$ provides the probability that the plaintext is P_0 and the ciphertext is: C_0 . $Pr(P=P_0, K=K_0) = Pr(P=P_0/K=K_0) Pr(P=K_0)$.

Two random variables P and K are said to be independent if $Pr(P, K) = Pr(P) Pr(K)$.

Impact of Information Theory

A cryptographic system is said to have perfect secrecy if $Pr(P=P_0 / C=C_0) = Pr(P=P_0)$ for all plaintext P_0 and all ciphertext C_0 .

Appendix: B

Relevant On-line Resources at the Author's Website

Rahul Banerjee: **Lecture Notes on Network Security**, Electronic Read-only edition, URL: <http://discovery.bits-pilani.ac.in/rahul/NetSec/> Lecture slides shall be also made available from time to time at this course page.

It shall be the responsibility of the individual student to be regular in maintaining the self study schedule as given in the course handout, attend the online/on demand lectures as per details that would be put up in the BITS DLP website <http://www.bits-pilani.ac.in/dlp-home/> or <http://202.54.26.115/bits/Portal/dlpd/> and take the prescribed components of the evaluation such as mid semester test, comprehensive examination as per scheduled dates in the course handout. If the student is unable to appear for the regular test/examination due to genuine exigencies, the student must refer to the procedure for applying for make-up test/examination, which will be available through the **Important Information** link on the [BITS DLP website](#).