Geethanjali College of Engineering and Technology

DEPARTMENT OF ELECTRONICS & COMMUNICATIONS

(Name of the Subject/Lab Course) : NETWORK SECURITY

(JNTU CODE: 56024) **Programme : UG**

Branch: ECE **Version No : 4**

Year: IV **Document Number : GCET/ECE/**

Semester: II **No. of Pages :**

Classification status (Unrestricted/Restricted) : Unrestricted

Distribution List:

Prepared by :	**prepared by :**
1) Name : S.SRIJA	**1) Name :**
2) Sign :	**2) Sign :**
3) Design : Assistant Professor	**3) Design :**
4) Date :	**4) Date :**

Verified by :*For Q.C only

1) Name :	**1)Name :**
2) Sign :	**2) Sign :**
3) Design :	**3) Design :**
4) Date :	**4) Date :**

Approved by (HOD) :

1) Name :

2) Sign :

3) Date :

2.SYLLABUS

UNIT - I

Security Attacks (Interruption, Interception, Modification and Fabrication), Security Services (Confidentiality, Authentication, Integrity, Non-repudiation, access Control and Availability) and Mechanisms, A model for Internetwork security, Internet Standards and RFCs, Buffer overflow & format string vulnerabilities, TCP session hijacking, ARP attacks, route table modification, UDP hijacking, and man-in-the-middle attacks.

UNIT - II

Conventional Encryption Principles, Conventional encryption algorithms, cipher block modes of operation, location of encryption devices, key distribution Approaches of Message Authentication, Secure Hash Functions and HMAC.

UNIT - III

Public key cryptography principles, public key cryptography algorithms, digital signatures, digital Certificates, Certificate Authority and key management Kerberos, X.509 Directory Authentication Service.

UNIT - IV

Email privacy: Pretty Good Privacy (PGP) and S/MIME.

UNIT - V

IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management.

UNIT - VI

Web Security Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET).

UNIT - VII

Basic concepts of SNMP, SNMPv1 Community facility and SNMPv3.

Intruders, Viruses and related threats.

UNIT - VIII

Firewall Design principles, Trusted Systems. Intrusion Detection Systems.

TEXT BOOKS :

1. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education.
2. Hack Proofing your network by Ryan Russell, Dan Kaminsky, Rain Forest Puppy, Joe Grand, David Ahmad, Hal Flynn Ido Dubrawsky, Steve W.Manzuik and Ryan Permeh, wiley Dreamtech

REFERENCES :

1. Fundamentals of Network Security by Eric Maiwald (Dreamtech press)
2. Network Security - Private Communication in a Public World by Charlie Kaufman, Radia Perlman and Mike Speciner, Pearson/PHI.
3. Cryptography and network Security, Third edition, Stallings, PHI/Pearson
4. Principles of Information Security, Whitman, Thomson.
5. Network Security: The complete reference, Robert Bragg, Mark Rhodes, TMH
6. Introduction to Cryptography, Buchmann, Springer.

3. Vision of the Department

To impart quality technical education in Electronics and Communication Engineering emphasizing analysis, design/synthesis and evaluation of hardware/embedded software using various Electronic Design Automation (EDA) tools with accent on creativity, innovation and research thereby producing competent engineers who can meet global challenges with societal commitment.

4. Mission of the Department

i. To impart quality education in fundamentals of basic sciences, mathematics, electronics and communication engineering through innovative teaching-learning processes.
ii. To facilitate Graduates define, design, and solve engineering problems in the field of Electronics and Communication Engineering using various Electronic Design Automation (EDA) tools.
iii. To encourage research culture among faculty and students thereby facilitating them to be creative and innovative through constant interaction with R & D organizations and Industry.
iv. To inculcate teamwork, imbibe leadership qualities, professional ethics and social responsibilities in students and faculty.

5.Program Educational Objectives and Program outcomes of B. Tech (ECE) Program

Program Educational Objectives of B. Tech (ECE) Program :

I. To prepare students with excellent comprehension of basic sciences, mathematics and engineering subjects facilitating them to gain employment or pursue postgraduate studies with an appreciation for lifelong learning.
II. To train students with problem solving capabilities such as analysis and design with adequate practical skills wherein they demonstrate creativity and innovation that would enable them to develop state of the art equipment and technologies of multidisciplinary nature for societal development.

III. To inculcate positive attitude, professional ethics, effective communication and interpersonal skills which would facilitate them to succeed in the chosen profession exhibiting creativity and innovation through research and development both as team member and as well as leader.

Program Outcomes of B.Tech ECE Program:

1. An ability to apply knowledge of Mathematics, Science, and Engineering to solve complex engineering problems of Electronics and Communication Engineering systems.
2. An ability to model, simulate and design Electronics and Communication Engineering systems, conduct experiments, as well as analyze and interpret data and prepare a report with conclusions.
3. An ability to design an Electronics and Communication Engineering system, component, or process to meet desired needs within the realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability and sustainability.
4. An ability to function on multidisciplinary teams involving interpersonal skills.
5. An ability to identify, formulate and solve engineering problems of multidisciplinary nature.
6. An understanding of professional and ethical responsibilities involved in the practice of Electronics and Communication Engineering profession.
7. An ability to communicate effectively with a range of audience on complex engineering problems of multidisciplinary nature both in oral and written form.
8. The broad education necessary to understand the impact of engineering solutions in a global, economic, environmental and societal context.
9. A recognition of the need for, and an ability to engage in life-long learning and acquire the capability for the same.
10. A knowledge of contemporary issues involved in the practice of Electronics and Communication Engineering profession
11. An ability to use the techniques, skills and modern engineering tools necessary for engineering practice.

12. An ability to use modern Electronic Design Automation (EDA) tools, software and electronic equipment to analyze, synthesize and evaluate Electronics and Communication Engineering systems for multidisciplinary tasks.
13. Apply engineering and project management principles to one's own work and also to manage projects of multidisciplinary nature

6. COURSE OBJECTIVES AND COURSE OUTCOMES

COURSE OBJECTIVES

1. Develop a basic understanding of cryptography, how it has evolved, and some key encryption techniques used today.
2. Develop an understanding of security policies (such as authentication, integrity and confidentiality), as well as protocols to implement such policies in the form of message exchanges.
3. Develop an understanding of latest viruses, threats, IDS and concepts of firewalls

COURSE OUTCOMES

Students will able to

1. Explain security concepts, Ethics in Network Security.
2. Identify and classify various of attacks and explain the same.
3. Compare and contrast symmetric and asymmetric encryption systems and their vulnerability to various attacks.
4. Explain the role of third-party agents in the provision of authentication services.
5. Comprehend and apply authentication, email security, web security services and mechanisms.
6. Distinguish and explain different protocol like SSL, TLS Vis-à-vis their applications.
7. Discuss the effectiveness of passwords in access control.
8. Comprehend and explain security services and mechanisms

7. Brief Notes On The Importance Of The Course And How It Fits Into The Curriculum

- students need to have a decent understanding of the basics of TCP/IP. You should know the difference between IP, ICMP, TCP, and UDP. You should know what port numbers and sequence numbers are, and have (some) understanding of the TCP flags.

- students should also be comfortable with sockets programming — some of the homework assignments will require you to implement network clients or servers.

8. Prerequisites :

.

- Students should have little basics of networks,
- students should know where security is necessary

9.**INSTRUCTIONAL LEARNING OUTCOMES**

Unit-1

1. Define information security and outline its major components.
2. Identify the major types of threats to information security and the associated attacks
3. Develop strategies to protect organization information assets from common attacks.
4. Understand how security policies, standards and practices are developed.

Unit-2

5. Describe the major types of cryptographic algorithms and typical applications
6. Write code to encrypt and decrypt information using some of the standard algorithms
7. Develop implementations for some of the common cryptographic algorithms

Unit-3

8. Explain the implementation and implications of authentication protocols and.
9. Demonstrates how digital signatures are performed and the role of digital certificates
10. Understand the role of cryptography in information security
11. Importance of X.509 Certificate and role of certificate authority.

Unit-4

12. Describe the significance of Email security and implementation of PGP
13. Learns about SMIME, Encoding techniques.

Unit-5

14. Understand the architecture of IP Security.
15. Will be able to differentiate Authentication Header and Encapsulating Security payload
16. Summarize the use of different key management protocols.

Unit-6

17. Significance of SSL protocol and describe the record format.
18. Understands the Transport layer protocol functionalities.
19. Analyze the implementation and security measures taken in Secure Electronic transaction.

Unit-7

20. Understands the basic concepts of SNMP
21. Identify and evaluate threats to network security and data loss.
22. Discuss the effectiveness of passwords in access control and the influence of human behavior.

Unit-8

23. Identify types of firewall implementation suitable for differing security requirements.
24. Apply and explain simple filtering rules based on IP and TCP header information.
25. Distinguish between firewalls based on packet-filtering routers, application level gateways and circuit level gateways.

10.MAPPING OF COURSE OUTCOMES TO PROGRAM OUTCOMES

S.No	Course Outcome	POs
1	Explain security concepts, Ethics in Network Security.	PO1, PO 3, PO 6, PO 7, PO 9, PO 11, PO 12
2	Identify and classify various kinds of attacks and explain the same.	PO1, PO 3, PO 6, PO 7, PO 9, PO 11, PO 12
3	Compare and contrast symmetric and asymmetric encryption systems and their vulnerability to various attacks.	PO1, PO 3, PO 6, PO 7, PO 9, PO 11, PO 12
4	Explain the role of third-party agents in the provision of authentication services.	PO1, PO 3, PO 6, PO 7, PO 9, PO 11, PO 12
5	Comprehend and apply authentication, email security, web security services and mechanisms.	PO1, PO 2, PO 3, PO 4, PO 5,PO 7, PO 8,PO 10, PO 11, PO 12, PO 13,
6	Distinguish and explain different protocol like SSL, TLS Vis-à-vis their applications.	PO1, PO 3, PO 6, PO 7, PO 9, PO 11, PO 12
7	Discuss the effectiveness of passwords in access control.	PO1, PO 3, PO 6, PO 7, PO 9, PO 11, PO 12
8	Comprehend and explain security services and mechanisms	PO1, PO 3, PO 6, PO 7, PO 9, PO 11, PO 12

11.CLASS TIME TABLE

12.INDIVIDUAL TIME TABLE

13.MICROPLAN WITH METHODOLOGY BEING USED/ ADOPTED

S. No	Period No	Unit No	Date	Topic to be covered in One lecture	Reg/Additional	Teaching aids used LCD/OHP/ BB	Remarks
1.		1		**UNIT-1**			
2.	1			Introduction	Regular	BB	
3.	2			Security Attacks, Services	Regular	OHP,BB	
4.	3			Mechanisms, Model(N/w security)	Regular	OHP,BB	
5.	4			Internet Standard, RFC	Regular	BB, OHP	
6.	5			Tcp Sessions hijacking,UDP	Regular	BB, INTERNET	
7.	6			ARP attack, Man in the middle	Regular	BB, OHP	
8.							
9.		2		**UNIT-2:**			
10	7			Conventional encryption Principles	Regular	BB	
11	8			Conventional encryption algorithm	Regular	BB	
12	9			Cipher block modes of operation	Regular	OHP,BB	
13	10			Location of encryption devices	Regular	BB,E-tutorial	
14	11			Message Authentication	Regular	BB, OHP	
15	12			Festal structure	Regular	BB, OHP	
16	13			Classical encryption technology	Regular	BB, OHP	
17	14			Secure hash functions, MAC	Regular	OHP,BB	
18	15			Whirlpool Hash Function	Additional	LCD, INTERNET	
19							
20		3		**UNIT-3:**			
21	16			Cryptography principles	Regular	OHP,BB	
22	17			Cryptography algorithm	Regular	BB, OHP, INTERNET	
23	18			Digital signature, certificates	Regular	BB, OHP	
24	19			Certificate Authority	Regular	BB, OHP	
25	20			Kerberos		OHP,BB	
26	21			Key Management Kerberos	Regular	OHP,BB	
27	22			Kerberos versions 5	Regular	BB	
28	23			X.509 Authentication Services	Regular	OHP,BB	

29							
30	24	4		**UNIT-4:**			
31	25			Email privacy	Regular	BB, OHP	
32	26			Pretty Good privacy	Regular	OHP,BB	
33	27			PGP Trusted key rings	Regular	OHP,BB	
34	28			SIMIME	Regular	BB	
35	29			SMIME Encoding	Regular	BB,E-tutorial	
36	30			Revision	Regular	LCD,Q&A, Group Task	
37	31			Assignment discussion for 1st Mid exam	Regular	BB, Group Task	
38							
39		5		**UNIT-5:**			
40	32			IP Security Overview	Regular	BB, OHP	
41	33			Architecture	Regular	BB	
42	34			Authentication Header	Regular	OHP,BB	
43	35			Encapsulating Security payload	Regular	BB, E-tutorial	
44	36			Key Management	Regular	BB, INTERNET	
45	37			Oakley	Regular	BB	
46	38			ISKAMP	Regular	BB,	
47							
48		6		**UNIT-6:**			
49	39			Web Security Requirements	Regular	BB	
50	40			Secure Socket Layer	Regular	BB	
51	41			SSL and TLS difference	Regular	BB	
52	42			Transport Layer Security	Regular	BB,E-tutorial	
53	43			Secure electronic transaction requirements	Regular	OHP,BB	
54	44			SET	Regular	OHP,BB	
55	45			Introduction to Computer Forensics	Additional	BB, INTERNET	
56							
57		7		**UNIT-7:**			
58	46			Basic Concepts of SNMP	Regular	BB	
59	47			SNMP V1 community facility	Regular	BB	
60	48			SNMP V3	Regular	OHP,BB	
61	49			Intruders	Regular	OHP,BB	
62	50			Viruses	Regular	BB, INTERNET	
63	51			Threats	Regular	OHP,BB	
64							
65	52	8		**UNIT-8:**			
66	53			Firewall Design principles	Regular	BB, OHP	
67	54			Types of Firewall	Regular	BB, OHP	
68	55			Trusted systems	Regular	BB, OHP	
69	56			Intrusion Detection Systems	Regular	BB, OHP,	

						INTERNET	
70	57			IDS	Regular	BB, OHP	
71	58			Revision	Regular	BB, Q&A, Group Task	
72	59			Assignment discussion for 1st Mid exam	Regular	Group Task	
73	60			JNTU Previous question paper discussion	Regular	BB, OHP	

14.DETAILED NOTES

UNIT –I

Objective:

This unit gives the. information regarding different types of attacks that are faced in networks, personel computer and over internet With the information regarding the services and mechanisms to overcome the security attacks. It also give the overview about the different internet standards and supporting organizations to approve a RFC

Information security is securing the enterprise's information

Earlier : No computers

- Using physical files which are locked for safe keeping
- Personnel screening to hire people with integrity.

Now : Information is in computer files

- We need automated tools for protecting these files
- When information is distributed we need network security measures to protect information during transmission

Information security over the network OR Network security will be discussed wrt

a) The **Security Attack:** Any action that compromises the security of information and hence creates need for Information security.

b) **Security Mechanism:** A mechanism that is designed to detect, prevent, or recover from a security attack.

c) **Security Service:** A service that enhances the security of data processing systems and information transfers. A security service makes use of one or more security mechanisms.

Security Attacks :

- **Interruption:** This is an attack on ***availability***

  Ex : Destruction of a hard disk Cutting of a communication line

- **Interception:** This is an attack on ***confidentiality***

  Ex : Unauthorised person/program gains access to information

- **Modification:** This is an attack on ***integrity***

  Ex : Unauthorised party changes values in files

- **Fabrication:** This is an attack on ***authenticity***

  Ex : Insertion of spurious messages in n/w OR addition of wrong records to a file

Categorisation of attacks :

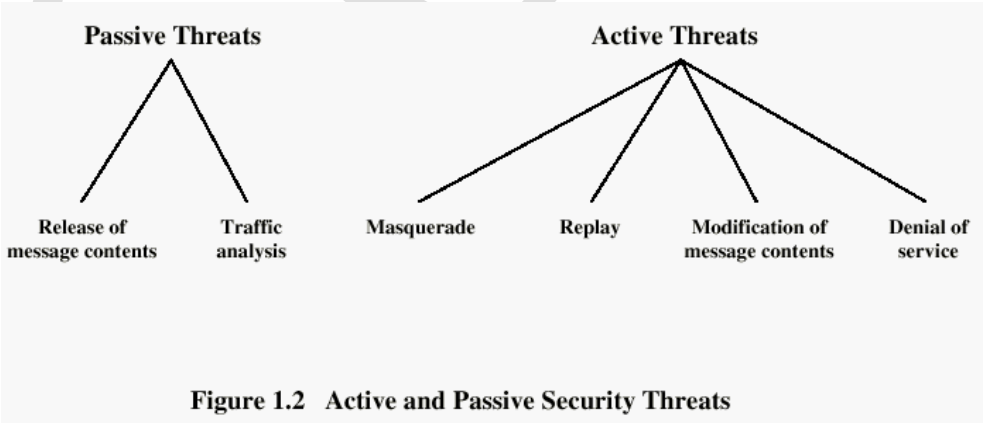


Figure 1.2 Active and Passive Security Threats

a) **Release of message contents :** Content of a message such as e_mail is directly stolen by unauthorized parties.

b) **Traffic analysis :** The msg is masked say using encryption.But the unauthorized party is able to guess the type of communication by observing pattern of communication ie the frequency & length of msgs being sent.

Emphasis is on prevention rather than detection.

c) Masquerade : Impersonating say a biometric.

d) Replay : Capture of data say password & subsequent reuse .

e) Modification of msg : Altering original msg

f) Denial of service : Preventing/inhibiting normal use of communication services

Ex: overloading the n/w with useless msgs so as to degrade n/w performance so that actual msg does not reach its intended destination OR reaches late.

Emphasis is on detection rather than prevention.

Security Services : Should ideally **ensure**

- ***Confidentiality*** : Transmitted data should be known only to *Sender & Reciever*.n/w & service should make sure that traffic analysis is made difficult.
- ***Authentication :*** the recipient that the msg is from the source that it claims to be from.
- ***Integrity :*** data is not altered.
- ***Non-repudiation :*** Sender/receiver cannot deny having sent/received msg.
- ***Access control :***The access to host systems & applications on the communications network is controlled to prevent misuse of resources.
- ***Availability*** : of elements of the communications n/w .

Be able to overcome Denial of Service Attacks Prevent Virus attacks that deletes files.

Internet standards and RFCs :

- Are the n/w security protocols & applications which come into being as the stds OR Request for comments.
- The Internet society is an organization which is responsible for the development & publication of these stds.
- It is further subdivided into

- **Internet Architecture Board (IAB) :** i)Responsible for defining the overall architecture of the internet .

  ii)Providing guidance to IETF.

- **Internet Engg Task Force (IETF)** :Takes care of defining & developing internet protocols thr working groups with voluantary membership.

- **Internet Engg Steering Group (IESG)**:

  i)Management of IETF activities.

  ii)Managing internet standards process

TCP session hijacking

"**TCP session hijacking**" is a technique that involves intercepting a TCP session initiated between two machines in order to hijack it.

In that the authentication check is performed only when opening the session, a pirate who successfully launches this attack is able to take control of the connection throughout the duration of the session

Buffer overflow vulnerabilities are among the most widespread of security problems.

Numerous incidents of buffer overflow attacks have been reported and many solutions have been proposed, but a solution that is both complete and highly practical is yet to no less dangerous.

Vulnerability to buffer overflow and format string overflow is due to the characteristics of the C language. For example, an array in C is not a first-class object and is represented as a pointer. Hence, it is difficult for a compiler to check on whether an operation will overflow an array. C allows variadic functions such as string format functions. Since the number of be found. Another kind of vulnerability called format string overflow has recently been found, and though not as popular as buffer overflow, format string overflow attacks are

arguments is not known at compile time, a string format function has to rely on the format string to figure it out at run time. Such characteristics are geared toward convenience and performance, and are therefore favored for numerous legacy applications. Such vulnerabilities

can be eliminated by programmers through careful programming and by rigorous checking of array bounds and the like

FORMAT STRING OVERFLOW VULNERABILITY

String format functions in the C library take variable number of arguments, one of which is the format string that is always required. The format string can contain two types of data: printable characters and format-directive characters. To access the rest of the parameters that the calling function pushed on the stack, the string format function parses the format string and interprets the format directives as they are read. For example, printf in Figure 28 parses the format string “format %s%d” and retrieves two parameters from the stack, a string pointer and an integer, in addition to printing the string “format ”. The number and types of the parameters pushed on the stack must match the directives in the format string. If the number of directives is less than the number of parameters, then the string format function will

“underflow” the stack (its activation record). If the number of directives exceed the number of

parameters, then it will “overflow” the stack. If a wrong directive is given for the corresponding

parameter, the string format function will misinterpret the parameter. Therefore, if users can control the format string, then they can exploit the behavior of string format functions and alter the memory space of the process; printf shown in Figure 28 is safe, since the format

string is static. However, printf in Figure 29 is vulnerable, since the format string is supplied by users.

Format string overflow attacks are similar to buffer overflow attacks, since they also can alter the memory space and execute arbitrary code, but it is a different kind of attack that exploits the vulnerability of variadic functions such as string format functions.

UNIT –II

Objective:

The objective of this unit is to give a brief introduction over symmetric encryption algorithms with three block encryption algorithms: DES, tripleDES, AES. It also gives a an introduction to one more important security function i.e. message authentication with the use of base MAC algorithm

Definitions :

Encryption : Converting a text into code or cipher.

Converting computer data and messages into something, incomprehensible use a key, so that only a holder of the matching key can reconvert them.

Conventional Or Symmetric Or Secret Key Or Single Key encryption:

Uses the same key for encryption & decryption.

Public Key encryption :

Uses different keys for encryption & decryption

II.Conventional Encryption Principles :

- An encryption scheme has five ingredients:

1. Plaintext – Original message or data.
2. Encryption algorithm – performs substitutions & transformations on plaintext.
3. Secret Key – exact substitutions & transformations depend on this
4. Ciphertext - output ie scrambled input.
5. Decryption algorithm - converts ciphertext back to plaintext.

Feistel Cipher Structure :

- Virtually all conventional block encryption algorithms, have a structure first described by Horst Feistel of IBM in 1973.
- The realization of a Fesitel structure depends on the choice of the following parameters and design features :

  1. Block size: larger block sizes mean greater security; but reduced encryption /decryption speed. Tradeoff is 64 bits.

  2. Key Size: larger key size means greater security;but reduced encryption /decryption speed. Tradeoff is 128 bits.

  3.Number of rounds: multiple rounds offer increasing security;typical size is 16 rounds.

  4.Subkey generation algorithm: greater complexity will lead to greater difficulty of cryptanalysis.

  5.Fast software encryption/decryption: the speed of execution of the algorithm becomes a concern

6. **6.Round function:** greater complexity will lead to greater difficulty of cryptanalysis

Cipher Block modes of operation :

- Symmetric block cipher processes one block of data at a time.
- Usual block size is 64 bits.
- Last block is padded if necessary.

1. **Electronic code book mode :**
   - Each blk of PT is encrypted using the same Key.
   - If the same 64 bit pattern repeats in PT , CT pattern is also repeated.

- **Drawback :**If the msg is highly structured ,a Cryptanalyst can exploit these patterns & crack the PT.
- Nxt two modes overcome this drawback.

2. Cipher Block Chaining Mode (CBC) :

- The input to the encryption algorithm is the XOR of the current plaintext block and the preceding ciphertext block.
- Same key is used for each block.
- First blk of CT is obtained by XORing first PT blk & an initialisation vector (IV)
- IV is known to sender & reciever and is protected like the key.

3. Cipher Feedback Mode :

- Works with DES like a stream cipher.
- Ex : if a character stream is being transmitted, each char is encrypted & transmitted .
- Desirable property is CT & PT should be of same length.ie if each char is 8 bits it should be encrypted using 8 bits.

  Note : draw fig here & equ

SHA-1:

STEP 1 :

- Msg is padded so that its length is 64 bits less than multiple of 512 bits.
- Padding consists of a single 1 bit followed by 0s.

STEP 2 :

- A blk of 64 bits is appended to the result of step1.
- This is an unsigned integer & carries the length of the original msg.

STEP 3 :

- A 160 bit buffer is used to hold intermediate & final results of hash function.
- The buffer consists of 5 , 32 bit registers A,B,C,D,E initialized with following hexadecimal values :

  A=67452301 ; B=EFCDAB89 ; C=98BADCFE ;

  D=10325476 ; E=C3D2E1F0

STEP 4 :

Processing of each 512-Bit Block , consists of applying compression function , which consists of 4 rounds of processing , each round with 20 steps.

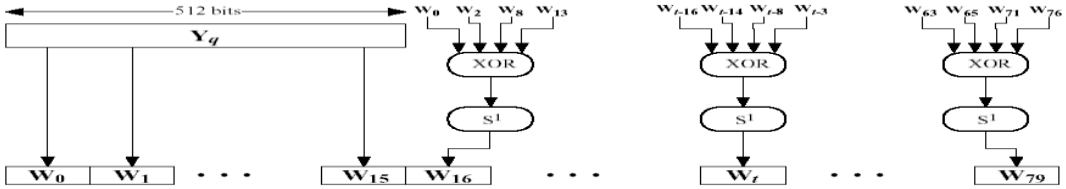


Figure 9.7 Creation of 80-word Input Sequence for SHA-1 Processing of Single Block

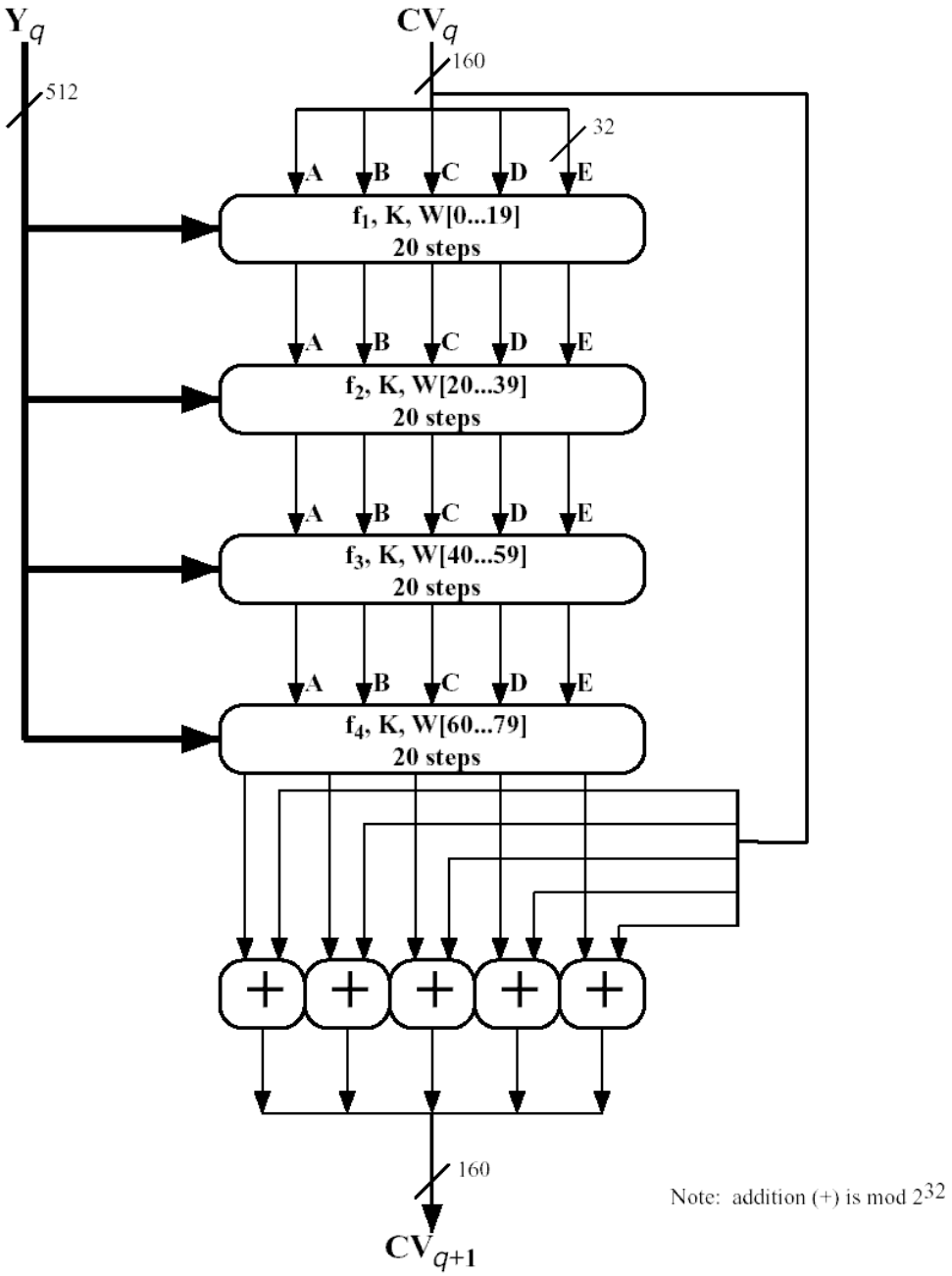


Figure 9.5 SHA-1 Processing of a Single 512-bit Block (SHA-1 Compression Function)

HMAC:

- Use a MAC derived from a cryptographic hash code, Ex SHA-1
- Cryptographic hash fns executes faster in s/w than encryption algorithms such as DES.
- Library code for cryptographic hash functions is widely available
- No export restrictions from the US

MAC=H(k ⊕ opad, H(k ⊕ ipad, data))

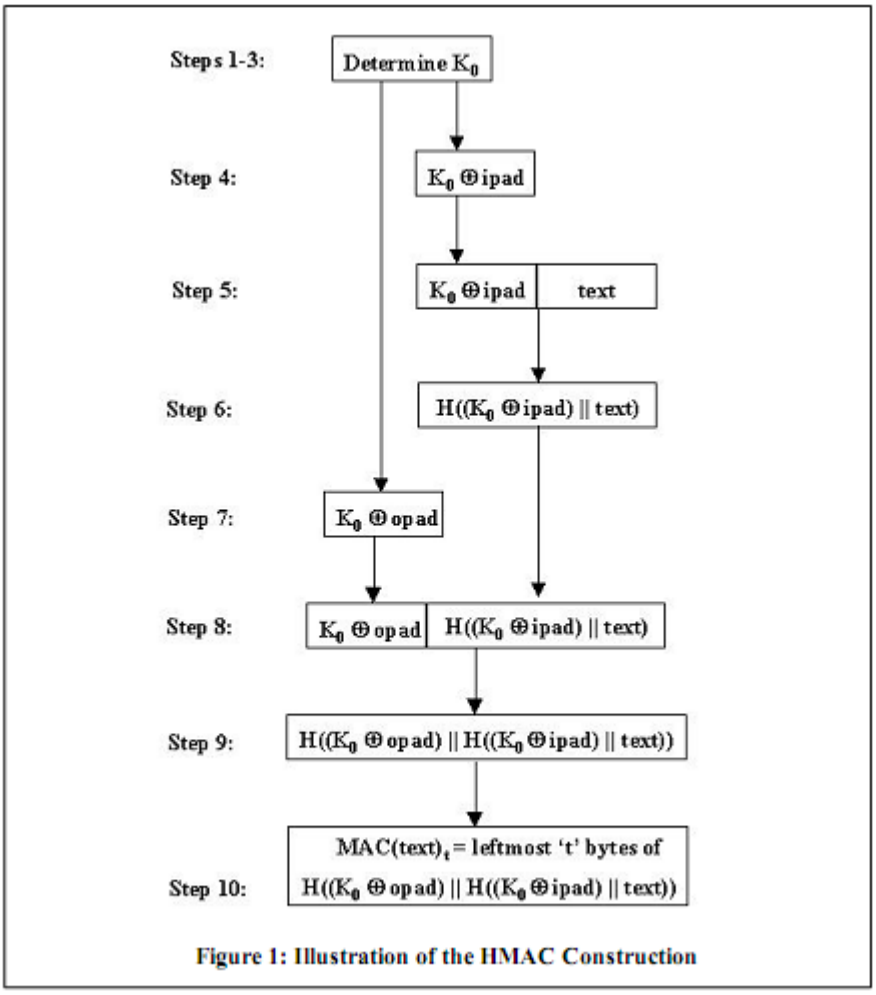


Figure 1: Illustration of the HMAC Construction

UNIT –III

Objective:

The objective of this unit is to develop encryption algorithms with asymmetric keys used in the algorithm called as public key encryption algorithms. Its describes two important public-key encryption algorithms that is RSA and Diffie-hellman

Public-Key Cryptography Principles :

- Public key encryption uses two keys & has applications in key distribution, confidentiality and authentication
- The scheme has six ingredients :
- Plaintext , Encryption algorithm , Public and private key (one used for encryption other for decryption) ,Ciphertext, Decryption algorithm .

The steps in public key encryption

- **Applications for Public-Key Cryptosystems :**
  - **Encryption/decryption:** The sender encrypts a message with the recipient's public key.
  - **Digital signature:** The sender "signs" a message with its private key.
  - **Key echange:** Two sides cooperate two exhange a session key.

Public-Key Cryptographic Algorithms :

1. **RSA** - Ron Rives, Adi Shamir and Len Adleman at MIT, 1977.
   - RSA is a block cipher & the most widely implemented.

RSA involves a **public key** and a **private key.** The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be

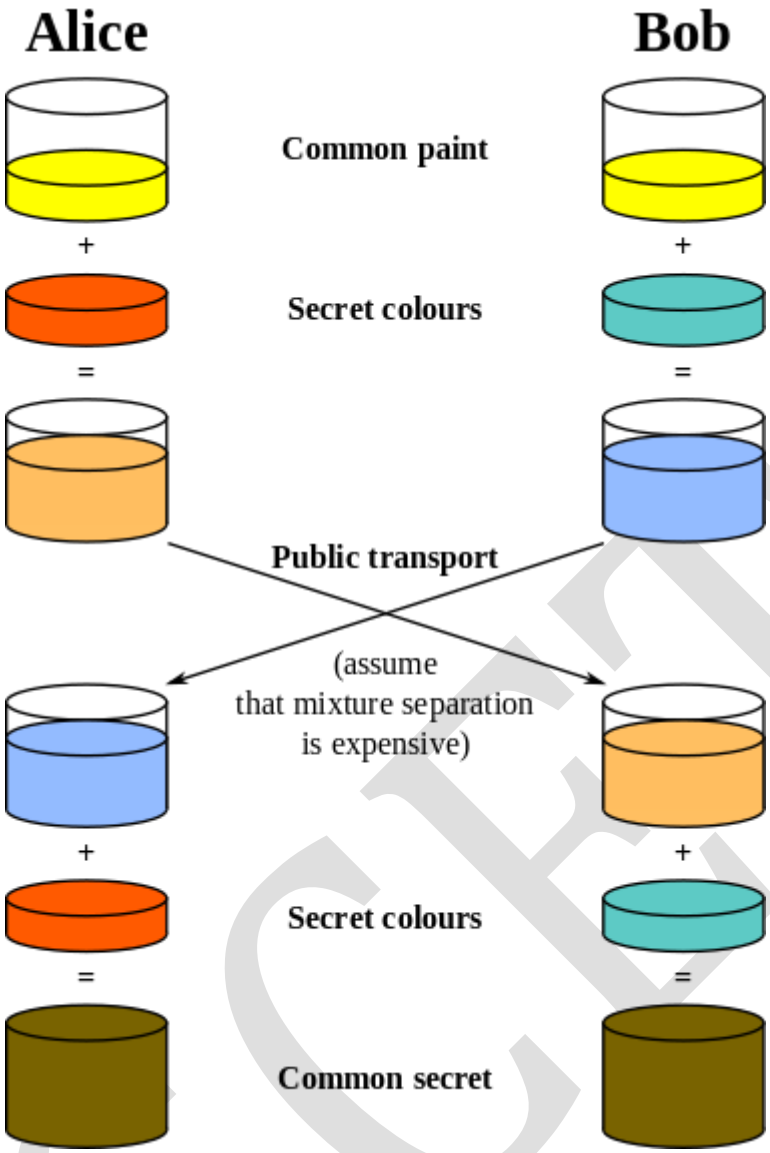
decrypted using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q.
    - For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.
2. Compute $n = pq$.
    - n is used as the modulus for both the public and private keys
3. Compute $\varphi(n) = (p-1)(q-1)$, where φ is Euler's totient function.
4. Choose an integer e such that $1 < e < \varphi(n)$ and greatest common denominator of $(e,\varphi(n)) = 1$, i.e. e and $\varphi(n)$ are coprime.
    - e is released as the public key exponent.
    - e having a short bit-length and small Hamming weight results in more efficient encryption - most commonly 0x10001 = 65537. However, small values of e (such as 3) have been shown to be less secure in some settings.[4]
5. Determine $d = e^{-1} \bmod \varphi(n)$; i.e. d is the multiplicative inverse of e mod $\varphi(n)$.
    - This is more clearly stated as solve for d given (d*e)mod $\varphi(n) = 1$
    - This is often computed using the extended Euclidean algorithm.
    - d is kept as the private key exponent.

Diffie-Hellman Key Echange :

- Used mainly for exchanging secret key securely.

Diffie–Hellman establishes a shared secret that can be used for secret communications by exchanging data over a public network. The following diagram illustrates the general idea of the key exchange:



Here is an explanation which includes the encryption's mathematics:

The simplest, and original, implementation of the protocol uses the multiplicative group of integers modulo *p*, where *p* is prime and *g* is primitive root mod *p*. Here is an example of the protocol, with non-secret values in blue, and secret values in **boldface red**:

Alice	Bob

Secret	Public	Calculates	Sends	Calculates	Public	Secret
a	p, g		p,g⟶			b
a	p, g, A	$g^a \bmod p = A$	A⟶		p, g	b
a	p, g, A		⟵B	$g^b \bmod p = B$	p, g, A, B	b
a, **s**	p, g, A, B	$B^a \bmod p = s$		$A^b \bmod p = s$	p, g, A, B	b, **s**

1. Alice and Bob agree to use a prime number p=23 and base g=5.
2. Alice chooses a secret integer $\boldsymbol{a}$=**6**, then sends Bob A = $g^a \bmod p$
   - A = $5^{6} \bmod 23$
   - A = **15,625** mod 23
   - A = 8
3. Bob chooses a secret integer $\boldsymbol{b}$=**15**, then sends Alice B = $g^b \bmod p$
   - B = $5^{15} \bmod 23$
   - B = **30,517,578,125** mod 23
   - B = 19
4. Alice computes **s** = $B^a \bmod p$
   - **s** = $19^{6} \bmod 23$
   - **s** = **47,045,881** mod 23
   - **s** = **2**
5. Bob computes **s** = $A^b \bmod p$
   - **s** = $8^{15} \bmod 23$
   - **s** = **35,184,372,088,832** mod 23
   - **s** = **2**
6. Alice and Bob now share a secret: **s** = **2**. This is because 6*15 is the same as 15*6. So somebody who had known both these private integers might also have calculated s as follows:
   - **s** = $5^{6*15} \bmod 23$
   - **s** = $5^{15*6} \bmod 23$
   - **s** = $5^{90} \bmod 23$

- **s** = **807,793,566,946,316,088,741,610,050,849,573,099,185,363,389,551,639,556,884,765,625** mod 23
- **s** = **2**

Digital Signature Standard (DSS):

- Makes use of the SHA-1
- Not for encryption or key echange

Elliptic-Curve Cryptography (ECC) :

- Good for smaller bit size
- Low confidence level, compared with RSA
- Very complex

Kerberos :

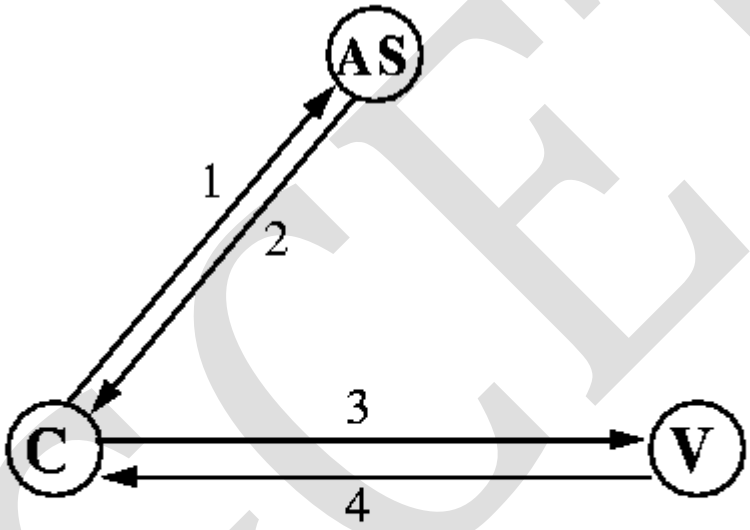
Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography. A free implementation of this protocol is available from the Massachusetts Institute of Technology

1. Suppose you want to access a server on another computer (which you may get to by sending a Telnet or similar login request). You know that this server requires a Kerberos "ticket" before it will honor your request.
2. To get your ticket, you first request authentication from the Authentication Server (AS). The Authentication Server creates a "session key" (which is also an encryption key) basing it on your password (which it can get from your user name) and a random value that represents the requested service. The session key is effectively a "ticket-granting ticket."
3. You next send your ticket-granting ticket to a ticket-granting server (TGS). The TGS may be physically the same server as the Authentication Server, but it's now performing a different service.The TGS returns the ticket that can be sent to the server for the requested service.
4. The service either rejects the ticket or accepts it and performs the service.
5. Because the ticket you received from the TGS is time-stamped, it allows you to make additional requests using the same ticket within a certain time period (typically, eight

hours) without having to be reauthenticated. Making the ticket valid for a limited time period make it less likely that someone else.

Application request and response

Messages 3 and 4 in figure 1 show the application request and response, the most basic exchange in the Kerberos protocol. It is through this exchange that a client proves to a verifier that it knows the session key embedded in a Kerberos ticket. There are two parts to the application request, a ticket (described above) and an authenticator. The authenticator includes, among other fields: the current time, a checksum, and an optional encryption key, all encrypted with the session key from the accompanying ticket.



1. as_req: c, v, $time_{exp}$, n
2. as_rep: $\{K_{c,v}$, v, $time_{exp}$, n, ...$\}K_c$, $\{T_{c,v}\}K_v$
3. ap_req: $\{ts,ck, K_{subsession}$, ...$\}K_{c,v}$ $\{T_{c,v}\}K_v$
4. ap_rep: $\{ts\}K_{c,v}$ (optional)

$T_{c,v} = K_{c,v}$, c, $time_{exp}$ ...

Figure 1: Basic Kerberos authentication protocol (simplified)

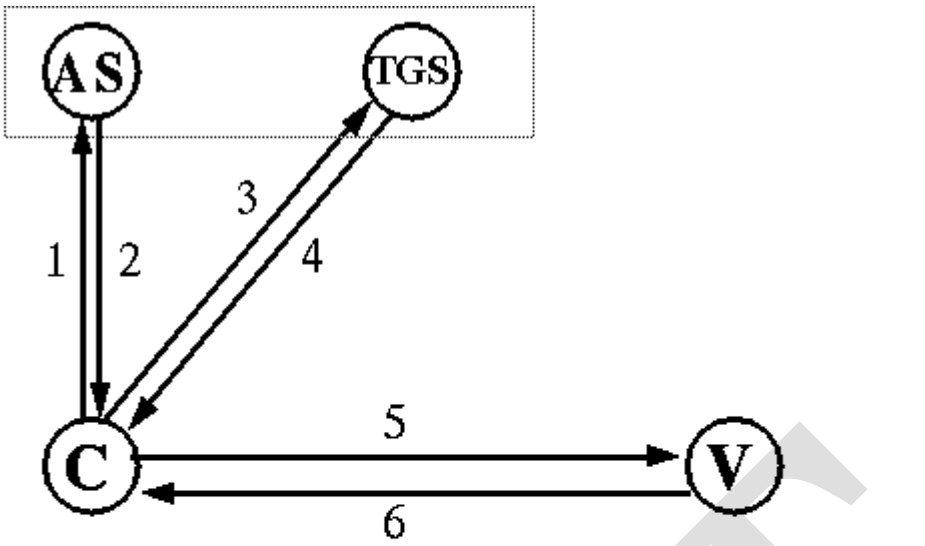
Obtaining additional tickets

The basic Kerberos authentication protocol allows a client with knowledge of the user's password to obtain a ticket and session key for and to prove its identity to any verifier registered with the authentication server. The user's password must be presented each time the user performs authentication with a new verifier. This can be cumbersome; instead, a system should support single sign-on, where the user logs in to the system once, providing the password at that time, and with subsequent authentication occurring automatically. The obvious way to support this, caching the user's password on the workstation, is dangerous. Though a Kerberos ticket and the key associated with it are valid for only a short time, the user's password can be used to obtain tickets, and to impersonate the user until the password is changed. A better approach, and that used by Kerberos, is to cache only tickets and encryption keys (collectively called credentials) that will work for a limited period.

The ticket granting exchange of the Kerberos protocol allows a user to obtain tickets and encryption keys using such short-lived credentials, without re-entry of the user's password. When the user first logs in, an authentication request is issued and a ticket and session key for the ticket granting service is returned by the authentication server. This ticket, called a *ticket granting ticket*, has a relatively short life (typically on the order of 8 hours). The response is decrypted, the ticket and session key saved, and the user's password forgotten.

Subsequently, when the user wishes to prove its identity to a new verifier, a new ticket is requested from the authentication server using the ticket granting exchange. The ticket granting exchange is identical to the authentication exchange except that the ticket granting request has embedded within it an application request, authenticating the client to the authentication server, and the ticket granting response is encrypted using the session key from the ticket granting ticket, rather than the user's password.

Figure 2 shows the complete Kerberos authentication protocol. Messages 1 and 2 are used only when the user first logs in to the system, messages 3 and 4 whenever a user authenticates to a new verifier, and message 5 is used each time the user authenticates itself. Message 6 is optional and used only when the user requires mutual-authentication by the verifier.

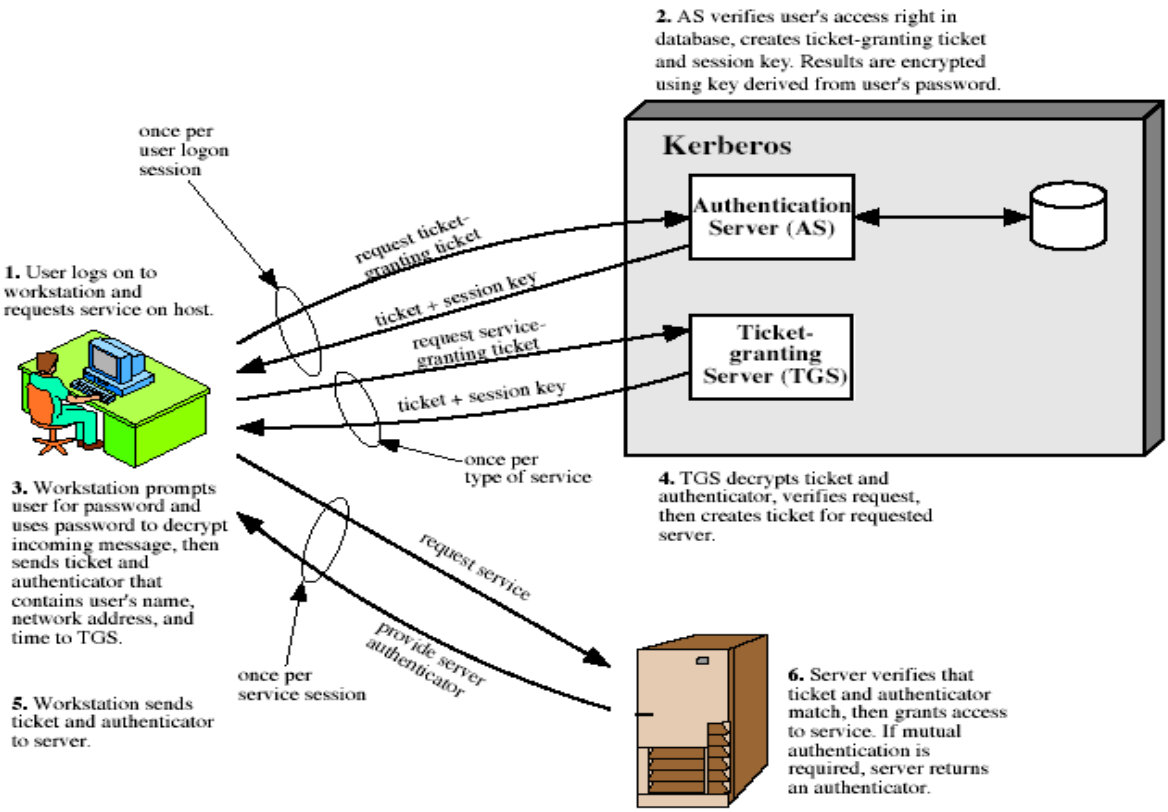


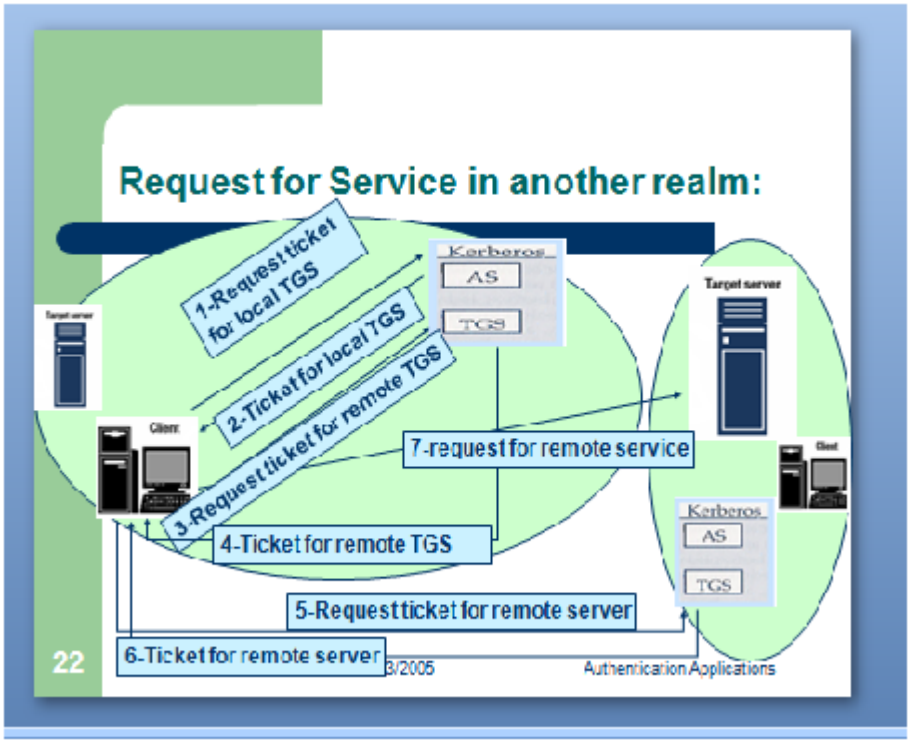
1. as_req: c, tgs, $time_{exp}$, n
2. as_rep: $\{K_{c,tgs}, tgs, time_{exp}, n, ...\}K_c$, $\{T_{c,tgs}\}K_{tgs}$
3. tgs_req: $\{ts, ...\}K_{c,tgs}$ $\{T_{c,tgs}\}K_{tgs}$, v, $time_{exp}$, n
4. tgs_rep: $\{K_{c,v}, v, time_{exp}, n, ...\}K_{c,tgs}$, $\{T_{c,v}\}K_v$
5. ap_req: $\{ts, ck, K_{subsession}, ...\}K_{c,v}$ $\{T_{c,v}\}K_v$
6. ap_rep: $\{ts\}K_{c,v}$ (optional)

Figure 2: Complete Kerberos Authentication Protocol (simplified)

Protecting application data

As described so far, Kerberos provides only authentication: assurance that the authenticated principal is an active participant in an exchange. A by-product of the Kerberos authentication protocol is the exchange of the session key between the client and the server. The session key may subsequently be used by the application to protect the integrity and privacy of communications. The Kerberos system defines two message types, the *safe message* and the *private message* to encapsulate data that must be protected, but the application is free to use a method better suited to the particular data that is transmitted.

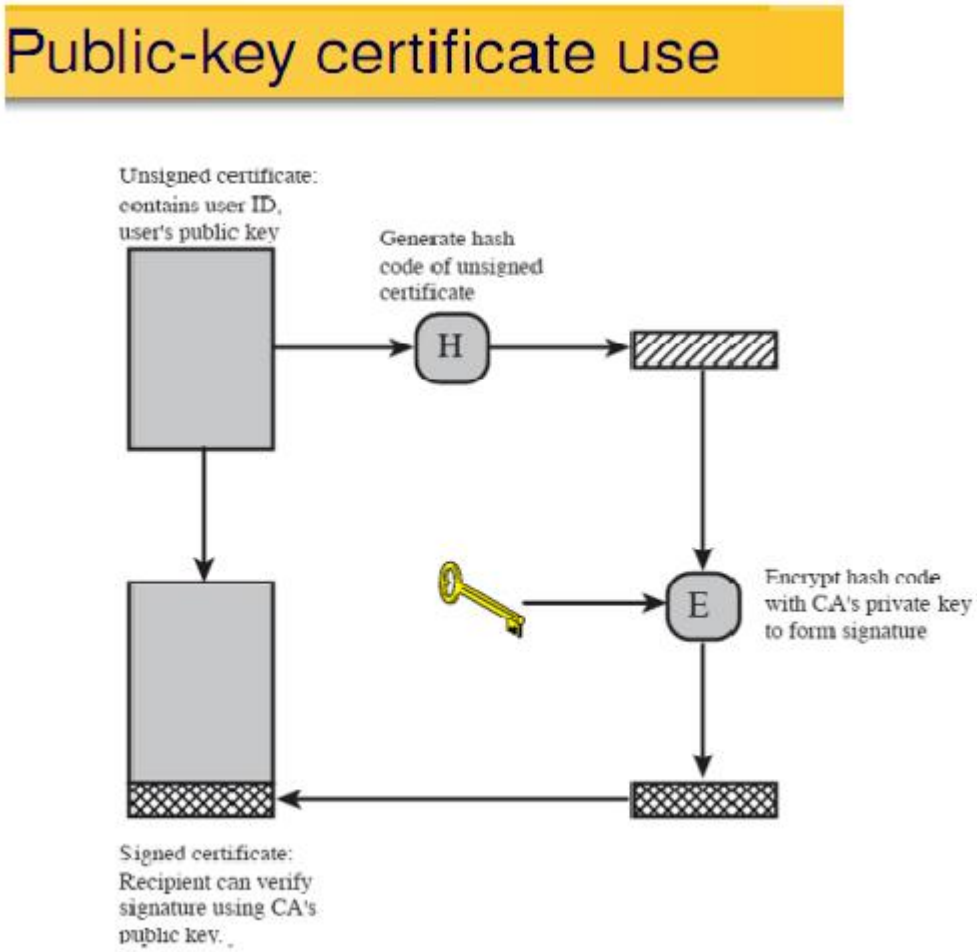

2. AS verifies user's access right in database, creates ticket-granting ticket and session key. Results are encrypted using key derived from user's password.
Kerberos
Authentication Server (AS)
Ticket-granting Server (TGS)
once per user logon session
1. User logs on to workstation and requests service on host.
request ticket-granting ticket
ticket + session key
request service-granting ticket
ticket + session key
once per type of service
4. TGS decrypts ticket and authenticator, verifies request, then creates ticket for requested server.
3. Workstation prompts user for password and uses password to decrypt incoming message, then sends ticket and authenticator that contains user's name, network address, and time to TGS.
request service
provide server authenticator
once per service session
5. Workstation sends ticket and authenticator to server.
6. Server verifies that ticket and authenticator match, then grants access to service. If mutual authentication is required, server returns an authenticator.


Request for Service in another realm:
1-Request ticket for local TGS
2-Ticket for local TGS
3-Request ticket for remote TGS
Kerberos
AS
TGS
Target server
Client
7-request for remote service
4-Ticket for remote TGS
5-Request ticket for remote server
6-Ticket for remote server
22
3/2005
Authentication Applications

Kerberos Version 5 Message Exchange:1

X.509 Authentication Service:

- Distributed set of servers that maintains a database about users.
- Each certificate contains the public key of a user and is signed with the private key of a CA.
- issued by a Certification Authority (CA), containing:
    - version (1, 2, or 3)
    - serial number (unique within CA) identifying certificate
    - signature algorithm identifier
    - issuer X.500 name (CA)
    - period of validity (from - to dates)
    - subject X.500 name (name of owner)
    - subject public-key info (algorithm, parameters, key)
    - issuer unique identifier (v2+)
    - subject unique identifier (v2+)
    - extension fields (v3)
    - signature (of hash of all fields in certificate)
- notation CA<<A>> denotes certificate for A signed by CA



X.509 Certificate format

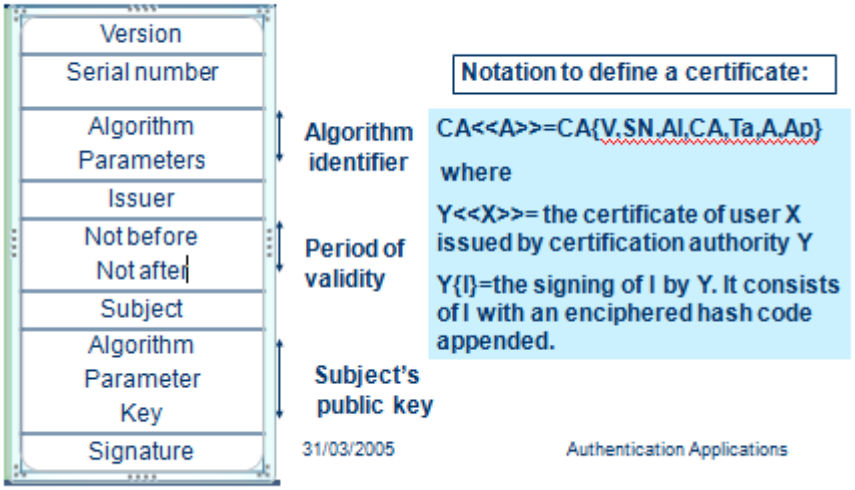
ITU-T Recommendation X.509 specifies the authentication service for X.500 directories, as well as the widely adopted X.509 certificate syntax. The initial version of X.509 was published in 1988, version 2 was published in 1993, and version 3 was proposed in 1994 and considered for approval in 1995. Version 3 addresses some of the security concerns and limited flexibility that were issues in versions 1 and 2.

Directory authentication in X.509 can be carried out using either secret-key techniques or public-key techniques; the latter is based on public-key certificates. The standard does not specify a particular cryptographic algorithm, although an informative annex of the standard describes the RSA algorithm

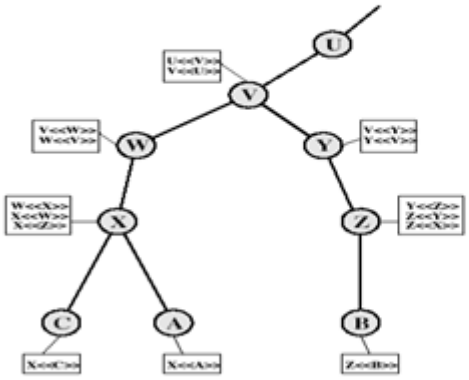
An X.509 certificate consists of the following fields:

1. version
2. serial number
3. signature algorithm ID
4. issuer name
5. validity period
6. subject (user) name
7. subject public key information
8. issuer unique identifier (version 2 and 3 only)
9. subject unique identifier (version 2 and 3 only)
10. extensions (version 3 only)
11. signature on the above fields

This certificate is signed by the issuer to authenticate the binding between the subject (user's) name and the user's public key. The major difference between versions 2 and 3 is the addition of the extensions field. This field grants more flexibility as it can convey additional information beyond just the key and name binding. Standard extensions include subject and issuer attributes, certification policy information, and key usage restrictions, among others.



X.509 CA Hierarchy



A acquires B certificate using chain:

X<<**W**>>W<<**V**>>V<<**Y**>> Y<<**Z**>> Z<<**B**>>

B acquires A certificate using chain:

Z<<**Y**>>Y<<**V**>>V<<**W**>> W<<**X**>> X<<**A**>>

Authentication Applications

UNIT –IV

Overview:

PGP and S/MIME used for providing security for different levels while sending the e-mail over the network channel. It also defines the documentations with in different RFC's

Pretty Good Privacy

- Philip R. Zimmerman is the creator of PGP.
- PGP provides a confidentiality and authentication service that can be used for electronic mail and file storage applications
- Why Is PGP Popular?
- Operational Description
- Compression
- E-mail Compatibility
- Segmentation and Reassembly
- Sumary of PGP Services
- Format of PGP Message
- Revoking Public Keys

PGP encryption uses a serial combination of hashing, data compression, symmetric-key cryptography, and, finally, public-key cryptography; each step uses one of several supported algorithms. Each public key is bound to a user name and/or an e-mail address. The first version of this system was generally known as a web of trust to contrast with the X.509 system which uses a hierarchical approach based on certificate authority and which was added to PGP implementations later. Current versions of PGP encryption include both options through an automated key management server.

Compatibility

As PGP evolves, PGP systems that support newer features and algorithms are able to create encrypted messages that older PGP systems cannot decrypt, even with a valid private key. Thus, it is essential that partners in PGP communication understand each other's capabilities or at least agree on PGP settings.

Confidentiality

PGP can be used to send messages confidentially. For this, PGP combines symmetric-key encryption and public-key encryption. The message is encrypted using a symmetric encryption algorithm, which requires a symmetric key. Each symmetric key is used only once and is also called a session key. The session key is protected by encrypting it with the receiver's public key thus ensuring that only the receiver can decrypt the session key. The encrypted message along with the encrypted session key is sent to the receiver.

Digital signatures

PGP supports message authentication and integrity checking. The latter is used to detect whether a message has been altered since it was completed (the *message integrity* property), and the former to determine whether it was actually sent by the person/entity claimed to be the sender (a *digital signature*). In PGP, these are used by default in conjunction with encryption, but can be applied to the plaintext as well. The sender uses PGP to create a digital signature for the message with either the RSA or DSA signature algorithms. To do so, PGP computes a hash (also called a message digest) from the plaintext, and then creates the digital signature from that hash using the sender's private key.

S/MIME

- Secure/Multipurpose Internet Mail Extension.
- S/MIME will probably emerge as the industry standard.

- Header fields in MIME
- S/MIME Functions

- Algorithms Used
- User Agent Role

UNIT –V

Objective :

IPSec is not a single protocol. Instead, IPSec provides a set of security algorithms plus a general framework that allows a pair of communicating entities to use whichever algorithms provide security appropriate for the communication.

- Applications of IPSec
  - Secure branch office connectivity over the Internet
  - Secure remote access over the Internet
  - Establsihing extranet and intranet connectivity with partners
  - Enhancing electronic commerce securit
- IP Security Scenario
- IP Security Overview
- IP Security Architecture
- IPSec Document Overview
- IPSec Services

Security Associations (SA)

- A one way relationsship between a sender and a receiver.
- Identified by three parameters:
  - Security Parameter Index (SPI)
  - IP Destination address

--Security Protocol Identifier

- Transport Mode (AH Authentication)
- Tunnel Mode (AH Authentication)

IPsec provides security services at the network layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services. IPsec can be used to protect one or more "paths" between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

The set of security services that IPsec can provide includes access control, connectionless integrity, data origin authentication, rejection of replayed packets (a form of partial sequence integrity), confidentiality (encryption), and limited traffic flow confidentiality. Because these services are provided at the IP layer, they can be used by any higher layer protocol, e.g., TCP, UDP, ICMP, BGP, etc.

These objectives are met through the use of two traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols. The set of IPsec protocols employed in any context, and the ways in which they are employed, will be determined by the security and system requirements of users, applications, and/or sites/organizations.

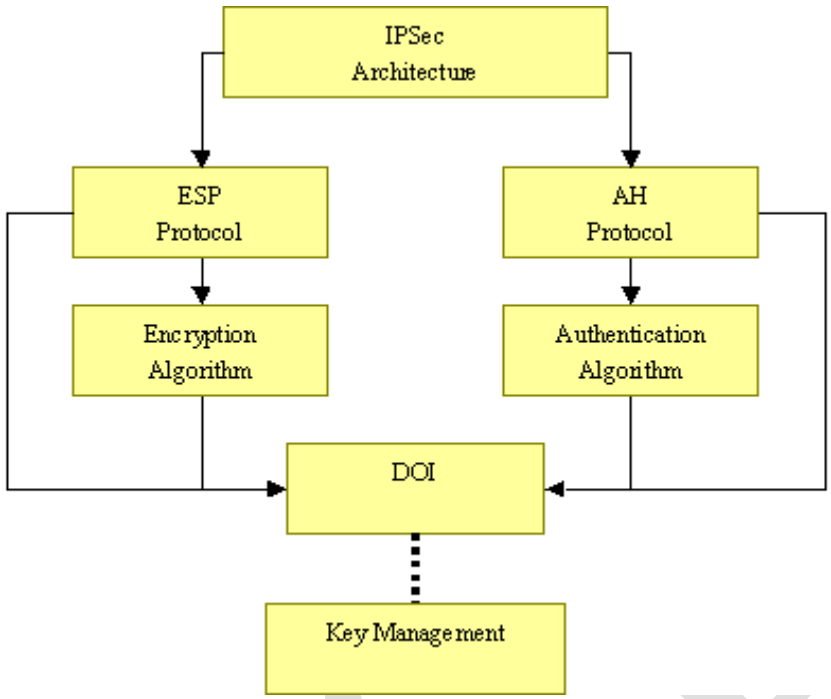
When these mechanisms are correctly implemented and deployed, they ought not to adversely affect users, hosts, and other Internet components that do not employ these security mechanisms for protection of their traffic. These mechanisms also are designed to be algorithm-independent. This modularity permits selection of different sets of algorithms without affecting the other parts of the implementation. For example, different user communities may select different sets of algorithms (creating cliques) if required.

A standard set of default algorithms is specified to facilitate interoperability in the global Internet. The use of these algorithms, in conjunction with IPsec traffic protection and key management protocols, is intended to permit system and application developers to deploy high quality, Internet layer, cryptographic security technology.

Protocol Structure - IPsec: Security Architecture for IP Network

IPsec Architecture included many protocols and algorithms. The relationship

of these protocols are displayed as follows:



Authentication Header (AH) is a member of the IPsec protocol suite. AH guarantees connectionless integrity and data origin authentication of IP packets. Further, it can optionally protect against replay attacks by using the sliding window technique and discarding old packets

- In IPv4, the AH protects the IP payload and all header fields of an IP datagram except for mutable fields (i.e. those that might be altered in transit), and also IP options such as the IP Security Option (RFC-1108). Mutable (and therefore unauthenticated) IPv4 header fields are DSCP/TOS, ECN, Flags, Fragment Offset, TTL and Header Checksum.[6]
- In IPv6, the AH protects the most of the IPv6 base header, AH itself, non-mutable extension headers after the AH, and the IP payload. Protection for the IPv6 header excludes the mutable fields: DSCP, ECN, Flow Label, and Hop Limit

AH operates directly on top of IP, using IP protocol number 51.

The following AH packet diagram shows how an AH packet is constructed and interpreted

he primary difference between the authentication provided by ESP and AH is the extent of the coverage. Specifically, ESP does not protect any IP header fields unless those fields are encapsulated by ESP. For more details on how to use AH and ESP in various network environments.

When used with IPv6, the Authentication Header normally appears after the IPv6 Hop-by-Hop Header and before the IPv6 Destination Options. When used with IPv4, the Authentication Header normally follows the main IPv4 header.

Protocol Structure - IPsec AH: IP Authentication Header

8	**16**	**32bit**
Next Header	Payload Length	Reserved
Security parameters index (SPI)		
Sequence Number Field		
Authentication data (variable)		

Next Header (8 bits)

Type of the next header, indicating what upper-layer protocol was protected. The value is taken from the list of IP protocol numbers.

Payload Len (8 bits)

The length of this *Authentication Header* in 4-octet units, minus 2 (a value of 0 means 8 octets, 1 means 12 octets, etcetera). Although the size is measured in 4-octet units, the length of this header needs to be a multiple of 8 octets if carried in an IPv6 packet. This restriction does not apply to an *Authentication Header* carried in an IPv4 packet.

Reserved (16 bits)

Reserved for future use (all zeroes until then).

Security Parameters Index (32 bits)

Arbitrary value which is used (together with the destination IP address) to identify the security association of the receiving party.

Sequence Number (32 bits)

A monotonic strictly increasing sequence number (incremented by 1 for every packet sent) to prevent replay attacks. When replay detection is enabled, sequence numbers are never reused because a new security association must be renegotiated before an attempt to increment the sequence number beyond its maximum value.[6]

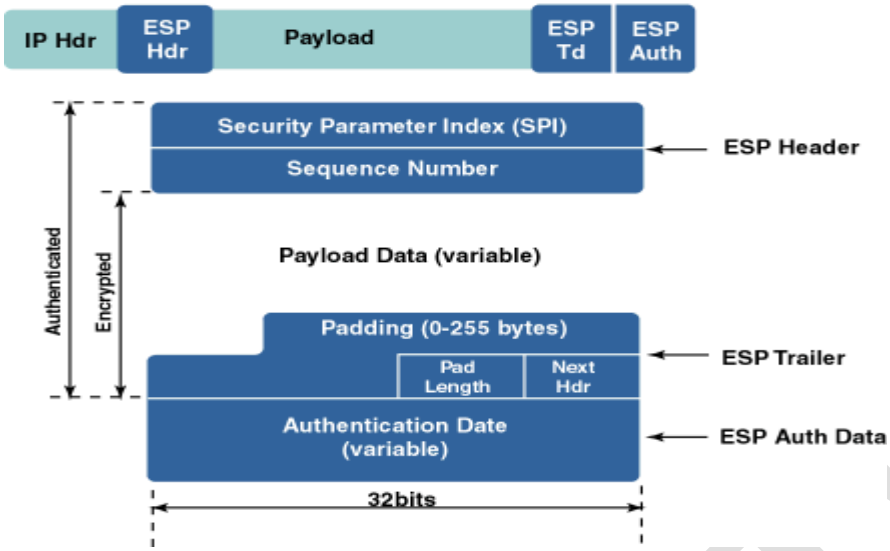
Integrity Check Value (multiple of 32 bits)

Variable length check value. It may contain padding to align the field to an 8-octet boundary for IPv6, or a 4-octet boundary for IPv4.

Encapsulating Security Payload

Encapsulating Security Payload (ESP) is a member of the IPsec protocol suite. In IPsec it provides origin authenticity, integrity, and confidentiality protection of packets. ESP also supports encryption-only and authentication-only configurations, but using encryption without authentication is strongly discouraged because it is insecure.[13][14][15] Unlike Authentication Header (AH), ESP in transport mode does not provide integrity and authentication for the entire IP packet. However, in Tunnel Mode, where the entire original IP packet is encapsulated with a new packet header added, ESP protection is afforded to the whole inner IP packet (including the inner header) while the outer header (including any outer IPv4 options or IPv6 extension headers) remains unprotected. ESP operates directly on top of IP, using IP protocol number 50

The following ESP packet diagram shows how an ESP packet is constructed and interpreted



Security Parameters Index (32 bits)

Arbitrary value which is used (together with the destination IP address) to identify the security association of the receiving party.

Sequence Number (32 bits)

A monotonically increasing sequence number (incremented by 1 for every packet sent) to protect against replay attacks. There is a separate counter kept for every security association.

Payload data (variable)

The protected contents of the original IP packet, including any data used to protect the contents (e.g. an Initialisation Vector for the cryptographic algorithm). The type of content that was protected is indicated by the *Next Header* field.

Padding (0-255 octets)

Padding for encryption, to extend the payload data to a size that fits the encryption's cypher block size, and to align the next field.

Pad Length (8 bits)

Size of the padding in octets.

Next Header (8 bits)

Type of the next header. The value is taken from the list of IP protocol numbers.

Integrity Check Value (multiple of 32 bits)

Variable length check value. It may contain padding to align the field to an 8-octet boundary for IPv6, or a 4-octet boundary for IPv4.

Security association

The IP security architecture uses the concept of a security association as the basis for building security functions into IP. A security association is simply the bundle of algorithms and parameters (such as keys) that is being used to encrypt and authenticate a particular flow in one direction. Therefore, in normal bi-directional traffic, the flows are secured by a pair of security associations.

Security associations are established using the Internet Security Association and Key Management Protocol (ISAKMP). ISAKMP is implemented by manual configuration with pre-shared secrets, Internet Key Exchange (IKE and IKEv2), Kerberized Internet Negotiation of Keys (KINK), and the use of IPSECKEY DNS records

In order to decide what protection is to be provided for an outgoing packet, IPsec uses the Security Parameter Index (SPI), an index to the security association database (SADB), along with the destination address in a packet header, which together uniquely identify a security association for that packet. A similar procedure is performed for an incoming packet, where IPsec gathers decryption and verification keys from the security association database.

For multicast, a security association is provided for the group, and is duplicated across all authorized receivers of the group. There may be more than one security association for a group, using different SPIs, thereby allowing multiple levels and sets of security within a group. Indeed, each sender can have multiple security associations, allowing authentication, since a receiver can only know that someone knowing the keys sent the data. Note that the relevant standard does not describe how the association is chosen and duplicated across the group; it is assumed that a responsible party will have made the choice.

Modes of operation

IPsec can be implemented in a host-to-host transport mode, as well as in a network tunnel mode.

Transport mode

In transport mode, only the payload (the data you transfer) of the IP packet is usually encrypted and/or authenticated. The routing is intact, since the IP header is neither modified nor encrypted; however, when the authentication header is used, the IP addresses cannot be translated, as this will invalidate the hash value. The transport and application layers are always secured by hash, so they cannot be modified in any way (for example by translating the port numbers). Transport mode is used for host-to-host communications.

A means to encapsulate IPsec messages for NAT traversal has been defined by RFC documents describing the NAT-T mechanism.

Tunnel mode

In tunnel mode, the entire IP packet is encrypted and/or authenticated. It is then encapsulated into a new IP packet with a new IP header. Tunnel mode is used to create virtual private networks for network-to-network communications (e.g. between routers to link sites), host-to-network communications (e.g. remote user access), and host-to-host communications (e.g. private chat).

Tunnel mode supports NAT traversal.

UNIT VI

Objective

This unit provides a detail information about how to provide security to the web by using protocols at different levels. It also provides the information about the transactions are to be done using SSL,SET

Web Security Considerations

- The WEB is very visible.
- Complex software hide many security flaws.
- Web servers are easy to configure and manage.
  - Users are not aware of the risks.

Security facilities in the TCP/IP protocol stack

- Network level
- Transport level
- Application level

- Sequence of events for transactions

1. The customer opens an account.
2. The customer receives a certificate.
3. Merchants have their own certificates.
4. The customer places an order.
5. The merchant is verified.
6. The order and payment are sent.
7. The merchant request payment authorization.
8. The merchant confirm the order.

9. The merchant provides the goods or service.

10. The merchant requests payments.

SSL stands for **Secure Socket Layer**. The protocol's name is now officially **TLS** but we will continue to use SSL since that's the better known name.

SSL was designed to permit web browsers and web servers to exchange sensitive information and prevent programs that could view the network traffic from reading the sensitive data.

The SSL documentation is in Secure Socket Layer (SSL) in socket.htm.

SSL has a notion of **client** and **server**. The client contacts the server and sends the first message. The first message causes the client and server to exchange a few messages to negotiate the encryption algorithm to use and to pick an encryption key to use for this connection. Then the client's data is sent to the server. After this is done the client and the server can exchange information at will.

The server must have an SSL certificate and the private key associated with that certificate. An SSL certificate contains the public key for the RSA encryption algorithm. This public key is sent to the client when it connects. The client will use the public key to encrypt a value and send it to the server. The server must then have the corresponding RSA private key so it can decode the client's message. Thus when creating an ssl server stream you must have a file that contains a concatenation of the SSL certificate and the private key associated with that certificate. We supply a sample file you can use to test ssl streams. If you want added privacy you should create or purchase your own SSL certificate. Note that SSL certificates contain other identifying information and have an expiration date. That information is ignored by the Allegro CL SSL interface code. You can use an expired SSL certificate that doesn't correspond to your machine. All the Allegro CL SSL interface cares about is the RSA public key in the certificate.

It is best to use two separate Lisps to test ssl connections. That is because when the client does the first write to the socket it will start a negotiation process that requires the client to write and read a few times. When the client writes the server must be sitting blocked waiting to read or the client write won't return. If you have a Lisp with multiple listener windows then you

can test it in one Lisp as you need the server reading in one window and the client writing in another. In our tutorial we will assume that you have got multiple windows on one Lisp or are running two separate Lisp processes.

SET (Secure Electronic transactions)

When it comes to e-commerce, first thing with pings someone mind is security!! Industry gurus have been putting heart n soul, in order to address this concern. SET was one of endeavor on same lines.

Secure Electronic Transaction (SET) is a standard protocol that is used for securing credit card transactions over insecure networks. With the increase in security concerns over Internet SET has emerged as popular protocol for addressing transactions over Internet. Please note clearly, SET itself is not a payment system. It is a a set of security protocols and formats that enables users to employ the existing credit card payment infrastructure on an open network in a secure fashion!

SET, developed by VISA and MasterCard (Credit card leaders) is based on X.509 certificates having several extensions. [Just FYI: X.509 is an ITU-T standard for a public key infrastructure (PKI. It specifies standard formats many things such as public key certificates, attribute certificates etc…]

SET features

SET has been developed with following features:

- Maintains confidentiality of information: Information is provided only to the concerned recipent.
- SET takes care of Integrity of data.
- SET employs a particular subset of protocol for carrying out cardholder account authentication.
- SET employs a particular subset of protocol for carrying out Merchant authentication.

Understanding SET Protocol SET itself is a family of protocols. The major ones are used for important tasks such as cardholder registration, merchant registration, purchase request, payment authorization, and payment capture. Apart from these major ones there are many minor protocols that are used for conducting tasks like error handling. SET is little complicated than its counterparts such as SSL. Because of this complexity this protocol is hardly used. However, it contains many features of interest such as :

- The model is different from the others. In the registration protocols, the applicant do not need

to possesses any digital proof for his identity. He just needs to authenticates himself by filing a simple registration form. Authentication is done outside this protocol when the cardholder's bank examines the completed form.

- An important innovation that has been introduced in SET is the dual signature. Like electronic signature dual signature is used to guarantee the authentication and integrity of data. Dual signature links two messages that are intended for two different recipients. A customer needs to send the order information (OI) to the concerned merchant and the payment information (PI) to the corrosponding bank. Through this dual signature the receipent only gets to know information he requires rather then getting any other information of the sender. E.g. The merchant does not need to get information about customer's credit card details where as bank does not need to know the details of the customer's order. However, a link is needed so that the customer can prove that the payment is intended for this order.
- SET also uses several types of digital envelopes. It can be understood as an encrypted message that uses both secret key and public key cryptography methods. The secret key is used for encrypting and decrypting the message where as the public key method is meant for sending the secret key to the other party. A digital envelope includes two parts:

    1. One part is encrypted using a public key which contains a fresh symmetric key K and identifying information.
    2. Other part is encrypted using K which conveys the full message text.

    SET employs cryptographic techniques to provide security during a online transaction. Digital certificates and public key cryptography are commonly used to allow parties for authenticating each other and for exchanging information in a secure manner. You must be curious to know how SET works.

UNIT–VII

Objective:

The objective of the unit is to provide a detail information about how the protocols are managed with in a network and how protocols are managed with in multiple networks. to handle such protocols and manage the network it describes a protocol called SNMP

1. Basic Concepts of SNMP

- An integrated collection of tools for network monitoring and control.
  - Single operator interface
  - Minimal amount of separate equipment. Software and network communications capability built into the existing equipment
- SNMP key elements:
  - Management station
  - Managament agent
  - Management information base
  - Network Management protocol
- Protocol context of SNMP

Proxy Configuration

1. SNMP v1 and v2
   - Trap – an unsolicited message (reporting an alarm condition)
   - SNMPv1 is ”connectionless” since it utilizes UDP
   -
   - (rather than TCP) as the transport layer protocol.
   - SNMPv2 allows the use of TCP for ”reliable, connection-oriented” service.

2. Comparison of SNMPv1 and SNMPv2
3. SNMPv1 Community Facility
4. SNMPv1 Administrative Concepts

1. SNMPv3

SNMPv3 defines a security capability to be used in conjunction with SNMPv1 or v2

2. SNMPv3 Flow

3. Traditional SNMP Manager

4. Traditional SNMP Agent.

5. SNMP3 Message Format with USM

6. User Security Model (USM)

Key Localization Process

SNMP was made with one design in mind… to be simple. SNMP is a simple protocol that can be used on just about any networking device in use today. In some environments it's used heavily, in others it's scarce. Some view it as a security threat; others see it as a way to efficiently manage some of their key systems. However you decide to see it, SNMP is a easy to use, easy to set up and not very difficult to understand.

The SNMP protocol was designed to provide a "simple" method of centralizing the management of TCP/IP-based networks – plain and simple. If you want to manage devices from a central location, the SNMP protocol is what facilitates the transfer of data from the client portion of the equation (the device you are monitoring) to the server portion where the data is centralized in logs for centralized viewing and analysis. Many application vendors supply network management software: IBM's Tivoli, Microsoft's MOM and HP Openview are three of over 100+ applications available today to manage just about anything imaginable. The protocol is what makes this happen. The goals of the original SNMP protocols revolved around one main factor that is still in use today: Remote Management of Devices. SNMP is commonly used to manage devices on a network.

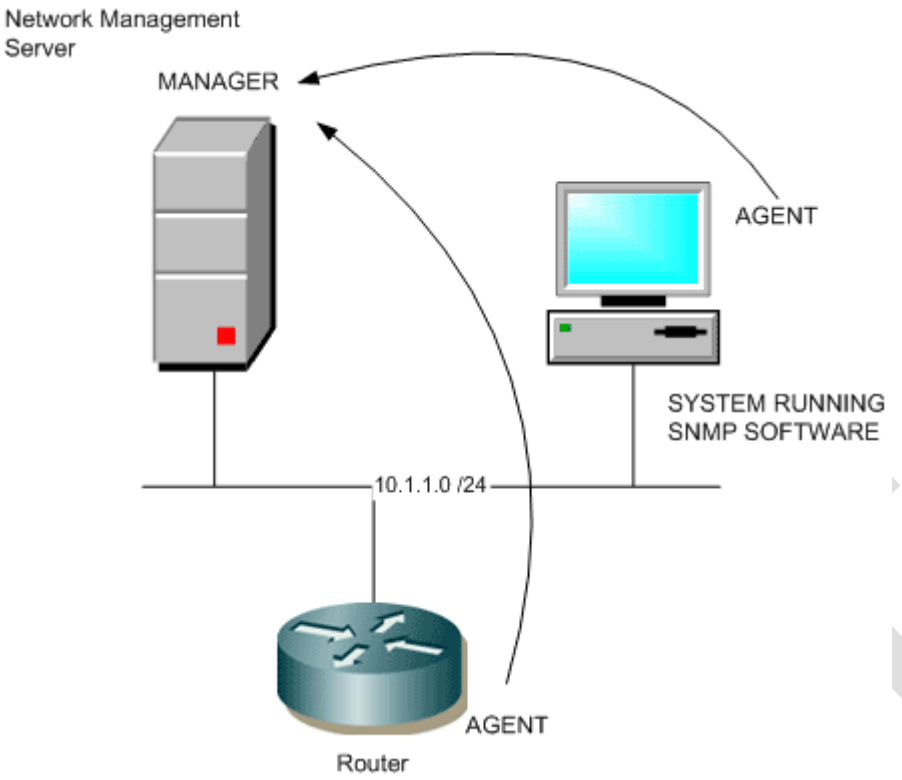
SNMP uses UDP

UDP stands for User Datagram Protocol and is the opposite of TCP, Transmission Control Protocol which is a very reliable and high overhead protocol.

User Datagram Protocol is very low overhead, fast and unreliable. It is defined by RFC 768. UDP is easier to implement and use than a more complex protocol such as TCP. It does however provide plenty of functionality to allow a central manager station to communicate with a remote agent that resides on any managed device that it can communicate with. The unreliability comes in the form of checks and balances whereas if TCP sends something, it waits for an acknowledgment and if it doesn't hear back, it will resend. Since logging of devices usually happens within a time period that is cyclic in nature, then it's common sense that you missed the event and you'll catch it next time… the tradeoff being that the low overhead protocol is simple to use and doesn't eat up all your bandwidth like TCP based applications going across your WAN.

SNMP Operation

SNMP design is pretty simple. There are two main players in SNMP. The manager and the agent. The manager is generally the 'main' station such as HP Openview. The agent would be the SNMP software running on a client system you are trying to monitor.



The manager is usually a software program running on a workstation or larger computer that communicates with agent processes that run on each device being monitored. Agents can be found on switches, firewalls, servers, wireless access points, routers, hubs, and even users' workstations – the list goes on and on. As seen in the illustration, the manager polls the agents making requests for information, and the agents respond when asked with the information requested.

Network Management Station (NMS)

The manager is also called a Network Management Station or NMS for short. The software used to create the NMS varies in functionality as well as expense. You can get cheaper applications with lesser functionality or pay through the nose and get the Lamborghini of NMS systems. Other functionalities of the NMS include reporting features, network topology mapping and documenting, tools to allow you to monitor the traffic on your network, and so on. Some management consoles can also produce trend analysis reports. These types of reports can help you do capacity planning and set long-range goals.

SNMP Primitives

SNMP has three control primitives that initiate data flow from the requester which is usually the Manager. These would be get, get-next and set. The manager uses the *get* primitive to get a single piece of information from an agent. You would use get-next if you had more than one item. When the data the manager needs to get from the agent consists of more than one item, this primitive is used to sequentially retrieve data; for example, a table of values. You can use set when you want to set a particular value. The manager can use this primitive to request that the agent running on the remote device set a particular variable to a certain value. There are two control primitives the responder (manager) uses to reply and that is get-response and trap. One is used in response to the requester's direct query (get-response) and the other is an asynchronous response to obtain the requester's attention (trap). As I mentioned earlier, I alluded to the fact that the manager doesn't always initiate – sometimes the agent can as well. Although SNMP exchanges are usually initiated by the manager software, this primitive can also be used when the agent needs to inform the manager of some important event. This is commonly known and heard of as a 'trap' sent by the agent to the NMS.

The Management Information Base (MIB)

We just learned what primitives were… the agent and the manager, exchanging data. The data they exchange also has a name. The types of data the agent and manager exchange are defined by a database called the management information base (MIB).The MIB is a virtual information store. Remember, it is a small database of information and it resides on the agent. Information collected by the agent is stored in the MIB. The MIB is precisely defined; the current Internet standard MIB contains more than a thousand objects. Each object in the MIB represents some specific entity on the managed device.

SNMPv2 and SNMPv3

With all TCP/IP related protocols, it's a well known fact that anything dating before the creation of IPv6 (or IPng) has security weaknesses such as passwords sent in cleartext. SNMP in its original form is very susceptible to attack if not secured properly, messages sent in cleartext exposing community string passwords, or default passwords of public and private being 'guessed' by anyone who knew how to exploit SNMP… beyond its inherent weaknesses SNMP in its original implementation is still very simple to use and has been widely used throughout the industry. SNMP in its first version lacked encryption or

authentication mechanisms. So, now that SNMP in its first version was good enough, work began to make it better with SNMPv2 in 1994. Besides for some minor enhancements, the main updates to this protocol come from the two new types of functionality, where traps can be sent from one NMS to another NMS as well as a 'get-bulk' operation that allows larger amounts of information to be retrieved from one request. SNMPv3 still being worked on and is incorporating the best of both versions and enhanced security as well. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security features provided in SNMPv3 are message integrity which ensures that a packet has not been tampered with while in transit, authentication which is determining the message is from a valid source and encryption, which is the securing of the packet by scrambling its contents.

Intruders and Viruses

- Intruders
    - Intrusion Techniques
    - Password Protection
    - Password Selection Strategies
    - Intrusion Detection
- **Viruses and Related Threats**
    - Malicious Programs
    - The Nature of Viruses
    - Antivirus Approaches

The problem of intruders in computer networks is rather old. In fact, it has been persistent since the beginning of the computer age. One of the first official documents concerning computer security and intruders is from 1980. It is the so called Anderson report [Ande1980]. Its contents point out how current the threat of intruders was even back then. The Anderson report [Ande1980] defines a lot of intrusion scenarios that are still up-to-date and applicable,

which is one of the reasons that it is still referred to today. On this account, section 2 of this article explains the different types of intruders and their characteristics.

The following section presents several intrusion detection techniques and how intrusions can be prevented. A promising approach for intrusion detection is introduced and its mode of operation is briefly depicted. Considering an example of the effectiveness of this approach we will show how the intrusion detection of this tool works in practice.

Whereas section 3 deals with closing security gaps by means of intrusion detection, section 4 brings out security issues regarding the password management on UNIX, and it describes general problems of the password selection. Good passwords need to be distinguished from bad passwords in order to make it a more difficult task for attackers to guess passwords. We will present some of the techniques that claim to be solutions to these problems and discuss their effectiveness.

TYPES OF INTRUDERS

The term "intruders" compromises more than just human attackers who manage to gain access to computer resources although the resource was not meant to be used by them in the first place. Apart from these human attackers who are popularly called "hackers", intruders can be computer programs that seem to be useful, but contain secret functionality to invade a system or a resource. These programs are also known as Trojan horses. Programs containing viruses can act as intruders too. Computer systems can be any kind of internal network, e.g. within a company. Computer resources can be work stations, mobile computers, as well as computer programs. Although we don't need to distinguish between human attackers and computer programs that perform illicit actions, we need to know some characteristics that define intruders. One has to keep in mind that the following definitions not only apply to human beings, but to illicit computer programs too, although below we will talk about "individuals" acting in different types of threat scenarios. This is done in accordance with most of the

literature about this subject.

In general, three types of intruders can be distinguished: the misfeasor, the masquerader, and the clandestine user. The definition for these terms can be traced back to [Ande1980] which establishes these terms in detail. To refrain from repeating an exhaustive list of definitions only the important differences in the characteristics of misfeasor, clandestine user, and masquerader will be addressed.

Misfeasor

Imagine someone who emails blueprints and schematics the company he works for is holding a patent on to his home email account in order to sell it to a competitor company. Another example of such a misfeasance of ones privileges is printing offensive material at work. Nowadays we can take for granted that someone has access to an email accounts or a printer at work. It is obvious that no data was accessed without authorization in both of these examples. However, the user misused some of his privileges.

On this account we define misfeasor as an individual who works within the scope of his privileges but misuses them.

Clandestine user

Another user might take advantage of a security hole in the operating system in order to gain administrative privileges to a computer resource. How this can be achieved on a recent operating system will be shown in section 3.3 and we define clandestine user as an individual who seizes supervisory control to disengage or avoid security mechanisms of the system such as audit and access controls.

Masquerader

A third individual could steal another user's login id and the associated password. If this data is at the disposal of an attacker he can use the system incognito for his illicit intensions. Yet,

sometimes stealing ids and passwords is not even necessary, because some users might choose very simple passwords, which can be a mere repetition of the login id, some easily accessible information related to their personal life, such as their spouse's name, or a password that is very short, for example only 4 characters or even shorter.

We define masquerader as an individual who overcomes a systems access control to exploit a legitimate user's account.

Common to misfeasor, clandestine user, and masquerader is that either they aim to increase the amount of their privileges or they use the system in an unforeseen way.

If a system is tricked by an attacker to provide users with privileges they did not hold before, the system is in a compromised state.

It has to be noted that misfeasors end clandestine users are internal attackers. That means, initially they are legitimate users having some privileges in the internal network, whereas the masquerader can be an attacker from outside the networks if he happens to correctly guess a password.

IDENTIFYING INTRUDERS

Typically, everyone stores plenty of sensitive data in ones user account, such as personal data, address books, data one is required to carefully protect by law, and data that grants access to other systems or that is supposed to prove one's identity for example. It is fairly easy to find examples for each of these types of data:

Personal data could be emails from your spouse. Address books might contain phone numbers and addresses of the suppliers the company does business with. Time tracking of engineers has to be handled with great care. Furthermore, if one has stored passwords or private and public keys on ones account, the security systems that try to grant secure access to other systems or that try to prove one's identity by these means will be useless. Moreover, if such sensible data can be accessed by others the owner runs a high risk of financial losses and

personal harm.

INTRUSION DETECTION

The threats of attackers have to be addressed to. To this end intrusion detection techniques have been developed to close security gaps of operating systems and network access controls. Below different types of intrusion detection techniques will be introduced briefly and an overview of their weaknesses and strengths will be given as they appear in [Stal2003] and [Ilgu1995].

- **Threshold Detection**

Threshold Detection is one of the most rudimentary intrusion detection techniques compared to the other ones. The idea of this approach is to record each occurrence of a suspicious event and to compare it to a threshold number. However, it turns out that establishing threshold numbers as well as rating the security relevance of events is a rather difficult task which is often based on experiences and intuition. An implementation of this approach was developed at Los Alamos National Laboratory and it is called NADIR.

- **Anomaly Detection**

Anomaly Detection is one of the earliest approaches which try to meet requirements described in [Ande1980] to distinguish masquerader, misfeasor, and clandestine user. Implementations of this approach are realized in statistical or rule based forms. Typically, anomaly detection requires little knowledge of the actual system beforehand. In fact, usage patterns are established automatically by means of neural networks for example. Intrusion detection systems that have already implemented this approach are IDES, Wisdom & Sense, and TIM.

- **Rule-based Penetration Identification**

Rule-based Penetration Identification systems are expert systems that recognize single events as well as sequences of events. The foundation pillar of this approach is a suspicious record for each user. Initially this record has the value zero and the more suspicious a user becomes,

the higher his suspicious record. Examples that implement this technique are IDES, NADIR, and Wisdom and Sense.

- **Model-based Intrusion Detection**

A higher level of abstraction than the approaches above is characteristic of this intrusion detection technique. The objective of Model-based Intrusion Detection is to build penetration scenarios of network rather than characterizing the behavior of a specific user. For identifying penetrations the pieces of evidence are evaluated against a hypothesis.

VIRUS AND RELATED THREATS

VIRUS

Computer Virus is a kind of malicious software written intentionally to enter a computer without the user's permission or knowledge, with an ability to replicate itself, thus continuing to spread. Some viruses do little but replicate others can cause severe harm or adversely effect program and performance of the system.

TYPES OF VIRUS

Resident Viruses

This type of virus is a permanent which dwells in the RAM memory. From there it can overcome and interrupt all of the operations executed by the system: corrupting files and programs that are opened, closed, copied, renamed etc.

Examples include: Randex, CMJ, Meve, and MrKlunky.

Boot Virus

This type of virus affects the boot sector of a floppy or hard disk. This is a crucial part of a disk, in which information on the disk itself is stored together with a program that makes it possible to boot (start) the computer from the disk.
The best way of avoiding boot viruses is to ensure that floppy disks are write-protected and

never start your computer with an unknown floppy disk in the disk drive.

Examples of boot viruses include: Polyboot.B, AntiEXE.

Macro Virus

Macro viruses infect files that are created using certain applications or programs that contain macros. These mini-programs make it possible to automate series of operations so that they are performed as a single action, thereby saving the user from having to carry them out one by one.

Examples of macro viruses: Relax, Melissa.A, Bablas, O97M/Y2K.

Polymorphic Virus

Polymorphic viruses encrypt or encode themselves in a different way (using different algorithms and encryption keys) every time they infect a system.This makes it impossible for anti-viruses to find them using string or signature searches (because they are different in each encryption) and also enables them to create a large number of copies of themselves.

Examples include: Elkern, Marburg, Satan Bug, and Tuareg.

Parasitic Viruses

Parasitic viruses modify the code of the infected file. The infected file remains partially or fully functional.Parasitic viruses are grouped according to the section of the file they write their code to:

- Prepending: the malicious code is written to the beginning of the file
- Appending: the malicious code is written to the end of the file
- Inserting: the malicious code is inserted in the middle of the file

Inserting file viruses use a variety of methods to write code to the middle of a file: they either move parts of the original file to the end or copy their own code to empty sections of the target file.

WORMS

A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program.

LOGIC BOMB

A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files (such as the salary database trigger), should they ever leave the company.

TROJAN HORSES

The Trojan horse, also known as trojan, in the context of computing and software, describes a class of computer threats (malware) that appears to perform a desirable function but in fact performs undisclosed malicious functions that allow unauthorized access to the host machine, giving them the ability to save their files on the user's computer or even watch the user's screen and control the computer.

MALWARE

Malwareis software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

SPYWARE

Spyware is computer software that is installed surreptitiously on a personal computer to collect information about a user, their computer or browsing habits without the user's informed consent.

UNIT–VIII

Objective :

The unit gives a detailed information the firewalls and there principal strategier principal Strategies to overcome different types of attacks that come across over internet and personal computers

Firewalls

- Firewall Design Principles
- Firewall Characteristics
- Types of Firewalls
    - Packet-filtering routers
    - Application-level gateways
    - Circuit-level gateways

Trusted Systems:.

- Data Access Control.
- The Concept of Trusted Systems.
- Trojan Horse Defense

Network Firewalls operate at different layers of the OSI and TCP/IP network models. The lowest layer at which a firewall can operate is the third level which is the network layer for the OSI model and the Internet Protocol layer for TCP/IP. At this layer a firewall can determine if a packet is from a trusted source but cannot grant or deny access based on what it contains. Firewalls that operate at the highest layer,

which is the application layer, know a large amount of information including the source and the packet contents. Therefore, they can be much more selective in granting access. This may give the impression that firewalls functioning at a higher layer must be better, which is not necessarily the case. The lower the layer the packet is intercepted the more secure the system. If the intruder cannot get past the third layer, it is impossible to gain control of the operating system.

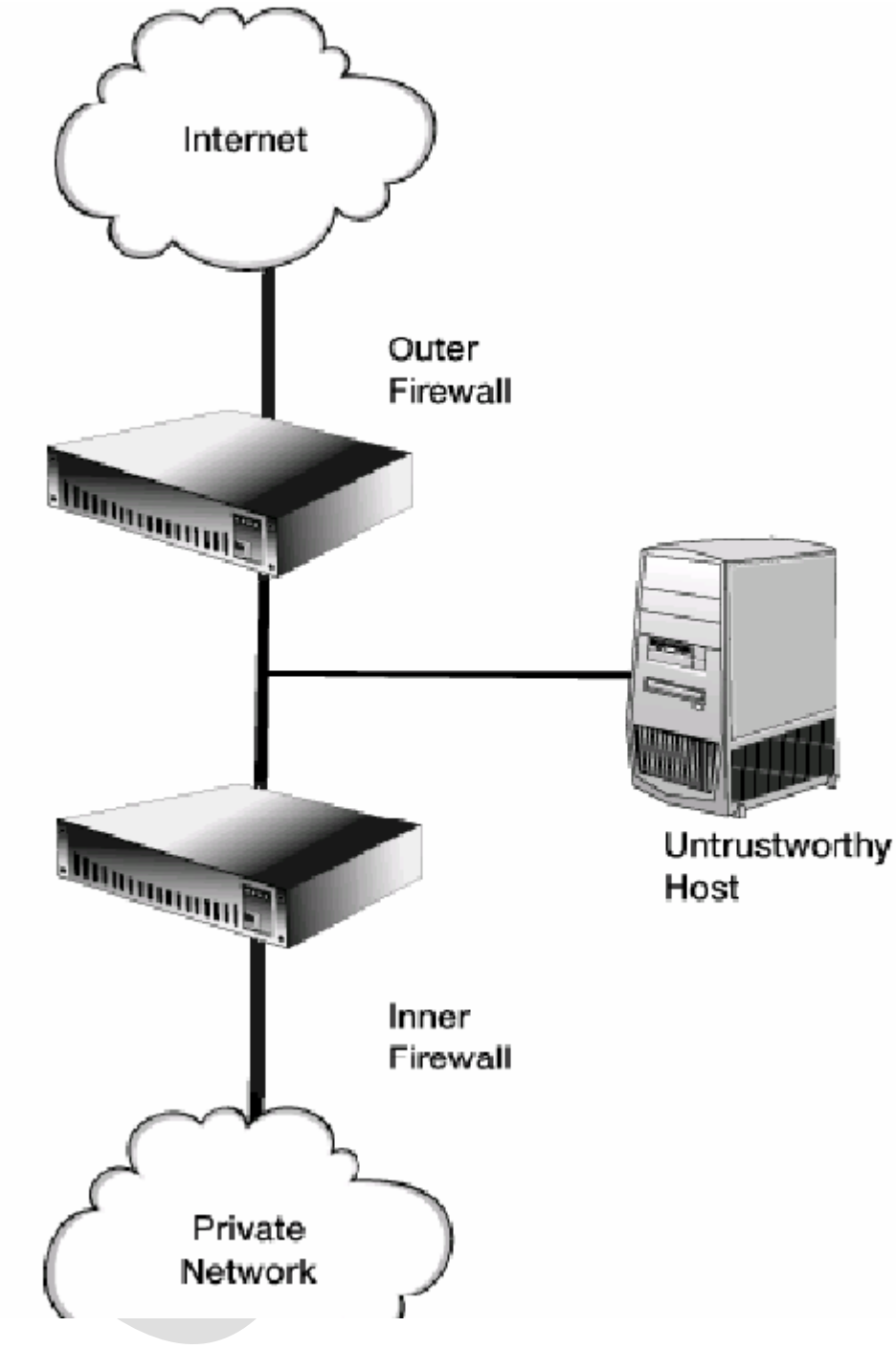
Firewalls fall into four broad categories: packet filters, circuit level gateways, application level gateways and stateful multilayer inspection firewalls. Packet filtering firewalls operate at the network level of the OSI model or the IP layer of TCP/IP. In a packet filtering firewall, each packet is compared to a set of rules before it is forwarded. The firewall can drop the packet, forward it, or send a message to the source. Circuit level gateways operate at the session layer of the OSI model, or the TCP layer of TCP/IP. Circuit level gateways examine each connection setup to ensure that it follows legitimate TCP handshaking. Application level gateways or proxies operate at the application layer. Packets received or leaving cannot access services for which there is no proxy. Stateful multilayer inspection firewalls combine aspects of the other three types of firewalls. They filter packets at the network layer, determine whether packets are valid at the session layer, and assess the contents of packets at the application layer.

Firewall Architectures

After deciding the security requirements for the network the first step in designing a firewall is deciding on a basic architecture. There are two classes of firewall architectures, single layer and multiple layer. In a single layer architecture, one host is allocated all firewall functions. This method is usually chosen when either cost is a key factor or if there are only two networks to connect. The advantage to this architecture is any changes to the firewall need only to be done at a single host.

The biggest disadvantage of the single layer approach it provides single

entry point. If this entry point is breached, the entire network becomes vulnerable to an intruder. In a multiple layer architecture the firewall functions are distributed among two or more hosts normally connected in series. This method is more difficult to design and manage, it is also more costly, but can provide significantly greater security by diversifying the firewall defense. A common design approach for this type of architecture using two firewall hosts with a demilitarized network (DMZ) between them separating the Internet and the internal network. Using this setup traffic between the internal network and the Internet must pass through two firewalls and the DMZ



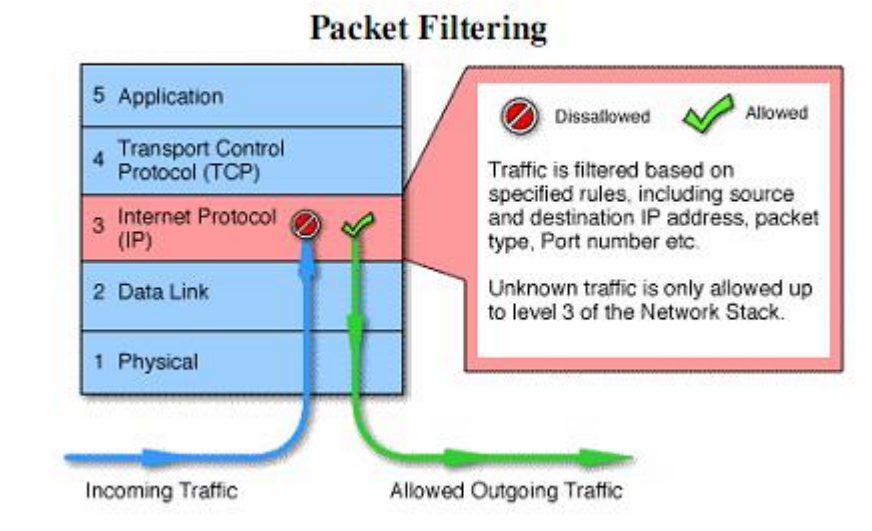
Firewall Types

After the security requirements are established, a basic architecture is selected then Firewall functions can be chosen to meet these needs. The following is a

detailed discussion of the 4 firewall categories:

Packet Filtering Firewalls :

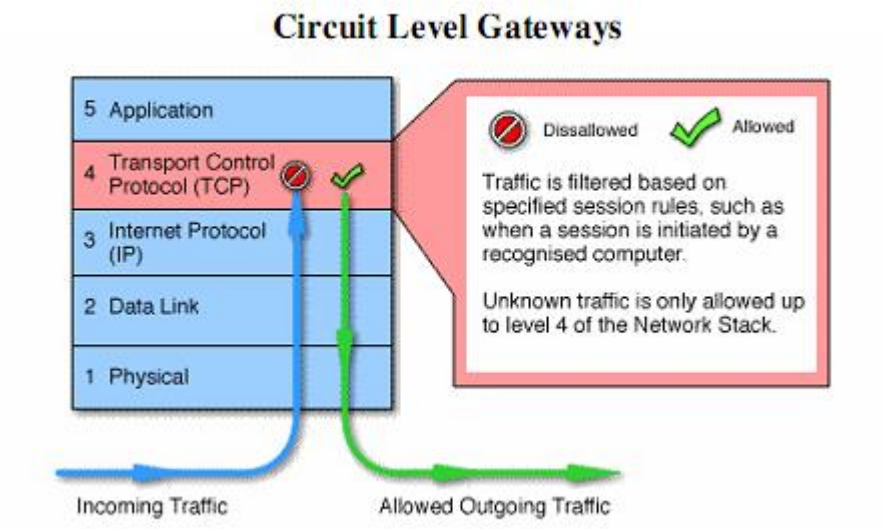
The first generation of firewall architectures appeared around 1985 and came out of Cisco' s IOS software division. These are called packet filter firewalls.[4] Packet Filtering is usually performed by a router as part of a firewall. A normal router decides where to direct the data, a packet filtering router decides if it should forward the data at all. Packet Filtering rules can be set on the following: physical network interface the packet arrives on; source or destination IP address, the type of transport layer (TCP, UDP, ICMP), or the transport layer source or destination ports. Packet filtering firewalls are low cost, have only a small effect on the network performance, and do not require client computers to be configured in any particular way. However, packet filtering firewalls are not considered to be very secure on their own because they do not understand application layer protocols. Therefore, they cannot make content-based decisions on the packets, which makes them less secure than application layer and circuit level firewalls. Another disadvantage of Packet filtering firewalls are they are stateless and do not retain the state of a connection. They also have very little or no logging capability which makes it hard to detect if the network is under attack. Testing the grant and deny rules is also difficult which may leave the network vulnerable or incorrectly configured.



Circuit Level Gateways :

Around 1989-1990, Dave Presotto and Howard Trickey of AT&T Bell Labs pioneered the second generation of firewall architectures with research in circuit relays which were called circuit level gateways.[4] Circuit level gateways are used for TCP connections to observe handshaking between packets to ensure a requested session is legitimate. Normally, it would store the following information: a unique session identifier, the state of the connection (i.e., handshake established or closing), sequencing information, source or destination IP address, and the physical network interface through which the packet arrives or departs. The firewall then checks to see if the sending host has permission to send to the destination, and that the receiving host has permission to receive from the sender. If the connection is acceptable, all packets are routed through the firewall with no more security tests. The advantages of circuit level gateways is that they are usually faster than application layer firewalls

because they perform less evaluations and they can also protect a network by blocking connections between specific Internet sources and internal hosts. The main disadvantages to circuit level gateways are that they cannot restrict access to protocol subsets other than TCP and similarly to packet filtering, testing the grant and deny rules can be difficult which may leave the network vulnerable or incorrectly configured.



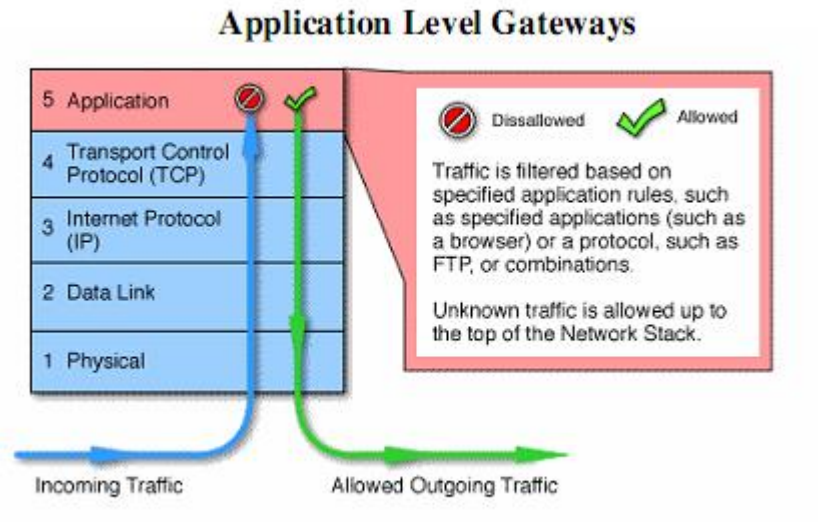
Application Level Gateways :

The third generation of firewall architectures called Application level gateways was independently researched and developed during the late 1980s and early 1990s mainly by Gene Spafford of Purdue University, Marcus Ranum, and Bill Cheswick of AT&T Bell Laboratories.[4] Application level gateways or proxy firewalls are software applications with two primary modes (proxy server or proxy client). When a user on a trusted network wants to connect to a service on an

untrusted network such as the Internet, the request is directed to the proxy server on the firewall. The proxy server pretends to be the real server on the Internet. It checks the request and decides whether to permit or deny the request based on a set of rules. If the request is approved, the server passes the request to the proxy client, which contacts the real server on the Internet. Connections from the Internet are made to the proxy client, which then passes them on to the proxy server for delivery to the real client. This method ensures that all incoming connections are always made with the proxy client, while outgoing connections are always made with the proxy server. Therefore, there is no direct connection between the trusted and untrusted networks. The main advantages are that application level gateways can set rules based on high-level protocols, maintain state information about the communications passing through the firewall server, and can keep detailed activity records. The main disadvantages are its complex filtering and access control decisions can require significant

are its complex filtering and access control decisions can require significant

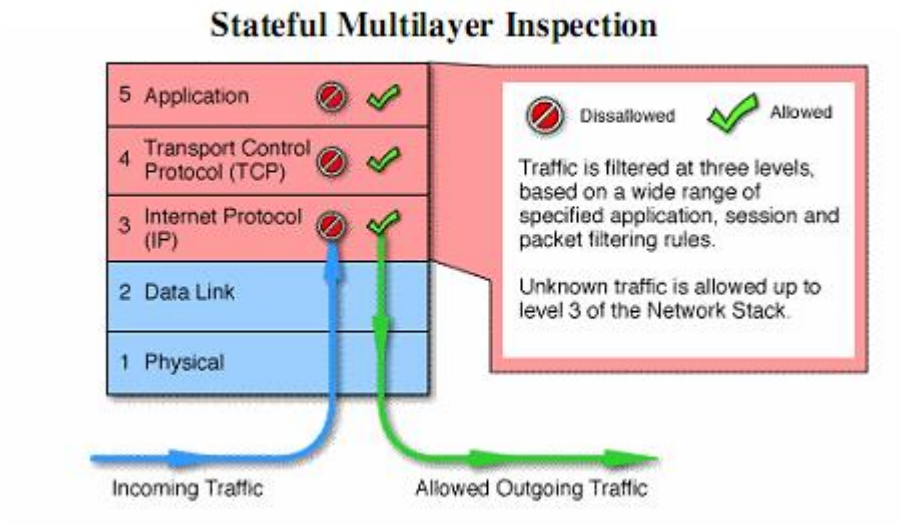
computing resources which can cause performance delays and its vulnerability to operating system and application level bugs.



Stateful Multilayer Inspection Firewalls :

Check Point Software released the first commercial product based on this fourth generation architecture in 1994 called stateful multilayer inspection firewalls.[4] Stateful multilayer inspection firewalls provide the best security of the four firewall types by monitoring the data being communicated at application socket or port layer as well as the protocol and address level to verify that the request is functioning as expected. An example is if during an FTP session the port numbers being used or an IP address were to change, the firewall would not permit the connection to continue. Another advantage is when a specific session is complete, any ports that were being used are closed. Stateful inspection systems can dynamically open and close ports for each session which differs from basic packet filtering that leaves ports in a constant opened or closed state. The main disadvantage to stateful multilayer inspection firewalls is that they can be costly because they

require the purchase of additional hardware and/or software that is not normally packaged with a network device.



15.ADDITIONAL TOPICS

1.WHIRLPOOL

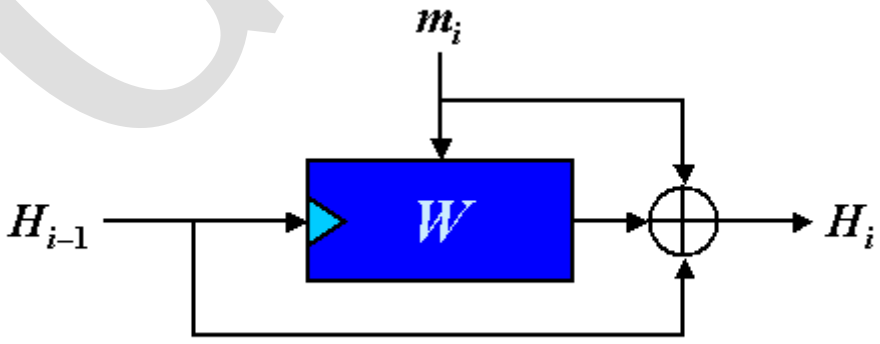
WHIRLPOOL is a hash function designed by Vincent Rijmen and Paulo S. L. M. Barreto that operates on messages less than 2^{256} bits in length, and produces a message digest of 512 bits.

Historically, **WHIRLPOOL** had three versions. The first version, **WHIRLPOOL-0**, was submitted to the NESSIE project. Its "tweaked" successor, **WHIRLPOOL-T**, was selected for the NESSIE portfolio of cryptographic primitives. A flaw in its diffusion layer reported by Shirai and Shibutani ("On the diffusion matrix employed in the Whirlpool hashing function," NESSIE public report, 2003) was fixed afterwards, and the final version (called simply **WHIRLPOOL** for short) was adopted by the International Organization for Standardization (**ISO**) in the ISO/IEC 10118-3:2004 standard.

The function

WHIRLPOOL uses Merkle-Damgård strengthening and the Miyaguchi-Preneel hashing scheme with a dedicated 512-bit block cipher called ***W***. This consists of the following. The bit string to be hashed is padded with a &lquo;'1'-bit, then with a sequence of '0'-bits, and finally with the original length (in the form of a 256-bit integer value), so that the length after padding is a multiple of 512 bits. The resulting message string is divided into a sequence of 512-bit blocks m_1, m_2, ... m_t which is then used to generate a sequence of intermediate hash values H_0, H_1, H_2, ... H_t. By definition, H_0 is a string of 512 '0'-bits. To compute H_i, ***W*** encrypts m_i using H_{i-1} as key, and XORs the resulting ciphertext with both H_{i-1} and m_i. Finally, the **WHIRLPOOL** message digest is H_t.

Miyaguchi-Preneel compression function:



The internal *W* block cipher

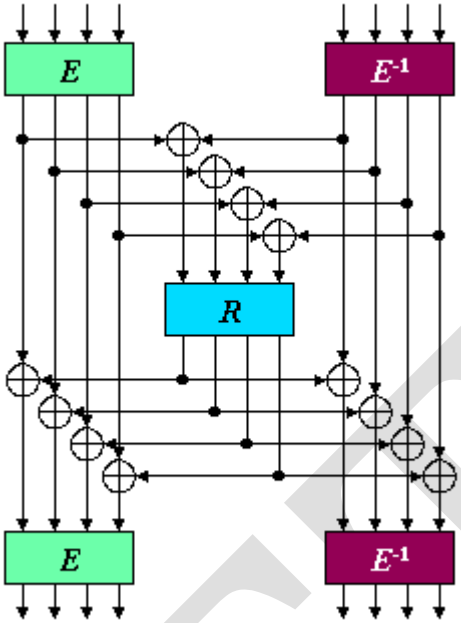
The ***W*** block cipher used by **WHIRLPOOL** is very similar to the AES algorithm, RIJNDAEL, the main differences being sketched in the following table:

Table 1: Differences between RIJNDAEL and *W*

	RIJNDAEL	***W***
Block size (bits)	128, 160, 192, 224, or 256	always 512
Number of rounds	10, 11, 12, 13, or 14	always 10
Key schedule	dedicated *a priori* algorithm	the round function itself
GF(2^8) reduction polynomial	$x^8 + x^4 + x^3 + x + 1$ (`0x11B`)	$x^8 + x^4 + x^3 + x^2 + 1$ (`0x11D`)
Origin of the S-box	mapping $u \rightarrow u^{-1}$ over GF(2^8), plus affine transform	recursive structure (see below)
Origin of the round constants	polynomials x^i over GF(2^8)	successive entries of the S-box
Diffusion layer	left-multiplication by the 4×4 circulant MDS matrix cir(2, 3, 1, 1)	right-multiplication by the 8×8 circulant MDS matrix cir(1, 1, 4, 1, 8, 5, 2, 9)

The ***W*** S-box, which in the original submission is generated entirely at random (i.e. lacks any internal structure), by a recursive structure: the new 8×8 substitution box is composed of smaller 4×4 "mini-boxes" (the exponential *E*-box, its inverse, and the pseudo-randomly generated *R*-box).

The recursive structure of the "tweaked" *S*-box:



The *E* mini-box:																
u	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
***E*(*u*)**	1	B	9	C	D	6	F	3	E	8	7	4	A	2	5	0

The E^{-1} mini-box:																
u	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$E^{-1}(u)$	F	0	D	7	B	E	5	A	9	2	C	1	3	4	8	6

The *R* mini-box:																
u	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
***R*(*u*)**	7	C	B	D	E	4	9	F	6	3	8	A	2	5	1	0

2. Computer Forensics

Computer security and computer forensics are distinct but related disciplines due to the degree of overlap of raw material used by both fields. In general, computer security aims to preserve a system as it is meant to be (as per the security policies) whereas computer forensics (and especially network or intrusion forensics) sets out to explain how a policy became violated. Therefore, the main difference can be seen as one of system integrity versus culpability for an event or set of events.

Whereas the two fields may use similar data sources, they have different and sometimes opposing aims. For example, security countermeasures such as encryption or data wiping tools may work against the computer forensic investigation. The security measures will complicate the investigation as the data must be decrypted prior to analysis. In addition, security functions tend to only implement minimal logging by design. Therefore, not all the information required will be available to the forensic analyst.

Computer security is an established field of computer science, whilst computer forensics is an emergent area. Increasingly, computer security will involve forensic investigation techniques, and vice versa. Therefore, both fields have much to learn from each other.

Tutorial-1

1. Explain security attacks, services and the related mechanisms
2. Explain internetwork security
3. Explain internet standers and RFCin detail
4. Explain Man-in the middle attack?
5. Explain how gateway works in internetwork security model
6. Explain how Address Resolution Protocol table becomes a victim for attacks.

Tutorial-2

1 Explain about conventional principles for encryption
2 Describe basic fiestal cipher structure for principle encryption algorithms
3 Explain basic DES algorithm and how it is dependent on fiestal structure
4 Describe one way hash functions for message authentication
5 Explain how SHA-512 works for message authentication
6 Describe hoe hash functions was developed based on MAC code

Tutorial-3

1. Describe public-key cryptography principles
2. Explain how public key cryptography algorithms are framed depending upon the principles
3. Explain RSA algorithms in detail\
4. Explain how key exchange is done using Diffie-Hellman key exchange
5. In detail explain Kerberos 4 and version 4 authentication dialogue
6. Explain how certification are issued using x.509 authentication service
7. Explain Kerberos realms and multiple kerberos

Tutorial-4

1. Explain the features of PGP
2. Explain how key rings work during message authentication and encryption
3. Explain S/MIME?
4. Describe the concepts of MIME
5. Explain the following
    a. Compatability
    b. Key legitimacy
    c. Multipart and message type in MIME

16.

Tutorial-5

1. Explain the architecture of IPSec
2. With a neat diagram explain the architecture of authentication header
3. Explain how encapsulation security payload works
4. Explain how key management is done in IP sec
5. Describe security association

Tutorial-6

1. Describe the requirements in web security
2. Describe how SSL works
3. Explain about TLS
4. Describe SET in detail
5. Explain secure session layer architecture with its requirements with a neat diagram

Tutorial-7

1. Explain the basic concepts of SNMP
2. Explain the features of SNMPv2
3. Differentiate SNMPv2 from SNMPv3
4. Explain the concept of intruders in detail
5. Write a brief notes on the concept of hacking
6.

Tutorial-8

1. Explain how the principles of firewall works in security
2. Write a brief notes on intrusion detection systems
3. Write a detailed notes on firewall
4. List three design goals for a firewall
5. What is IP address spoofing and how can it be prevented using a firewall

17.PREVIOUS QUESTION PAPERS

Code No: 2320504 **Set No. 1**

III B.Tech II Semester Regular Examinations, April/May 2009
INFORMATION SECURITY
(Computer Science & Engineering)

Time: 3 hours **Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) "Internetwork security is both fascinating and complex" - Justify the statement with valid reasoning.
   (b) Explain the terms related to Buffer overflow:
      i. Stack dumping
      ii. Execute Payload. [8+8]
2. (a) Explain with a neat illustration the automatic key distribution.
   (b) Explain the various steps involved in the HMAC algorithm. [8+8]
3. (a) Explain the procedure involved in RSA public-key encryption algorithm.
   (b) Explain what Kerberos is and give its requirements. [8+8]
4. (a) Explain the following terms in relation with the e-mail software - PGP:
      i. E-mail compatibility
      ii. Segmentation and reassembly.
   (b) Describe how authentication and confidentiality are handled in S/MIME. [8+8]
5. (a) When tunnel mode is used, a new outer IP header is constructed. For both IPV4 and IPV6, indicate the relationship of each outer IP header field and each extension header in the outer packet to the corresponding field or extension header of the inner IP packet. That is, indicate which outer values are derived from inner values and which are constructed independently of the inner values?
   (b) IP Sec Architecture document mandates support for two types of key management. What are they? [12+4]
6. Explain how the following threats to web security can be defended by SSL.
   (a) Known plaintext dictionary attack
   (b) Replay attack
   (c) Password sniffing
   (d) SYN flooding. [16]

7. (a) Explain how proxy accommodates devices that do not implement SNMP?
   (b) Discuss SNMPV1 administrative concepts. [8+8]

8. (a) What are two default policies that can be taken in a packet filter if there is no match to any rule? Which is more conservative? Explain with example rule sets both the policies?
   (b) What are the advantages of decomposing a user operation into elementary actions?
   (c) What are false negatives and false positives? [6+6+4]

Code No: 2320504 **Set No. 2**

III B.Tech II Semester Regular Examinations, April/May 2009
INFORMATION SECURITY
(Computer Science & Engineering)

Time: 3 hours **Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) "Gaining control over the Routing tables at layer 3 is one of the attacks" - explain how Route tables modification is crucial.
   (b) Explain how Buffer overflow is created for any known platforms (eg., WINDOWS NT / LINUX). [8+8]
2. (a) Describe the various steps of encryption and decryption in an AES algorithm.
   (b) Write about Message authentication. [10+6]
3. (a) What is Key exchange? What is its importance? Discuss the Diffie-Hellman key exchange algorithm.
   (b) Explain the Digital Signature Algorithm (DSA) with a relevant example. [8+8]
4. (a) Explain the importance and usage of the following in relation to PGP:
      i. Session key
      ii. Signature
      iii. Public / Private keys.
   (b) Describe how S/MIME works towards emerging as an industry standard for e-mail security at commercial and organizational use levels. [8+8]
5. (a) When tunnel mode is used, a new outer IP header is constructed. For both IPV4 and IPV6, indicate the relationship of each outer IP header field and each extension header in the outer packet to the corresponding field or extension header of the inner IP packet. That is, indicate which outer values are derived from inner values and which are constructed independently of the inner values?
   (b) IP Sec Architecture document mandates support for two types of key management. What are they? [12+4]
6. (a) With a neat diagram explain SSL record protocol operation?
   (b) Discuss about the passive attacks and active attacks in WWW? [10+6]
7. (a) Draw the figure showing VACM logic and explain?
   (b) The encryption scheme used for UNIX passwords is one way; it is not possible to reverse it. Therefore, would it be accurate to say that this is, in fact, a hash code rather than an encryption of the password. [8+8]

8. (a) What is a bastion host? List the common characteristics of a bastion host?
   (b) Explain the concept of reference monitor in detail with a neat sketch? [8+8]

Code No: 2320504 **Set No. 3**

III B.Tech II Semester Regular Examinations, April/May 2009
INFORMATION SECURITY
(Computer Science & Engineering)

Time: 3 hours **Max Marks: 80**

Answer any FIVE Questions
All Questions carry equal marks

⋆ ⋆ ⋆ ⋆ ⋆

1. (a) Explain about how the Internet standards and RFCs.
   (b) Explain how Address Resolution Protocol table becomes a victim for attacks. [8+8]
2. (a) Compare AES cipher versus RC4 encryption algorithm.
   (b) Compare and contrast SHA-1 and HMAC functions. [8+8]
3. (a) Alice and Bob wish to share private messages, where each of them of two separate keys generated. What kind of strategy would you suggest to ensure confidentiality, key management and authentication for the conversation between Alice and Bob? Explain the strategy and also highlight the design issues related to the strategy proposed.
   (b) Describe the X.509 version 3 in detail. [8+8]
4. (a) Explain how the exchange of secret key takes place between 'X' and 'Y' users with PGP.
   (b) Write about the MIME Content types. [8+8]
5. (a) Discuss about the documents regarding IPSec protocol?
   (b) Describe any four ISAKMP payload types listing the parameters of the payload? [8+8]
6. Describe how brute-force attack and man-in-the-middle attack can be counted by SSL? [16]
7. (a) Draw the figure indicating the relationship among the different versions of SNMP by means of the formats involved. Explain.
   (b) Discuss in detail the advanced anti virus techniques? [6+10]
8. (a) What can be the two main attacks on corporate networks?
   (b) Give a detailed description of the two approaches to intrusion detection? [4+12]

⋆ ⋆ ⋆ ⋆ ⋆

18.UNIT WISE QUESTION BANK

UNIT-I

1. What is man-in-the-middle attack? Explain with an example?
2. List and explain the different internet standards related to information rmation security?
3. Explain the buffer overow attack with an example?
4. Explain the format string vulnerability?
5. What is TCP session hijacking?
6. Explain UDP hijacking?
7. Explain the route table modification vulnerability?
8. Explain the security mechanisms?

UNIT-II

1. Write short notes on: Location of encryption devices,Fiestel cipher structure.
2. Explain the block cipher modes of operation?
3. What is the difference between a block cipher and a stream cipher?
4. What is a product cipher?
5. Explain the fiestel cipher structure?
6. Explain the AES algorithm?

UNIT-III

1. Explain the procedure involved in RSA public-key encryption algorithm?
2. Explain what Kerberos is and give its requirements.
3. Explain how confidentiality service is achieved in public key cryptography?
4. Explain the operation of Kerberos?
5. What are three broad categories of application of public key cryptosystems?
6. What requirements must a public key cryptosystem fulfil to be a securealgorithm?
7. Describe the approaches of key distribution in public key cryptosystems?
8. Explain the X.509 authentication procedures?
9. Describe the approaches of key distribution in public key cryptosystems?

UNIT-IV

1. Compare and contrast the nature of certificates in PGP andS/MIME.
2. Explain the web of trust made from certi_cates in PGP and in
3. Explain S/MIME?
4. List and explain the PGP services?
5. Draw and explain the transmission and reception of PGP messages?

6. Explain the general structure of private and public key rings?
7. Explain the PGP trust model?
8. Explain MIME encoding techniques?
9. What is Radix-64 format? Explain how both PGP and S/MIME perform the
10. Radix-64 conversion is performed.
11. Describe the negative principal services that Pretty Good Privacy (PGP) provides

UNIT-V

1. Explain about the routing applications of IPSec?
2. Give the formats of ISAKMP header and Generic payload header? Explain
3. various fields?
4. Explain the benefits of IPSec?
5. Give an overview of IPSec document?
6. Explain the anti-replay mechanism in IPSec?
7. Explain how Diffie-Hellman protocol is vulnerable to man-in-the-middle attack? How is rectified in Oakley protocol?
8. Discuss the purpose of SA selectors?
9. Enumerate on the _ve default ISAKMP exchange types?

UNIT-VI

1. What is the difference between an SSL connection and an SSL session? List and briey explain the parameters that define an SSL session state?
2. Explain the various web security threats?
3. List and explain the SET requirements?
4. Explain the operations of SSL Record Protocol?
5. Explain the various web security threats?
6. Explain the significance of dual signature in SET?
7. What are the steps involved in the SSL record protocol transmission?
8. Explain the construction and purpose of dual signature?

UNIT-VII

1. Discuss the key elements included in the model of network management used for SNMP?
2. Explain the functional enhancements made in SNMPV2 over SNMPV1
3. What is the role of compression and encryption in the operation of a virus?
4. Explain the SNMPv3?
5. Explain the principles and limitations of a firewall?
6. Statistical anomaly detection
7. Application-level gateway.

8. What is the structure of a virus?
9. Discuss the two techniques for developing an effective and efficient proactive password checker?

UNIT-VIII

1. Explain the intrusion detection tool audit records?
2. What are the services provided by Firewalls?
3. Describe the main characteristics of computer virus.
4. Write short note on intruder?
5. Explain the general structure of private and public key rings?
6. Explain the PGP trust model?
7. Explain MIME encoding techniques?
8. Explain the different types of firewall configurations?
9. With a neat diagram explain the working principle of packet-filtering
10. router?
11. (What is a reference monitor? What are the rules that it has to enforce?
12. Discuss its properties?

19.ASSIGNMENT QUESTIONS

Assignment -1

1 Describe security attacks in brief
2 Explain in brief internetwork security
3 Explain internet network standards and the internetwork society
4 Explain about Man-in-the-middle attack
5 What is UDP and TCP HIJACKING?
6 Explain the Security services mentioned in X.800 in detail.

Assignment -2

1. Explain conventional encryption principles
2. Explain DES encryption algorithm in brief with diagrams
3. Explain different cipher blocks modes of operation
4. Explain SHA-1 secure hash function in detail
5. Explain the approaches to message authentication
6. Explain terms related to key distribution methods:
   i. Session key
   ii. Master key
   iii. Key distribution center

Assignment -3

1. Explain the RSA public –key encryption algorithm in detail
2. Explain Diffie- Hellman key exchange
3. Explain different crypto algorithms where public key cryptosystems are used
4. Explain the context of kerberos in details
5. Describe X.506 directory authentication service
6. Explain the concepts of digital signatures

Assignment -4

1 Describe the following relation with S/MIME
   a. RFC 822
   b. MIME Header fields
   c. MIME Content types
2 Explain the following terms in relation with the e-mail software - PGP
   a. E-mail compatibility
   b. compression
3 Describe clearly the Public key management in PGP
4 Show how the s/mime certification process in carried out in PGP
5 Explain the concept of key legitimacy with a neat diagram

Assignment-5

1. Explain IP security architecture
2. Describe in brief about Authentication header
3. Explain how encapsulating security payload provides confidentiality

4. Explain in details about combinations in security association
5. Explain the key management portioned IPSec

Assignment-6

1. Explain how SSL architecture provides security services?
2. Explain SET encryption and security specification
3. Explain different SSL protocol

Assignment -7

1 .Explain the functionality SNMP protocol
2. Explain in relationship among SNMPv1, SNMPv2, and SNMPv3?
3. Write short notes about elements of the VACM model
4. Explain the concept of intruders, viruses and threats
5. Describe in details about intrusion detection

Assignment -8

1Explain firewall design principles
2. Explain the concept of data access control
3. Explain common criteria for information technology security evaluation
4. What is the difference between a packet filtering router and a stateful inception firewall
5. What is application level gateway?

18.Discussion Topics

1. Biometrics
2. Blowfish
3. Elgamal
4. Rabin
5. Brain Gate Technology
6. Cryptography and Steganography
7. Distributed Firewalls
8. Encrypted hard disks
9. Encrypted Text chat Using Bluetooth
10. Firewalls
11. Human Area Networks

19.**OBJECTIVE QUESTIONS**

Unit-1

1. Which of the following documents provides the description of a packet authentication extension to IPv4 and IPv6

a. RFC 2401

b. RFC 2402

c. RFC 2406

d. RFC 2408

2. Which of the following documents provides the description of a packet encryption extension to IPv4 and IPv6

a. RFC 2401

b. RFC 2402

c. RFC 2406

d. RFC 2408

3. IPv6 header has a fixed size of

a. 40 octets

b. 80 octets

c. 20 octets

d. 160 octets

4. Addresses and exploit applications that use authentication based on IP address is called

a. Packet sniffing

b. IP Spoofing

c. Eaves dropping

d. Modification

5. A process by which packets from one network are broken into smaller pieces to be transmitted on another network is know as

a. segmentation

b. bifurcation

c. fragmentation

d. segregation

6. IPv4 header has a minimum size of

a. 180 bits

b. 160 bits

c. 256 bits

d. 512 bits

7. The version field in the IPv4 header has a size of

a. 6 bits

b. 4 bits

c. 8 bits

d. 16 bits

8. The number of fields in the IPv4 and IPv6 headers respectively are

a. 12 & 8

b. 8 &12

c. 6 & 10

9. Which among the following functional areas is not encompassed by IP-level Security

a. Integrity

b. Authenticity

c. Confidentiality

d. Key Management

Unit-2

1. Which of the following algorithms are used by IPSec to provide per-packet authentication and data integrity

a. HMAC MD5

b. 3DES

c. AES
d. Digital signatures, based on RSA and DSA

2. Which among the following is carried in AH and ESP headers to enable the receiving system to select the Security associations under which a received packet will be processed

a. Security Parameters index

b. Security Protocol identifier

c. IP destination address

d. Network address

3. Masquerade is an attack on

a. Data retrieval
b. Authentication
c. Non-repudiation
d. Data access

4. IPSec is provided at the layer
a. Bel w transport Layer

b. Belowcomnetwork layer

c. At the application layer
d. At the physical layer

5. Which among the following indicates whether the Security

a. Security Parameters index
b. Security Protocol identifier
c. IP destination address
d. Network address

6. Which among the following mechanisms assures the receiver that the received packet was transmitted by authorized person
a. Confidentiality

b. Non-repudiation
c. Authentication
d. key management

7. Which among the following mechanisms assures the receiver that the messages are received as sent, with no duplication, insertion, modification, reordering or replays.

a. Confidentiality
b. Non-repudiation

c. Authentication
d. Integrity

8. Which among the following mechanisms prevents either

sender or receiver from denying a transmitted message

a. Confidentiality
b. Non-repudiation
c. Authentication
d. Integrity

Unit-3

1. Which of the following documents provides Specification of key management

c. IP payload and selected portions of IP Header
d. none of IP header and IP payload

2. AH in tunnel mode authenticates which of the following

a. inner IP header
b. inner IP payload
c. inner IP payload + IP Header

d. inner IP payload + inner IP Header+ selected portions of outer Ip header +outer IPv6 extension headers

3. Which of the following fields is not present in the

Authentication Header

a. sequence number

b. payload length
c. security parameters index
d. padding

4. The size of Security parameters index field in

Authentication Header is
a. 8 bits

b. 16 bits
c. 32 bits
d. 64 bits

5. The sequence number field in the IPSec Authentication Header is designed to thwart

which of the following attacks

a. Eaves dropping
b. Replay

c. Interruption

d. Modification

6. A 32-bit value used to generate the sequence number field in AH headers is

a. Sequence counter overflow

b. Sequence number counter

c. Anti replay window

d. AH information

7. Anti-replay mechanism uses the window size of

a. w-1
b. w+1

c. 2w
d. w

Unit-4

1. Which among the following payloads defines a security transform to be used to secure the communications channel for the designated protocol

a. Transform payload
b. Proposal payload
c. Key exchange payload
d. Identification payload

2. Which among the following payloads transfers a public-key Certificate

a. Transform payload
b. Proposal payload
c. Certificate payload
d. Identification payload

3. Which among the following payloads contains either error or status information associated with the SA.

a. Transform payload
b. Proposal payload
c. Notification payload
d. Identification payload

4. What type of protocol is Oakley

a. Routing protocol
b. Transport Protocol
c. Key exchange protocol

5. Which of the following is a useful program or command procedure containing hidden code that, when invoked, performs some unwanted or harmful Function

a. Trap door
b. Logic bomb
c. Trojan Horses
d. Bacteria

6. Which of the following is not a network vehicle for spreading worms

a. Electronic mail facility
b. Remote execution capability
c. Routing facility
d. Remote login capability

7. Which of the following programs do not explicitly damage any files but reproduce exponentially

a. Worms
b. Trojan horses
c. Bacteria
d. Trap door

Unit-5

1. Which among the following is a group of internet computers that are set up, without the owner's knowledge ,to forward transmission to other computers on the internet

a. Zombie army

b. Rojan

c. RIC

d. RATs

2. Which is a program that lets anyone hold line keyboard conversation wth people or computer around the world

a. RATs

b. Root kits

c. Worms

d. IRC

3. A way of protecting password file is through

a. Access control

b. Assessment control

c. Check method

d. Nonrepudiation

4. Line tapping can be countered using

a. Antivirus software

b. Spyware

c. Link encryption techniques

d. Access control

5. What do you mean by pishing?

a. Bogus email

b. Viruses

c. RATs

d. Worms

6. Which of the following bypasses restrictions on access

a. Worm

b. Insect

c. Trojan horse

d. Bacteria

7. the front line of defense against intruders is

a. Encryption system

b. Password system

c. Antivirus system

d. Spy ware

8. Typically, salt value in UNIX password scheme is related to which parameter

a. Password

b.Time

c.User id

Unit-6

1. Which is a virus that mutates with every infection

a. Memory-resident virus

b. Parasitic virus

c. Polymorphic virus

d. Stealth Virus

2. Which portion of the virus creates a random encryption key to encrypt the remainder of the virus.

a. Mutation engine

b. Conversion engine

c. Generation engine

d. Keying engine

3. In which among the following phases of a virus, is a virus idle and will Eventually be activated by some event

a. Dormant phase

b. Propagation Phase

c. Triggering Phase

4. AH in tunnel mode authenticates which of the following

a. inner IP header

b. inner IP payload

c. inner IP payload + IP Header

d. inner IP payload + inner IP Header+ selected portions of outer Ip header +outer IPv6 extension headers

5. Which of the following fields is not present in the Authentication Header

a. sequence number

b. payload length

c. security parameters index

d. padding

6. The size of Security parameters index field in

Authentication Header is

a. 8 bits

b. 16 bits

c. 32 bits

d. 64 bits

7. The sequence number field in the IPSec Authentication

Header is designed to thwart which of the following attacks

a. Eaves dropping

b. Replay

c. Interruption

d. Modification

Unit-7

1. For Tunnel Mode AH, where is Authentication Header inserted

a. After original IP header & before IP payload

b. After original IP header & before new outer IP header

c. Before new outer IP header & before original IP header

d. Between original IP header & new outer IP header

2. AH in transport mode authenticates which of the following

a. IP header only

b. IP payload only

c. After transport layer header & before ESP trailer

d. Before original IP header

3. ESP in transport mode encrypts and optionally authenticates which of the following

a. IP header

b. IP payload

c. Both IP header and payload

d. None of IP header and payload

4. In tunnel mode ESP, where is the ESP header placed

a. After original IP header

b. prefixed to the packet

c. suffixed to the packet

d. before new IP header

5. The extension header that follows the main IP header for encryption is known as the

a. Encapsulating Security Payload header

b. authentication header

c. encryption header

d. auxiliary header

6. Which of the following terms refers to applying more than

one security protocol to the same IP packet, without invoking tunneling

a. Transport Adjacency

b. Iterated tunneling

c. Multiple protocols

d. Transport coherence

7. Which of the following defines payloads for exchanging key

generation and authentication data.

a. UDP

b. HTTP

c. ISAKMP

d. TCP

Unit-8

1. Which of the following is a useful program or command procedure containing hidden code that, when invoked, performs some unwanted or harmful function

a. Trap door

b. Logic bomb

c. Trojan Horses

d. Bacteria

2. Which of the following is not a network vehicle for spreading worms

a. Electronic mail facility

b. Remote execution capability

c. Routing facility

d. Remote login capability

3. Which of the following programs do not explicitly damage any files but reproduce exponentially

a. Worms

b. Trojan horses

c. Bacteria

d. Trap door

4. Who among the following is an individual who is not authorized to use the computer and who penetrates a system access controls to exploit a legitimate user account.

a. Masquerader

b. Misfeasor

c. Clandestine user

d. Casual user

5. Who among the following is an individual who accesses data, programs, or resources for which such access is not authorized

a. Masquerader

b. Misfeasor

c. Clandestine user

6. Who among the following is an individual who seizes

supervisory control of the system

and uses this control to evade auditing and access controls.

a. Masquerader

b. Misfeasor

c. Clandestine user

d. Casual user

20.REFRENCES:

R1: "Fundamentals of Network Security" by Eric Maiwald, Dreamtech Press.

R2: "Network Security–Private Communication in a Public World" by Charlie Kaufman, Radia

Perlman and Mike Spenciner, Pearson/PHI.

R3: "Cryptography and Network Security", Third edition, Stallings, PHI/Pearson.

R4: "Principles of Information Security",Whitman, Thomsan,.

R5: "Network Security: The Complete reference",Robert Bragg, Mark Rhodes,, TMH.

R6: "Introduction to Cryptography",Buchmann, Springer. WEBSITES

JOURNALS

J1.International Journal of Security and Networks
J2.International Journal of Computer Science and Network Security
J3.International Journal of Network Security

WEBSITES

W1.http://www.slideshare.net/netlabacademy/network-security-notes
W2. http://www.nprcet.org/NETWORKSECURITY.pdf
W3. http://jfdm.host.cs.st-andrews.ac.uk/notes/netsec/

21.QUALITY CONTROL SHEETS

22.STUDENT LIST

ECE-4

