Question Paper
Cryptography, Computer Security + Disaster Recovery (MB3H2IT): October 2008

Section A : Basic Concepts (30 Marks)

- This section consists of questions with serial number 1 - 30.
- Answer all questions.
- Each question carries one mark.
- Maximum time for answering Section A is 30 Minutes.

1. Which of the following statements is/are **false** about the security service, "Confidentiality"? <Answer>

I. Confidentiality is the protection of transmitted data from active attacks.
II. The broadest service of confidentiality protects all user data transmitted between two users over a period of time.
III. The other aspect of confidentiality is the protection of traffic flow from analysis which requires an attacker that cannot able to observe the source and destination, frequency, length or other characteristics of the traffic on a communications facility.

(a) Only (I) above
(b) Only (II) above
(c) Both (I) and (II) above
(d) Both (I) and (III) above
(e) Both (II) and (III) above.

2. Which of the following statements is/are **true**? <Answer>

I. The process of attempting to discover the plaintext is known as cryptanalysis.
II. The strategy used by the cryptanalyst depends on the nature of the encryption scheme and the information available to the cryptanalyst.
III. If the cryptanalyst is able somehow to get the source system to insert into the system a message chosen by the analyst, then a chosen-plaintext attack is possible.

(a) Only (I) above
(b) Only (II) above
(c) Both (I) and (II) above
(d) Both (II) and (III) above
(e) All (I), (II) and (III) above.

3. Which of the following statements is/are **false** about the security service, "Authentication"? <Answer>

I. In the case of a single message such as warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from.
II. Authentication service must assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.
III. Authentication service prevents either sender or receiver from denying a transmitted message.

(a) Only (I) above
(b) Only (II) above
(c) Only (III) above
(d) Both (I) and (II) above
(e) Both (II) and (III) above.

4. Which of the following is **not** a type of Active attacks? <Answer>

(a) Masquerade
(b) Traffic analysis
(c) Replay
(d) Modification of messages
(e) Denial of service.

5. Which of the following statements is/are **false** about Active attacks? <Answer>

I. Active attacks involve some modification of the data stream or the creation of a false stream.
II. Active attacks are easy to prevent.

III. The goal of active attacks is to detect them and to recover from any disruption or delays caused by them.

(a) Only (I) above
(b) Only (II) above
(c) Only (III) above
(d) Both (I) and (III) above
(e) Both (II) and (III) above.

<Answer>

6. Which of the following statements is/are **true** in Network Access Security Model?

I. Information access threats intercept or modify data on behalf of users who should not have access to that data.
II. Gatekeeper function includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses and other similar attacks.
III. Service threats exploit service flaws in computers to inhibit use by legitimate users.

(a) Only (I) above
(b) Only (II) above
(c) Both (I) and (II) above
(d) Both (II) and (III) above
(e) All (I), (II) and (III) above.

<Answer>

7. Automatic Key Distribution for Connection-Oriented Protocol configuration consists of two elements namely, Key Distribution Center (KDC) and Front-End Processor (FEP).Which of the following statements is/are **false** about KDC?

I. The KDC determines which systems are allowed to communicate with each other.
II. When permission is granted for two systems to establish a connection, the KDC provides a one-time session key for that connection.
III. KDC performs end-to-end encryption and obtains session keys on behalf of its host or terminal.

(a) Only (I) above
(b) Only (II) above
(c) Only (III) above
(d) Both (II) and (III) above
(e) All (I), (II) and (III) above.

<Answer>

8. Which of the following statements is/are **false** about Ciphertext?

I. Ciphertext is the scrambled message produced as output.
II. Ciphertext depends on the plain text and the secret key.
III. For a given message two different keys will produce same ciphertext.

(a) Only (I) above
(b) Only (II) above
(c) Only (III) above
(d) Both (I) and (III) above
(e) Both (II) and (III) above.

<Answer>

9. Which of the following statements is/are **false** about X.509 Authentication Service?

I. X.509 defines a framework for the provision of authentication services by the X.500 directory to its users.
II. X.509 defines alternative authentication protocols based on the use of private-key certificates.
III. X.509 is an important standard because the certificate structure and authentication protocols defined are used in variety contexts.
IV. X.509 standard dictates the use of a specific algorithm.

(a) Only (I) above
(b) Only (III) above
(c) Only (IV) above
(d) Both (II) and (IV) above
(e) Both (III) and (IV) above.

<Answer>

10. Which of the following is **not** an ingredient of Public-key encryption scheme?

(a) Plaintext

(b) Encryption algorithm
(c) Public and Private key
(d) Ciphertext
(e) Certification Authority.

11. Kerberos Version 4 was developed for use within the project Athena environment and accordingly did not fully address the need to be of general purpose and this led to several environmental shortcomings. Which of the following relates to the environmental short comings of Kerberos Version 4? <Answer>

I. Version 4 requires the use of Internet Protocol (IP) addresses. Other address types such as ISO network address are not accommodated.
II. In version 4, message byte ordering technique follows established conventions.
III. Lifetime values in version 4 are encoded in an 8-bit quantity in units of five minutes.

(a) Only (I) above
(b) Only (II) above
(c) Only (III) above
(d) Both (I) and (II) above
(e) Both (I) and (III) above.

12. In Kerberos Version 4 apart from the environmental limitations, there are technical deficiencies. Most of these deficiencies were documented and version 5 attempts to address these technical deficiencies. Which of the following relates to the technical deficiencies of Kerberos version 4? <Answer>

I. In version 4, the tickets provided to clients are encrypted twice.
II. Encryption in version 4 makes use of a nonstandard mode of Data Encryption Standard (DES) known as Propagating Cipher Block Chaining (PCBC).
III. In version 4, the Session key is used only by the server to protect messages passed during that session.

(a) Only (I) above
(b) Only (II) above
(c) Only (III) above
(d) Both (I) and (II) above
(e) Both (II) and (III) above.

13. The capacity of message digest length in Secure Hash Algorithm (SHA-1) is <Answer>

(a) 128 bits
(b) 256 bits
(c) 160 bits
(d) 512 bits
(e) 1,024 bits.

14. In Pretty Good Privacy (PGP), which of the following algorithms is used for e-mail compatibility function? <Answer>

(a) DSS algorithm
(b) Radix-64 conversion algorithm
(c) ZIP algorithm
(d) RSA algorithm
(e) Diffie-Hellman algorithm.

15. Which of the following Internet Protocol Security (IPSec) documents gives the specification of key management capabilities? <Answer>

(a) RFC 2408
(b) RFC 1636
(c) RFC 2406
(d) RFC 2402
(e) RFC 2401.

16. In each Internet Protocol Security (IPSec) implementation, there is a nominal Security Association Database that defines the parameters associated with each Security Association (SA). Which of the following is **not** a parameter that defines the SA? <Answer>

(a) Sequence Number Counter
(b) Sequence Counter Overflow
(c) Anti-Replay Window
(d) Source IP Address
(e) AH Information.

17. Which of the following is **not** a web security threat of Integrity Service? <Answer>

(a) Modification of user data
(b) Trojan horse browser
(c) Data forgery
(d) Modification of memory
(e) Modification of message traffic in transit.

18. Which of the following is **not** a parameter that defines Secure Socket Layer (SSL) Session state? <Answer>

(a) Initialization vector
(b) Session identifier
(c) Peer certificate
(d) Compression method
(e) Cipher spec.

19. The final step of Secure Socket Layer (SSL) record protocol processing is to prepend a header with some fields. Which of the following represents the capacity of Content Type field? <Answer>

(a) 8 bits
(b) 12 bits
(c) 16 bits
(d) 24 bits
(e) 32 bits.

20. In payment processing, which of the following Secure Electronic Transaction (SET) type allows the merchant to request payment from the payment gateway? <Answer>

(a) Payment authorization
(b) Payment capture
(c) Payment gateway certificate request
(d) Merchant registration
(e) Capture reversal.

21. A fundamental tool for intrusion detection is the audit record. Which of the following statements is/are **true** about the plans used in audit records? <Answer>

I. Advantage of using native audit records is that no additional collection software is needed.
II. Disadvantage of native audit records is, they may not contain the needed information or may not contain it in the convenient form.
III. Advantage of detection-specific audit records is that it could not be made vendor independent and ported to a variety of systems.

(a) Only (I) above
(b) Only (II) above
(c) Only (III) above
(d) Both (I) and (II) above
(e) Both (II) and (III) above.

22. In statistical anomaly intrusion detection, various approaches are considered for performing various tests to determine whether current activity fits with acceptable limits. Which of the following approach is based on a judgment of what is considered abnormal, rather than an automated analysis of past audit records? <Answer>

(a) Mean and standard deviation
(b) Multivariate model
(c) Markov process model
(d) Time series model
(e) Operational model.

23. Rule-based intrusion detection involves an attempt to define a set of rules that can be used to decide that the given behavior is of an intruder. Which of the following statements is/are **true** about Rule-based intrusion detection? <Answer>

I. For Rule-based anomaly detection, rules are developed to detect deviation from previous usage patterns.
II. Rule-based penetration identification is an expert system approach that searches for suspicious behavior.

III. With the rule-based anomaly detection approach, historical audit records are analyzed to identify usage patterns and to generate automatically rules that describe those patterns.

(a) Only (I) above
(b) Only (II) above
(c) Both (I) and (II) above
(d) Both (II) and (III) above
(e) All (I), (II) and (III) above.

24. Which of the following statements is/are **false** about Network worms? <Answer>

I. Network worm programs use network connections to spread from system to system.
II. Once active within a system, a network worm can behave as a computer virus or bacteria.
III. Network worms are easy to counter.

(a) Only (II) above
(b) Only (III) above
(c) Both (I) and (II) above
(d) Both (I) and (III) above
(e) Both (II) and (III) above.

25. Which of the following is a type of virus that is explicitly designed to hide itself from detection by antivirus software? <Answer>

(a) Parasitic virus
(b) Memory-resident virus
(c) Boot sector virus
(d) Stealth virus
(e) Polymorphic virus.

26. In network security, which of the following statements is/are **false** about Bastion Host? <Answer>

I. A bastion host is a system identified by the firewall administrator as a critical strong point in the network security.
II. Each proxy is dependent of other proxies on the bastion host.
III. The bastion host hardware platform executes a secure version of its operating system, making it a trusted system.

(a) Only (I) above
(b) Only (II) above
(c) Only (III) above
(d) Both (II) and (III) above
(e) All (I), (II) and (III) above.

27. Which of the following statements is/are **true** about the advantages of Screened Subnet Firewall Configuration? <Answer>

I. Screened subnet firewall configuration offers three levels of defense to thwart intruders.
II. In Screened subnet firewall configuration the outside router advertises only the existence of the screened subnet to the Internet.
III. In Screened subnet firewall configuration the inside router advertises only the existence of the screened subnet to the internal network; therefore, the systems on the inside network cannot construct direct routes to the internet.

(a) Only (I) above
(b) Only (II) above
(c) Only (III) above
(d) Both (I) and (III) above
(e) All (I), (II) and (III) above.

28. In Data Access Control, which of the following statements is/are **true** about the basic elements of Access matrix model? <Answer>

I. “Subject” is an entity capable of accessing objects.
II. “Object” is anything to which access is controlled.
III. “Access right” is the way in which an object is accessed by a subject.

(a) Only (I) above
(b) Only (II) above
(c) Only (III) above
(d) Both (II) and (III) above
(e) All (I), (II) and (III) above.

29. Which of the following statements is/are **false** about Polymorphic Virus? <Answer>

I. A polymorphic virus creates copies during replication that are functionally equivalent but have distinctly different bit patterns.
II. Polymorphic virus is explicitly designed to hide itself from detection by antivirus software.
III. Polymorphic virus mutates with every infection, making detection by the "signature" of the virus impossible.

(a) Only (I) above
(b) Only (II) above
(c) Only (III) above
(d) Both (II) and (III) above
(e) All (I), (II) and (III) above.

30. In Secure Socket Layer (SSL) handshake protocol, which of the following message type has the parameter "Hash value"? <Answer>

(a) hello_request
(b) certificate
(c) server_done
(d) finished
(e) certificate_verify.

END OF SECTION A

Section B : Problems/Caselet (50 Marks)

er.

Explain the steps involved in HMAC algorithm with a neat sketch.

Explain the DES algorithm with a neat sketch.

Caselet

Read the caselet carefully and answer the following questions:

With respect to the caselet, do you think spending too much money for d
organization? Justify your answer.

Explain the different possible software threats faced by the banks.

If you are in the position of an IT manager, what are the security measures
Web?

Discuss the design goals of a firewall.

Web 2.0 term has changed the entire aspect of users involved with the mo
features. There is a whole rash of new devices coming out to enable people t
and smart phones. While it took a decade or more to gain a level of hygiene
and generally there is a feeling that developers haven't paid enough attent
10,000 samples a day and they are growing in sophistication as organized
purposes. The Potential from a criminal perspective has expanded dramatica
more alarming. Contents in the Web2.0 world can be produced by any ind

social networking sites. The browser is now the operating system providin telephony and any other number of services. The security perimeter is advancement had created more sharp programmers which can amazingly crea as hackers. IT spent years of learning how to best authenticate users in comp now authenticating software to software or computers to computers. The fire the Internet to establish a controlled link and to erect an outer security wall c the premises network from Internet based attacks and to provide a single chok

In the banking world, allowing a data breach might be the surest way to end caused by Web2.0 has forced many banks to take a harder line allowing emp their jobs. Every device in the network is locked down, whether it's a compute

Any device that can move information out of the corporation is pretty transmission that goes out of the organization are expected to know, when a who has access to it.

Too much security can harm the bottom line and annoy users. It is a balancin Banks can protect money but its new idea for a bank to protect vast amou dollars on security but it does not generate any new revenue. Spending all th should be in a position to figure out what level of risk they are willing to toler

END OF CASELET

END OF SECTION B

Section C : Applied Theory (20 Marks)

ons with serial number 7 - 8.

ch question.
0 minutes on Section C.

What are the technical deficiencies of Kerberos Version 4? Give a summary Message Exchanges.

Explain in detail about the antivirus technique, "Digital Immune System" with

END OF SECTION C

END OF QUESTION PAPER

Suggested Answers
Cryptography, Computer Security + Disaster Recovery (MB3H2IT): October 2008

Section A : Basic Concepts

Answer	Reason	
1. A	Confidentiality is the protection of transmitted data from passive attacks.	< TOP >
2. E	The process of attempting to discover the plaintext is known as cryptanalysis. The strategy used by the cryptanalyst depends on the nature of the encryption scheme and the information available to the cryptanalyst. If the cryptanalyst is able somehow to get the source system to insert into the system a message chosen by the analyst, then a chosen-plaintext attack is possible.	< TOP >
3. C	Nonrepudiation prevents either sender or receiver from denying a transmitted message.	< TOP >
4. B	Traffic analysis is a type of Passive Attacks.	< TOP >
5. B	Active attacks are difficult to prevent.	< TOP >
6. E	Information access threats intercept or modify data on behalf of users who should not have access to that data. Gatekeeper function includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses and other similar attacks. Service threats exploit service flaws in computers to inhibit use by legitimate users.	< TOP >
7. C	The front-end processor performs end-to-end encryption and obtains session keys on behalf of its host or terminal.	< TOP >
8. C	For a given message, two different keys will produce two different ciphertexts.	< TOP >
9. C	X.509 standard does not dictate the use of a specific algorithm.	< TOP >
10E	Public-Key Encryption scheme has six ingredients given as Plaintext, Encryption algorithm, Public and private key, Ciphertext and Decryption algorithm. Certificate Authority (CA) is the third party agency for Digital Certificates.	< TOP >
11E	Version 4 requires the use of Internet Protocol (IP) addresses. Other address types such as ISO network address are not accommodated. Lifetime values in version 4 are encoded in an 8-bit quantity in units of five minutes. Message byte ordering technique does not follow established conventions.	< TOP >
12.	In version 4 the tickets provided to clients are encrypted twice. Encryption in version 4 makes use of a nonstandard mode of Data Encryption Standard (DES) known as Propagating Cipher Block Chaining (PCBC). In version 4 the Session key may subsequently be used by the client and the server to protect messages passed during that session.	< TOP >
13C	SHA-1 produces an output of 160-bit message digest.	< TOP >
14B	In PGP, Radix-64 conversion algorithm is used for e-mail compatibility function.	< TOP >
15A	IPSec document, RFC 2408 is the specification of key management capabilities. RFC 2401 gives Overview of Security Architecture, RFC 2402 gives description of packet Authentication extension to IPV4 and IPv6, RFC 2406 gives the Description of packet Encryption extension IPV4 and IPV6 and RFC 1636 is about the Security in the Internet Architecture.	< TOP >
16D	The following are the parameters that define Security Associations. Sequence Number Counter,. Sequence Counter Overflow, Anti-Replay Window, AH Information, ESP Information, Life time of this security Association, IPSec protocol mode, Path MTU. Source IP Address is one of the selectors that determine a Security Policy Database (SPD) entry.	
17C	For the Integrity factor these are the threats: Modification of user data, Trojan horse browser, Modification of memory, Modification of message traffic in transit. Data	< TOP >

forgery is a Threat related with Authentication on the Web.

18A A Session State is defined by the following parameters: Session identifier, Peer certificate, Compression method, Cipher spec, Master secret and IS Resumable. < TOP >

Initialization Vector is a parameter that defines Connection State.

19A Capacity of Content type field is 8 bits. < TOP >

20B Payment capture allows the merchant to request payment from the payment gateway. < TOP >

21D Advantage of using native audit records is that no additional collection software is needed. Disadvantage of native audit records is, they may not contain the needed information or may not contain it in the convenient form. Advantage of detection specific audit records is that it could be made vendor independent and ported to a variety of systems. < TOP >

22E An Operational model is based on a judgment of what is considered abnormal, rather than an automated analysis of past audit records. < TOP >

23E For Rule-based anomaly detection, rules are developed to detect deviation from previous usage patterns.Rule-based penetration identification is an expert system approach that searches for suspicious behavior.With the rule-based approach, historical audit records are analyzed to identify usage patterns and to generate automatically rules that describe those patterns. < TOP >

24B Network worms are difficult to counter. < TOP >

25D Stealth Virus is a form of virus explicitly designed to hide itself from detection by antivirus software. < TOP >

26B A bastion host is a system identified by the firewall administrator as a critical strong point in the network security. The bastion host hardware platform executes a secure version of its operating system, making it a trusted system. Each proxy is independent of other proxies on the bastion host. < TOP >

27E Screened subnet firewall configuration offers three levels of defense to thwart intruders. The outside router advertises only the existence of the screened subnet to the Internet. The inside router advertises only the existence of the screened subnet to the internal network; therefore, the systems on the inside network cannot construct direct routes to the internet. < TOP >

28E “Subject” is an entity capable of accessing objects. < TOP >

“Object” is anything to which access is controlled.

“Access right” is the way in which an object is accessed by a subject.

29B Stealth virus is explicitly designed to hide itself from detection by antivirus software. < TOP >

30D In Secure Socket Layer Handshake protocol, message type “finished” has the parameter “Hash value”. < TOP >

Section B : Problems/Caselet

1. HMAC Algorithm < TOP >

The following illustrates the overall operation of HMAC. We define the following terms:

H = embedded hash function (e.g., SHA-1)

M = message input to HMAC (including the padding specified in the embedded hash function)

Yi = i th block of M, $0 \leq i \leq (L - 1)$

L = number of blocks in M

b = number of bits in a block

n = length of hash code produced by embedded hash function

K = secret key; if key length is greater than b, the key is input to the hash function to produce an n-bit key; recommended length is $\geq$ n

K^+ = K padded with zeros on the left so that the result is b bits in length

ipad = 00110110 (36 in hexadecimal) repeated b/8 times

opad = 01011100 (5C in hexadecimal) repeated b/8 times

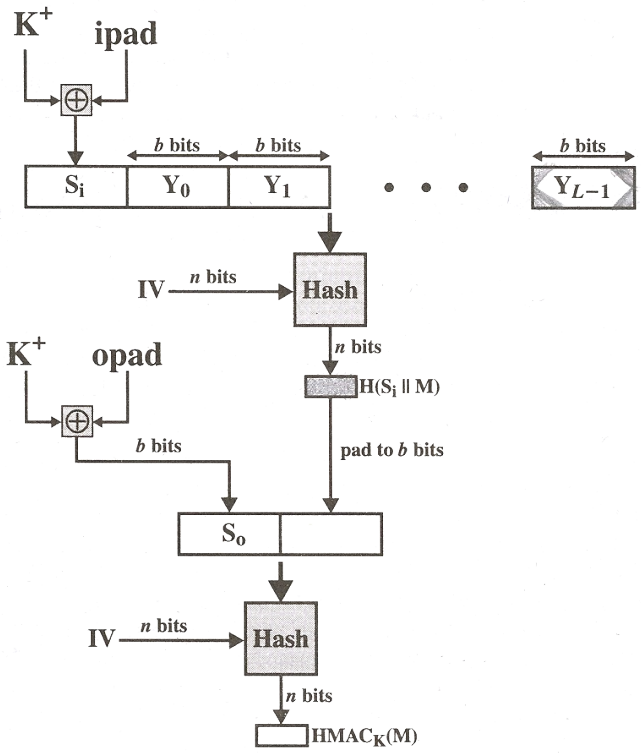


Fig: HMAC Structure

Then HMAC can be expressed as follows:

$HMAC_K = H[(K \oplus opad) \| H[(K \oplus ipad) \| M]]$

In words,

i. Append zeros to the left end of K to create a b-bit string K^+ (e.g., if K is of length 160 bits and b = 512, then K will be appended with 44 zero bytes 0x00).

ii. XOR (bitwise exclusive-OR) K^+ with ipad to produce the b-bit block S_i

iii. Append M to S_i.

iv. Apply H to the stream generated in step 3.

v. XOR K^+ with opad to produce the b-bit block S_o.

vi. Append the hash result from step 4 to S_o.

vii. Apply H to the stream generated in step 6 and output the result.

Note that the XOR with ipad results in flipping one-half of the bits of K. Similarly, the XOR with opad results in flipping one-half of the bits of K, but a different set of bits. In effect, by passing S_i and S_o through the hash

algorithm, two keys from K are pseudo randomly generated.

HMAC should execute in approximately the same time as the embedded hash function for long messages. HMAC adds three executions of the basic hash function (for S_i, S_o, and the block produced from the inner hash).

HMAC Design Objectives

RFC 2104 lists the following design objectives for HMAC:

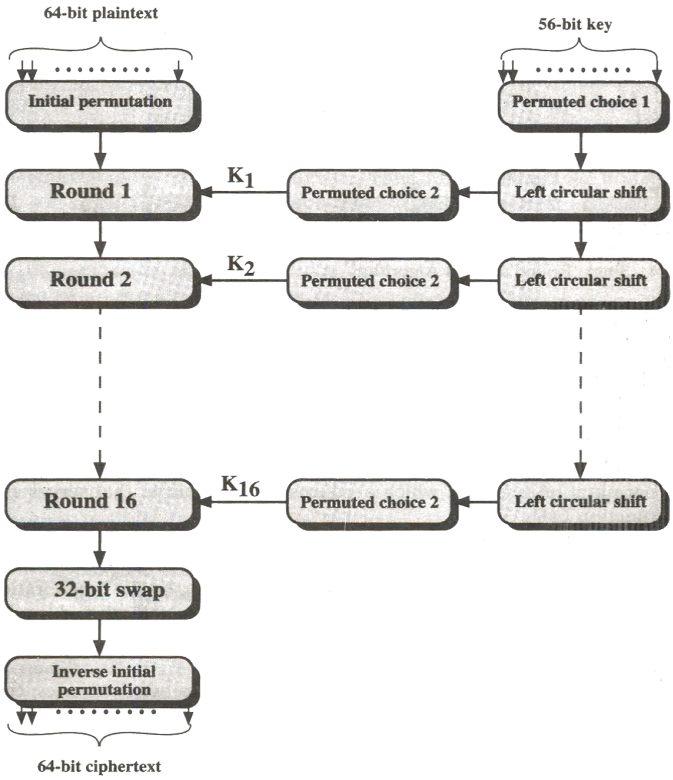
- To use, without modifications, available hash functions (in particular, hash functions that perform well in software, and for which code is freely and widely available)
- To allow for easy replaceability of the embedded hash function in case faster or more secure hash functions are found or required
- To preserve the original performance of the hash function without incurring a significant degradation
- To use and handle keys in a simple way
- To have a well-understood cryptographic analysis of the strength of the authentication mechanism based on reasonable assumptions on the embedded hash function

The first two objectives are important to the acceptability of HMAC. HMAC treats the hash function as a "black box." This has two benefits. First, an existing implementation of a hash function can be used as a module in implementing HMAC. In this way, the bulk of the HMAC code is prepackaged and ready to use without modification. Second, if it is ever desired to replace a given hash function in an HMAC implementation, all that is required is to remove the existing hash function module and drop in the new module. This could be done if a faster hash function were desired. More important, if the security of the embedded hash function were compromised, the security of HMAC could be retained simply by replacing the embedded hash function with a more secure one.

The last design objective in the preceding list is, in fact, the main advantage of HMAC over other proposed hash-based schemes. HMAC can be proven secure provided that the embedded hash function has some reasonable cryptographic strengths.

2. The overall scheme for DES encryption is illustrated in the following figure 1. The plain-text is 64 bits in length and the key is 56 bits in length; longer plaintext amounts are processed in 64-bit blocks. < TOP >

Figure 1: General Depiction of DES Encryption Algorithm



The left-hand side of the figure1 shows that the processing of the plaintext proceeds in three phases. First, the 64-bit plaintext passes through an Initial Permutation (IP) that rearranges the bits to produce the permuted input. This is followed by a phase consisting of 16 iterations of the same function. The output of the last (sixteenth) iteration consists of 64 bits that are a function of the input plaintext and the key. The left and right halves of the output are

swapped to produce the preoutput. Finally, the preoutput is passed through a permutation (IP^{-1}) that is the inverse of the initial permutation function, to produce the 64-bit ciphertext.

The right-hand portion of figure 1 shows the way in which the 56-bit key is used. Initially, the key is passed through a permutation function. Then, for each of the 16 iterations, a subkey (K_i) is produced by the combination of a left circular shift and a permutation. The permutation function is the same for each iteration, but a different subkey is produced because of the repeated shifting of the key bits.

Figure 2: Single Round of DES Algorithm

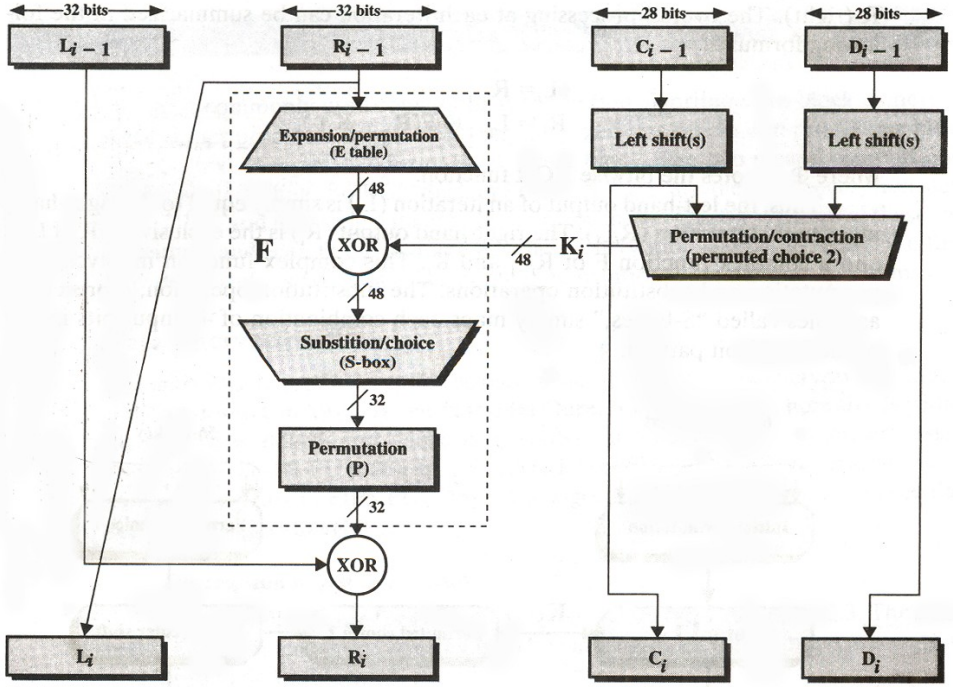


Figure 2 examines more closely the algorithm for a single iteration. The 64-bit permuted input passes through 16 iterations, producing an intermediate 64-bit value at the conclusion of each iteration. The left and right halves of each 64-bit intermediate value are treated as separate 32-bit quantities, labeled L (left) and R (right). The overall processing at each iteration can be summarized in the following formulas:

$L_i = R_{i-1}$

$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

Where $\oplus$ denotes the bitwise XOR function

Thus, the left-hand output of iteration (L_i) is simply equal to the right-hand input to that iteration (R_{i-1}). The right-hand output (R_i) is the exclusive OR of L_{i-1} and a complex function F of R_{i-1} and K_i. This complex function involves both permutation and substitution operations. The substitution operation, represented as tables called "S-boxes," simply maps each combination of 48 input bits into a particular 32-bit pattern.

In the figure 1 we see that the 56-bit key used as input to the algorithm is first subjected to a permutation. The resulting 56-bit key is then treated as two 28-bit quantities, labeled C_0 and D_0. At each iteration, C and D are separately subjected to a circular left shift, or rotation, of 1 or 2 bits. These shifted values serve as input to the next iteration. They also serve as input to another permutation function, which produces a 48-bit output that serves as input to the function F (R_{i-1}, K_i).

The process of decryption with DES is essentially the same as the encryption process. The rule is as follows: Use the ciphertext as input to the DES algorithm, but use the keys K_i in reverse order. That is, use K_{16} on the first iteration, K_{15} on the second iteration and so on until K_1 is used on the sixteenth and last iteration.

3. NO. Spending too much money without a proper perspective about a Security solution is an Unwise proposition. First we have to assess about the areas of vulnerabilities in the Information Technology which is prone to security threats. After analyzing the vulnerabilities, we have to work out what are the effective solutions which are practical to the assessed Vulnerabilities. After working out this we have to see the Financial constraints of Implementing the worked out solution. < TOP >

If the Security solution which has been worked out is found to be feasible in all sense, we can accept it and give it for approval.

4. Malicious programs as well as Viruses are the threats to the software security of the bank. The most notorious Virus named Trojan horse is the kind of virus which proliferates rapidly through Internet and many antiviruses cannot able to block its mass proliferation in the web. Another kind of threat is from Worms which spread from < TOP >

system to system. Once active within a system, a network worm can behave as a computer virus or bacteria or it could implant Trojan horse programs or perform any number of disruptive or destructive actions. Another important threat is Network security threats like hacking of the websites and defacing the sites. Mostly in bank websites hackers do steal the credit card IDs as well as the information which are vital to banks which usually happens in Online banking.

5. As an IT manger in the Banking Organization, He/She should first workout where are the vulnerabilities of Risk relating to the software security and have to see what are the cost effective measures to be implemented from my part as an IT manager. Implementation of Firewall is an effective idea to maintain the Confidentiality of some of the matters. Periodically the IT manager should have to conduct the Audit relating to the Security aspects and give wise directions to the subordinates in maintaining the Security aspects in the Bank. < TOP >

6. The design goals for a firewall can be characterized as follows: < TOP >

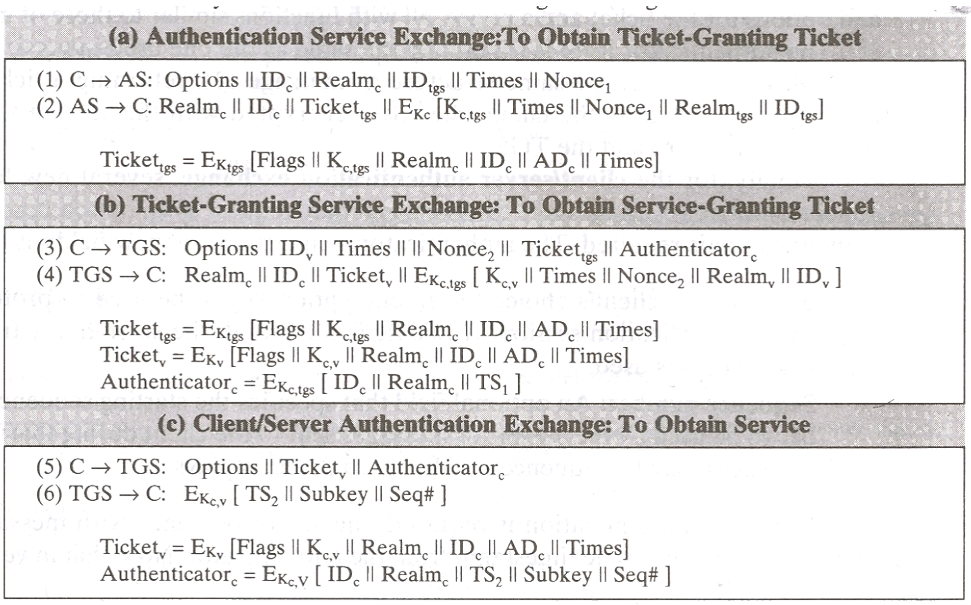
1. All traffic from inside to outside, and vice versa must pass through the firewall. This is achieved by physically blocking all access to the local network except via the firewall.
2. Only authorized traffic, as defined by the local security policy will be allowed to pass.
3. The firewall itself is immune to penetration. This implies the use of a trusted system with a secure operating system.

Section C: Applied Theory

7. The technical deficiencies of version 4 addressed in Version 5. < TOP >

1. Double encryption: The tickets provided to clients are encrypted twice, once with the secret key of the target server and then again with a secret key known to the client. The second encryption is not necessary and is computationally wasteful.
2. PCBC encryption: Encryption in version 4 makes use of a nonstandard mode of DES known as propagating cipher block chaining (PCBC). It has been demonstrated that this mode is vulnerable to an attack involving the interchange of cipher text blocks. PCBC was intended to provide an integrity check as part of the encryption operation. Version 5 provides explicit integrity mechanisms, allowing the standard CBC mode to be used for encryption.
3. Session keys: Each ticket includes a session key that is used by the client to encrypt the authenticator sent to the service associated with that ticket. In addition, the session key may subsequently be used by the client and the server to protect messages passed during that session. However, because the same ticket may be used repeatedly to gain service from a particular server, there is the risk that an opponent will replay messages from an old session to the client or the server. In version 5, it is possible for a client and server to negotiate a sub session key, which is to be used only for that one connection. A new access by the client would result in the use of a new sub session key.
4. Password attacks: Both versions are vulnerable to a password attack. The message from the AS to the client includes material encrypted with a key based on the client's password. An opponent can capture this message and attempt to decrypt it by trying various passwords. If the result of a test decryption is of the proper form, then the opponent has discovered the client's password and may subsequently use it to gain authentication credentials from Kerberos. Version 5 does provide a mechanism known as preauthentication, which should make password attacks more difficult, but it does not prevent them.

Summary of Kerberos Version 5 Message Exchanges :



First, consider the authentication service exchange. Message (1) is a client request for a ticket-granting ticket. As before, it includes the ID of the user and the TGS. The following new elements are added:

Realm: Indicates realm of user

Options: Used to request that certain flags be set in the returned ticket

Times: Used by the client to request the following time settings in the ticket:

– from: the desired start time for the requested ticket

– a till: the requested expiration time for the requested ticket

  – time: requested renew-till time

- Nonce: A random value to be repeated in message (2) to assure that the response is fresh and has not been replayed by an opponent. Message (2) returns a ticket-granting ticket, identifying information for the client, and a block encrypted using the encryption key based on the user's password. This block includes the session key to be used between the client and the TGS, times specified in message (1), the nonce from message (1), and TGS identifying information. The ticket itself includes the session key, identifying information for the client, the requested time values, and flags that reflect the status of this ticket and the requested options. These flags introduce significant new functionality to version 5.

The ticket-granting service exchange for versions 4 and 5. The message (3) for both versions includes an authenticator, a ticket, and the name of the requested service. In addition, version 5 includes requested times and options for the ticket and a nonce, all with functions similar to those of message (1). The authenticator itself is essentially the same as the one used in version 4.

Message (4) has the same structure as message (2), returning a ticket plus information needed by the client, the latter encrypted with the session key now shared by the client and the TGS.

Finally, for the client/server authentication exchange, several new features appear in version 5. In message (5), the client may request as an option that mutual authentication is required. The authenticator includes several new fields as follows:

Sub key: The client's choice for an encryption key to be used to protect this specific application session. If this field is omitted, the session key from the ticket (Kcv) is used.

Sequence number: An optional field that specifies the starting sequence number to be used by the server for messages sent to the client during this session. Messages may be sequence

numbered to detect replays.

If mutual authentication is required, the server responds with message (6). This message includes the timestamp from the authenticator. Note that in version 4, the timestamp was incremented by one. This is not necessary in version 5 because the nature of the format of messages is such that it is not possible for an opponent to create message (6) without knowledge of the appropriate encryption keys. The sub key field, if present, overrides the sub key field, if present, in message (5). The optional sequence number field specifies the starting sequence number to be used by the client.

8. The digital immune system is a comprehensive approach to virus protection developed by IBM. The motivation for this development has been the rising threat of Internet-based virus propagation. We first say a few words about this threat and then summarize IBM's approach. < TOP >

Traditionally, the virus threat is characterized by the relatively slow spread of new viruses and new mutations. Antivirus software is typically updated on a monthly basis, and this has been sufficient to control the problem. Also traditionally the Internet played a comparatively small role in the spread of viruses. But as points out, two major trends in Internet technology will have an increasing impact on the rate of virus propagation in recent years:

Integrated mail systems: Systems such as Lotus Notes and Microsoft Outlook make it very simple to send anything to anyone and to work with objects that are received.

Mobile-program systems: Capabilities such as Java and ActiveX allow programs to move on their own from one system to another.

In response to the threat posed by these Internet-based capabilities, IBM has developed a prototype digital immune system. This system expands on the use of program emulation discussed in the preceding subsection and provides a general-purpose emulation and virus-detection system. The objective of this system is to provide rapid response time so that viruses can be stamped out almost as soon as they are introduced. When a new virus enters an organization, the immune system automatically captures it, analyzes it, adds detection and shielding for it, removes it, and passes information about that virus to systems running IBM Anti-Virus so that it can be detected before it is allowed to run elsewhere.

Figure illustrates the typical steps in digital immune system operation:

i. A monitoring program on each PC uses a variety of heuristics based on system behavior, suspicious changes to programs, or family signature to infer that a virus may be present. The monitoring program forwards a copy of any program thought to be infected to an administrative machine within the organization.

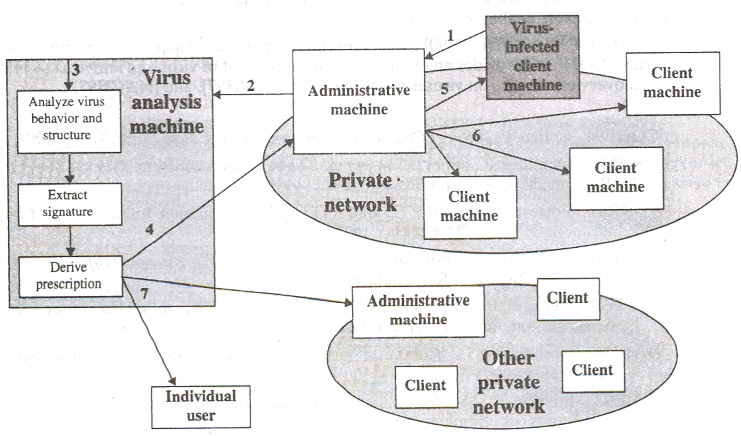


Figure: Digital Immune System

ii. The administrative machine encrypts the sample and sends it to a central virus analysis machine.

iii. This machine creates an environment in which the infected program can be safely run for analysis. Techniques used for this purpose include emulation, or the creation of a protected environment within which the suspect program can be executed and monitored. The virus analysis machine then produces a prescription for identifying and removing the virus.

iv. The resulting prescription is sent back to the administrative machine.

v. The administrative machine forwards the prescription to the infected client.
vi. The prescription is also forwarded to other clients in the organization.
vii. Subscribers around the world receive regular antivirus updates that protect them from the new virus.

The success of the digital immune system depends on the ability of the virus analysis machine to detect new and innovative virus strains. By constantly analyzing and monitoring the viruses found in the wild, it should be possible continually to update the digital immune software to keep up with the threat.

< TOP OF THE DOCUMENT >