MSDS 7349 Data and Network Security Exam 2 (Final Exam)

Shanqing Gu

Due Day: 08/06/2018

Q1- Q5 (each 8 points)
Answer each question fully and completely. Show your work and state your assumptions where appropriate.

Q1: Kerberos is an authentication service that is often used to allow a user to gain access to a computer that is connected to the network or to establish a secure communication channel. In one to two pages, explain how Kerberos works, explain why Kerberos is secure, and draw a figure that illustrates the steps involved to using Kerberos to authenticate two systems to one another while establishing a secure communication channel (where the secure communication channel uses a shared secret key). Be sure to explain each step in this symmetric session key establishment protocol.

Relying exclusively on symmetric encryption without use of public-key encryption, Kerberos provides a mutual authentication between networked users and resources. Briefly, user is provided a ticket that is issued by the Kerberos authentication server (AS), the user presents this ticket to the network for a service or application, and the service then examines the ticket to verify the identity of the user. Kerberos is the foundation for authentication in Microsoft Windows operating systems, and Internet Explorer and Mozilla Firefox have built-in support for Kerberos authentication to web servers.

(1) How Kerberos works?

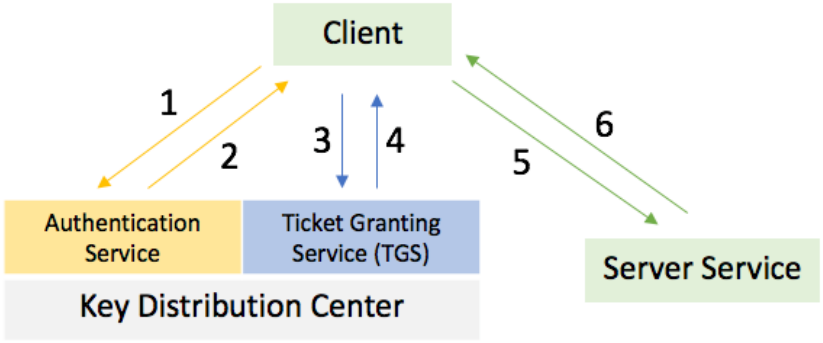
1) User logs on to workstation and requests service on host (once per user logon session)
2) AS verifies user's access rights in database, creates ticket-granting ticket and session key. Results are encrypted using key derived from user's password.
3) Workstation prompts user for password to decrypt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

(2) Why Kerberos is secure?

1) Kerberos is more secure than other authentication methods because it does not send plain text passwords over the network and instead uses encrypted tickets. The AS provides both the client and the TGS with s secret piece of information in a secure manner. Then the client can prove its identity to the TGS by revealing the secret information-again in a secure manner. An efficient way of accomplishing this is to use session key in Kerberos.
2) Kerberos's two-fold security ensures the service trusts the credentials in the service ticket, acknowledging the ticket could only be created by the KDC and the end-user must have been authenticated by the KDC in order to receive the ticket.
3) Because the end-user and server are mutually authenticated, Kerberos authentication prevents server attacks and malicious programs that try to impersonate the server to get the end-user's private information.
4) The Kerberos service ticket has a limited lifetime and the receiving service can store used tickets, thus preventing replay attacks.
5) Kerberos removes the need for administrators to manage separate passwords for multiple enterprise servers by making it possible for end-users to authenticate one time and then access additional applications or Websites without further prompting for a username and password.
6) Kerberos' ability to accurately identify end-users and servers allows programmers and administrators to provide authorization and auditing to further enhance the security of their networks.

(3) Configure a Key Distribution Center (KDC) for Kerberos authentication

KDC as a network service provides an AS to authenticate users and services, and a TGS issues tickets to access services. The following diagram is an overview of a Kerberos transaction:



1) A client logs on and sends a request to the authentication service and is authenticated.
2) The authentication service client's access right in database and responds with a ticket and session key. Results are encrypted using key derived from client's password.
3) The client requests a ticket for a specific server.
4) The TGS returns a response with the appropriate ticket for requested application server.

5) The client requests a service from server host, and workstation sends ticket and authenticator to host.
6) Host verifies that ticket and authenticator match, and then access grants access to service.

Q2: The Border Gateway Protocol (BGP) is used for routing packets between Internet Service Providers (ISPs). BGP routers from each ISP communicate with one another exchanging information such as the IP addresses that are serviced within the ISP. In one to two pages, explain how BGP operates, and explain how this operation may be exploited by an adversary to allow the adversary to cause all packets destined for a particular IP address that is not serviced within the ISP to flow through that ISP. Identify and discuss at least one news article published in either 2014 or 2015 or 2016 that discusses victims of this type of attack.

The Border Gateway Protocol (BGP, as defined in RFC 1163 and RFC 1267) is the complex routing protocol that allows independently operated networks (also called autonomous systems, AS) to inform each other about their reachability. Emphasizing on security and scalability, BGP routing information is usually exchanged between competing business entities in the form of internet service providers (ISPs) in an open and hostile environment (i.e. the public internet).

(1) How BGP operates?

BGP works with a network, an AS number that identifies user network, an IP prefix, a BGP router, a BGP interconnection. AS and IP prefixes are allocated by Regional Internet Registry (RIR), access to internet resources allocation by the WHOIS protocol.

With BGP, an operator uses update messages to announce its IP prefixes, and withdraw messages to remove its IP prefixes. There are three simples BGP rules: messages are forwarded to neighbors, after adding the ASN; only the shortest AS path is forwarded; and packets are sent to the most specific prefix. Each time, a BGP router advertises IP prefix to its neighbor. The newly received information is compared against the router's stored knowledge and updated to locally and all immediate neighbors when there is a better path to reach a certain network.

(2) How this operation may be exploited by an adversary to allow the adversary to cause all packets destined for a particular IP address that is not serviced within the ISP to flow through that ISP.

There are three ways in which attackers can potentially abuse BGP:

1). BGP route manipulation: A malicious device alters the content of the BGP table, preventing traffic from reaching the intended destination;

2). BGP route hijacking: A route device maliciously announces a victim's prefixes to reroute traffic to or through itself, which otherwise would not happen. Rerouting traffic can cause

instability in some networks with a sudden load increase. This allows attackers to access potentially unencrypted traffic to which they would otherwise not have access or use hijacked BGP to launch spam campaigns, bypassing IP blacklist mitigation;

3). BGP denial-of-service (DoS): A malicious device sends unexpected or undesirable BGP traffic to a victim, exhausting all resources and rendering the target system incapable of processing valid BGP traffic.

For over a decade, BGP hijacking and leak incidents have been a recurring threat to take control of a group of IP prefixes assigned to a potential victim. For instance, a BGP hijack caused a global YouTube outage in 2008 (https://securityintelligence.com/bgp-internet-routing-what-are-the-threats/).

(3) Identify and discuss at least one news article published in either 2014 or 2015 or 2016 that discusses victims of this type of attack

1). News article in 2014 for bitcoin theft:

In a 2014 attack analyzed by Dell SecureWorks, the hijackers targeted 51 networks from 19 ISPs in order to redirect miners to their own mining pools. The redirection technique tricked the pool's participants into continuing to devote their processors to bitcoins mining while allowing the hacker to keep the proceeds. In total, there were 22 hijacks that lasted around 30 seconds each and the hijacker was able to steal at least $83,000 worth of cryptocurrency stolen in the BGP attack over a two-month period (Reference: https://www.wired.com/2014/08/isp-bitcoin-theft/).

2). News article in 2016 for prefix hijacking done by an ISP toward Google's network prefixes (Reference: https://ieeexplore.ieee.org/document/7871109/)

Q3: The ACM Code of Ethics provides a strong ethical roadmap by which engineers and computer scientists may guide their careers and decisions when faced with any issue that may arise. Identify the five primary tenets of the ACM Code of Ethics that you believe would be used most often to guide one's career. For each of these, in 5-10 sentences explain why that tenet is likely to be used often.

From the ACM Code of Ethics and Professional Conduct (https://www.acm.org/code-of-ethics), there are five primary tenets of the ACM Code of Ethics that I believe would be used most often to guide one's career.

1. Avoid harm to others

Examples of harm include unjustified destruction or disclosure of information, and unjustified damage to property, reputation and the environment. These harms can bring significant and unjust consequences. To prevent harming others indirectly or unintentionally, computing professionals should follow generally accepted best practices unless there is a compelling ethical reason to do otherwise. In addition, a computing professional has the obligation to report any signs of system risks that must result in harm. Before reporting risks, a computing professional should carefully assess relevant aspects of the situation.

2. Be honest and trustworthy

   A computing professional should not make deliberately false or misleading claims, fabricating or falsifying data, offering or accepting bribes, and other dishonest conduct to violate the code. On the contrary, professionals should provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties and be transparent, honest and trustworthy.

   Computing professionals should be honest about their qualifications and limitations in their competence to complete a task, forthright about any circumstances that might lead to either real or perceived conflicts of interest or otherwise tend to undermine the independence of their judgment.

   Computing professionals should not misrepresent an organization's policies or procedures and speak on behalf of an organization unless authorized to do so.

3. Honor intellectual property rights and give proper credit

   Computing professionals should honor intellectual property and avoid the following examples of types of violations: misrepresentation of authorship, the origin or ownership of ideas or work; misappropriation of a commons, unauthorized use, copying, or derivative works, and counterfeiting. Contributing time and energy to help others in projects that help society illustrate a positive aspect of this imperative to make contributions to projects that are in the public domain, free or open source software.

4. Respect the privacy of others

   Computing professionals should become conversant in the various definitions and forms of privacy and understand the rights and responsibilities associated with the collection and use of personal information.

   Computing professionals should only use personal information for legitimate ends and without violating the rights of individuals and groups. This requires taking precautions to prevent re-identification of anonymized data or unauthorized data collection.

Computing professionals should establish transparent policies and procedures that allow individuals to understand what data is being collected and how it is being used, to give informed consent for automatic data collection, and to review, obtain, correct inaccuracies in, and delete their personal data.

5. Strive to achieve the highest quality in both the processes and product of professional work

   Computing professionals should insist on and support high quality work from themselves and from colleagues, respect the right of those involved to transparent communication about the project, and be cognizant of any serious negative consequences affecting any stakeholder that may result from poor quality work and resist inducements to neglect this responsibility.

Q4: In one to two pages, explain how a public key cipher is typically used to provide a digital signature and explain how a user is able to authenticate a signature to verify that it came from a known individual. Be sure to include a description of how the user is able to determine the identity of the individual to whom the public key in the public key cipher is associated. Illustrate how a digital signature is used within a commonly used network communication protocol or security service. Be sure to identify the protocol or service.

(1) How a public key cipher is typically used to provide a digital signature?

Public-key is a very appealing and exciting technology, embedding both encryption and digital signature. Public key involves asymmetric key pairs (a public key and a private key) for encryption and decryption, and digital signature is a mechanism by which a message is authenticated i.e. providing that a message is effectively coming from a given sender. Both encryption and digital signature can be combined, hence providing privacy and authentication.

Here is the example to explain digital signature and its verification with public key cipher: when Alice wants to digitally sign a message to Bob, she uses her private key to encrypt the message, and sends the message along with her public key as attached to the signed message. Since Alice's public-key is the only key that can decrypt that message, a successful decryption constitutes a digital signature verification, meaning that there is no doubt that it is Alice's private key that encrypted the message.

(2) How a user is able to authenticate a signature to verify that it came from a known individual?

Hashing technique is used for digital signature verification. Hashing produces a message digest that is a small and unique representation of the complete message. Hashing algorithms are a one-way encryption, i.e. it is impossible to derive the message from the digest. The main reasons for producing a message digest are: 1). the message integrity being sent is preserved; any message

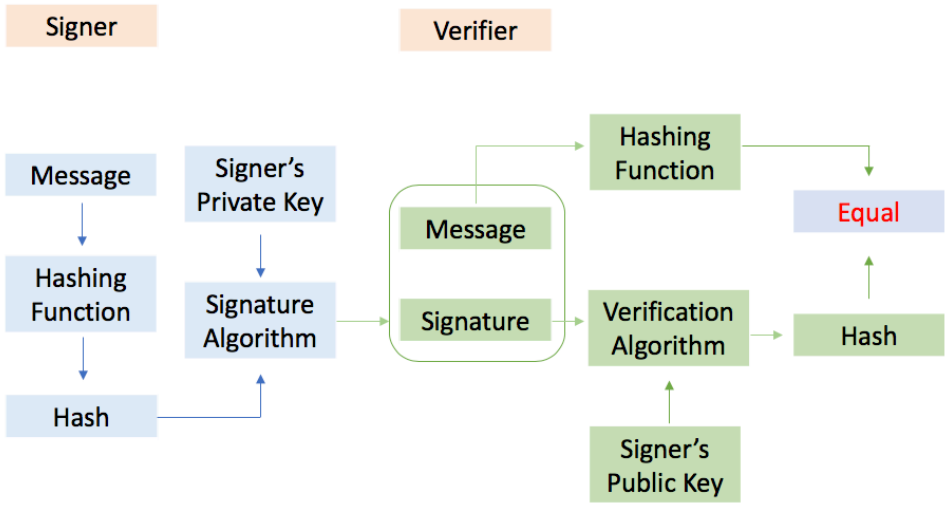
alteration will immediately be detected; 2). the digital signature will be applied to the digest, which is usually considerably smaller than the message itself; 3). Hashing algorithms are much faster than any encryption algorithm (asymmetric or symmetric).

If there is a match between the decrypted and evaluated digests, the signature can be verified, and the recipient can accept the message as coming unaltered from the issuer. If there is a mismatch this could mean that: 1) the message has not been signed by the issuer; 2) the message has been altered, or 3) in both cases, the message should be rejected.

(3) How the user is able to determine the identity of the individual to whom the public key cipher is associated?

This issue is solved by the use of certificate validation. Like a passport, a certificate is a piece of information that proves the identity of a public-key's owner. Certificates are signed and delivered securely by a trusted third-party entity called a Certificate Authority (CA). A certificate contains the CA's identity and signature of that certificate, the owner's identity and public key, and the certificate expiration date. With a certificate instead of a public key, a recipient can compare the owner's identity and verify the certificated is still valid and has been signed by a trusted CA with the issuer's certificate signature.

(4) Illustrate how a digital signature is used within a commonly used network communication protocol or security service.



Briefly, the public-private key pair used for encryption /decryption and signing/verifying are different (signer's private key is referred as the signature key and the public key as the verification key). Singer feeds data to the hash function and generated hash of data. Digital signature produced by signature algorithm with hash value and signature key is appended to the data and then both are sent to the verifier. The verifier run the verification algorithm and hashing function. For verification,

the hash value and output algorithm are compared. Based on the comparison result, verifies decides if the digital signature is valid.

Q5: In one to two pages, define and discuss the operation of both viruses and worms. Compare and contrast the effectiveness of these two types of malware. Identify and discuss at least one news article published in either 2014 or 2015 or 2016 that discusses victims of these types of malware.

(1) Define and discuss the operation of both viruses and worms

A computer virus is a small malicious program able to inject its code into other programs/applications or data files, without the permission or knowledge of the user. The virus must execute and replicate itself. Purpose of viruses is very often of a harmful nature such as data deletion or corruption on the targeted host. There are five recognized types of viruses: file infector viruses, boot sector viruses, master boot record viruses, multipartite viruses, and macro viruses.

In contrast to viruses which require the spreading of an infected host file, worms are programs that replicated themselves form system to system without the use of a host file. Worms generally exist inside of other files, often Word documents, Excel spreadsheets, Access database files, etc. The most common categorization of worms relies on the methods how they spread: email worms, internet worms, network worms, and multi-vector worms.

(2) Compare and contrast the effectiveness of these two types of malware

	Computer Virus	Computer Worms
Infection Route	Insert into a file or executable program	Exploits a weakness in an application or operating system by replicating itself
Human action	Needed	Not required
Spread	Rely on users transferring infected files /programs to other computer systems	Can use a network to replicate itself to other computer systems without user intervention
File Infection	Yes. It deleted or modifies files. Sometimes a virus can change file locations	Usually not. Worms usually only monopolize the CPU and memory
Speed	Virus is slower than worm	Worm is faster than virus.

(3) Identity and discuss at least one news article published in wither 2014 or 2015 or 2016 that discusses victims of these types of malware

In 2014, a backdoor computer worm named Win32.IRCBot spread through MSN Messenger and Windows Live Messenger. After being installed on a PC, the worm replicates itself into a Windows system folder, creates a new file named as "Windows Genuine Advantage Validation Notification" and becomes part of the computer's automatic startup. This worms also send itself to all MSN contacts by an attachment named 'photos.zip'. Executing this zip file will install the worm onto the local PC. This worm provides a backdoor server, allows a remote intruder to gain access and control over the computer via an Internet Relay Chat channel which allows confidential information to be transmitted to a hacker. (Reference: Rajesh et al. A survey paper on malicious computer worms. Intentional Journal of Advanced Research in Computer Science & Technology (IJARCST 2015), http://ijarcst.com/doc/vol3issue2/ver2/brajesh.pdf)

In 2016, Northern Lincolnshire and Goole NHS Foundation Trust was hit by computer virus attack which forced three hospitals offline and caused the cancellation of all routine operations and outpatient appointments. The nature of the virus was not disclosed to the. (Reference: https://www.hipaajournal.com/virus-forces-shutdown-medstar-health-systems-10-hospital-computer-network-3372/).

Q6- Q7 (each 6 points)
Answer the question by providing an answer for the 'blank' and write at least 5-10 sentences (2-3 paragraphs) explaining why your answer is correct.

Q6: Defined as a Proposed Internet Standard in RFC 2246, _____ is an IETF standardization initiative whose goal is to produce an Internet standard version of SSL. Identify and explain the goals of your answer.

Defined as a Proposal Internet Standard in RFC 2246. TLS (Transport Layer Security) is an IETF standardization initiative whose goal is to produce an Internet standard version of SSL.

SSL and TLS are the protocols above TCP to protect user's privacy when using Internet.

SSL (Secure Sockets Layer) is the standard technology to secure an internet connection, protect any sensitive data sent between two systems (a server and a client, or server to server), and prevent modifying any information transferred (i.e. potential personal details). SSL does not necessarily protect data that is held on the server when protecting information that is passed through the internet channels.

TLS (Transport Layer Security) is an updated and more secure version of SSLv3 to meet the internet community's demands as a standardized protocol. TLS implements a standardized MAC (H-MAC) which operates with any hash function, not just MD5 or SHA which is used by the SSL protocol.

HTTPS employs TLS encryption security beyond the popular HTTP protocol. TLS encryption can help protect web applications from attacks such as DDoS (Distributed denial-of-Service) attacks and data breaches.

Q7: A _____ provides a form of NAC by allowing or denying network traffic between an enterprise host and an external user.

A firewall provides a form of NAC by allowing or denying network traffic between an enterprise host and an external user. Firewall limits scope of data and application access.

A firewall protects a private corporate network from a hostile intrusion that could cause data corruption, denial of service or compromise data confidentiality, while a corporate firewall must have at least two network interfaces. Firewall examines the coming traffic and based on ACL and firewall policy, it could drop the coming traffic, or forward the traffic to DMZ, or internal network. Firewalls operate at different layers (OSI network layer, transport TCP layer, application layer) to use different criteria to filter, examine and restrict traffic.

NAC (Network Access Control) is an umbrella term for managing access to a network. NAC systems deal with these three categories of components: Access Requestor (AR), Policy Server, and Network Access Server (NAS). NAC authenticates users logging into the network, determines what data they can access and actions they can perform, and also examines the health of the user's computer or mobile service. NAC can be implemented with multiple software components or via integrated package.

NAC as a potential personal firewall that uses more comprehensive parameters in making access decisions than a traditional firewall does. NAC might integrate the automatic remediation process into the network systems, allowing the network infrastructure as routers, switches and firewalls to work together with back office servers and end users computing equipment to ensure the information system is operating securely before interoperability is allowed.

Q8- Q15 (each 6 points)

For each multiple-choice question, record the one letter of your chosen answer (3 points) and write at least 2-5 sentences explaining why your chosen answer is correct and another 2-5 sentences for each of the other answer choices explaining why they are not the correct answer (3 points).

Q8: Which of the following defines a number of techniques for key management? Explain your answer by describing the techniques in 2-3 paragraphs.

a) KEP
b) DH key exchange
c) KMP
d) IKE

The correct answer is answer d (IKE). IKE (Internet Key Exchange) defines a number of techniques for key management. IKE is an IPSec (Internet Protocol Security) standard protocol used to ensure security for virtual private network (VPN) negotiation and remote host or network access, also defines an automatic means of negotiation and authentication for IPSec security associations (SA).

KEP (Key Exchange Protocols, answer a) are essential for enabling the use of shared-key cryptography to protect transmitted data via insecure networks. For example, Diffie-Hellman Key Exchange (DH key exchange, answer b) enables two users to securely exchange a key that can then be used for subsequent symmetric encryption of messages.

DH key exchange (Diffie-Hellman key exchange, answer b) is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols, and establishes a shared secret between two parties that can be used for secret communication for exchanging data over a public network.

A Key Management Policy (KMP, answer c) is a high-level set of rules that are established by an organization to describe the goals, responsibilities, and overall requirements for the management of cryptographic keying material used to protect private or critical facilities, processes, or information. KMPs are implemented by system administrators through a combination or security mechanisms and procedures.

Q9: In IPSec, applying authentication to all of the packets except for the IP header is called which of the following? Explain why this is secure in 2-3 paragraphs.

a) Tunnel Mode
b) Transport Mode
c) Association Mode
d) Security Mode

The correct answer is answer b (Transport Mode). In IPSec, authentication applied to all of the packet except for the IP header is transport mode (answer b), while authentication applied to the entire original IP packet is tunnel mode (answer a). Transport Mode (answer b) provides primarily for upper-layer protocols. Typically, transport mode is used for end-to-end

communication between two hosts (e.g., a client and a server, or two workstations). 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).

One of the examples when transport mode will be used is for protection of router management traffic. It can also be that you use an encrypted RDP session or SSH from your PC to Server. It will also be good there to use transport mode as in that case two host are speaking directly to each other through the IPSec tunnel.

Tunnel mode (answer a) provide protection to the entire IP packet. In order to achieve this, the entire packet plus security fields is treated as the payload of new outer IP packet with a new outer IP after the AH or ESP fields are added to the IP packet. With tunnel mode, a number of hosts on networks behind firewalls may engage in secure communications without implementing IPSec.

Association Mode (answer c) determines how the wireless clients will establish the association with the access point. The network administrator can choose one of three association modes: Open, WPA, or WPA2.

Generally, security modes refer to information systems security modes of operations used in mandatory access control (MAC) system. Both Tunnel mode and Transport mode are Security Modes for traffic that is transmitted between user host and network.

Q10: Which of the following are functional areas encompassed by IPsec?

a) Authentication
b) Key Management
c) Confidentiality
d) All of the above
e) None of the above

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. It encompasses three functional areas: authentication (answer a), key management (answer b) and confidentiality (answer c). Therefore, the correct answer is answer d (all of the above).

Authentication (answer a) makes use of the HMAC message authentication code and can be applied to the entire original IP packet (tunnel mode) or to all of the packet except for the IP header (transport mode).The authentication mechanism assures that a received packet was

transmitted by the party identified as the source in the packet header and the packet has not been altered in transit.

The key management (answer b) facility is concerned with the secure exchange of keys. Internet Key Exchange (IKE) defines a number of techniques.

Confidentiality (answer c) is provided by an encryption format know as encapsulating security payload. Both tunnel and transport modes can be accommodated. The confidentiality facility enables communication nodes to encrypt messages to prevent eavesdropping by third parties.

Q11: Which of the following is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it?

a) SAD
b) SPD
c) SA
d) SPI

Security Association (SA, answer c) is one-way relationship between a sender a receiver that affords security service to the traffic carried on and allows hosts to share information that is needed to send and receive secured datagrams. Parameters that defines a SA: authentication algorithm and keys for AH or ESP, encryption algorithm and keys for ESP , life time of SA, IPsec protocol mode (tunnel or transport), anti-replay service parameters.

Security Association Database (SAD, answer a) contains all active SAs. Each SA entity is indexed by outer destination IP address, security parameters index, and security protocol identifier (AH or ESP). Each SA entry (in a SAD) contains authentication algorithm and keys, encryption algorithm and keys, lifetime of SA, IPSec protocol mode (tunnel or transport), selector values, anti-replay service parameters.

Security Policy Database (SPD, answer b) is used to relate IP traffic to specific SAs. SPD is used to relate IP traffic to specific SAs. Each policy entry is keyed by one or more selectors that define that set of all IP traffic encompassed by this entry. Each policy entry includes packet handling policy (discard packet, bypass IPSec, or process IPSec) and link to an active SA (or SAs) in the SAD.

Security parameters Index (SPI, answer d) is a 32-bit unsigned integer assigned to this SA and having local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.

Q12: Which of the following consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication? [Hint: The current specification is RFC 4303.]

a) SPI
b) ESP
c) ISA
d) IPsec

ESP (Encapsulating Security Payload, answer b) is the correct answer. ESP consists of an encapsulating header and trailer used to provide encryption or combined encryption/authentication and the current specification is RFC 4303. ESP encrypts IP payload and any IPv6 extension headers following the ESP header in transport mode SA and encrypts entire inner IP packet in tunnel mode SA.

Security parameters Index (SPI, answer a) is a 32-bit unsigned integer assigned to this SA and having local significance only. The SPI is carried in AH and ESP headers to enable the receiving system to select the SA under which a received packet will be processed.

ISA (answer c, Internet Security Association) is security document that specifies the technical and security requirement for establishing, operating and maintaining the interconnection. ISA and Key management Protocol (ISAKMP) are needed to negotiate, establish, modify and delete security associations and their corresponding data.

IPsec (answer d) 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. It encompasses three functional areas: authentication, key management and confidentiality.

Q13: What is the term used for certified 802.11b products?

a) WAP
b) WEP
c) WPA
d) Wi-Fi

The correct answer is answer d (Wi-Fi). Wi-Fi (Wireless Fidelity, answer d) is the term used for certified 802.11b products. 802.11b is the first 802.11 standard to gain broad industry acceptance. Wi-Fi alliance has been extended to 802.11g products.

WAP (Wireless Application Protocol, answer a) is a standard to provide mobile users of wireless phones and other wireless terminals access to telephony and information services including the internet and the web.

Wired Equivalent Privacy (WEP, answer b) is a security algorithm for IEEE 802.11 wireless networks. WEP was the only encryption protocol available to 802.11a and 802.11b devices built before the WPA standard, which was available for 802.11g device.

Wi-Fi Protected Access (WPA, answer c): set of security mechanisms that eliminates most 802.11 security issues, based on the current state of the 802.11i standard. WPA2 incorporates all of the features of the IEEE 802.11i WLAN security specification.

Q14: Which of the following is an umbrella term for managing access to a network?

a) NAS
b) NAC (Network access control)
c) ARQ
d) RAS

The correct answer is answer b (NAC). NAC (answer b, Network Access Control) is an umbrella term for managing access to a network. It includes these three components: Access Requestor (AR), Policy Server, and Network Access Server (NAS). NAC authenticates users logging into the network, determines what data they can access and actions they can perform, and also examines the health of the user's computer or mobile service. NAC can be implemented with multiple software components or via integrated package.

Network Access Server (NAS, answer a) functions as an access control point for users in remote locations connecting to an enterprise's internal network. NAS is also called a media gateway, remote access server (RAS), or policy server. NAS may also include its own authentication services or rely on a separate authentication service from the policy server.

Automatic Repeat request (ARQ, answer c) is a method of handling communication errors in which the receiving station requests retransmission if an error occurs.

Remote Access Server (RAS. Answer d) is dedicated to handling users that are not on a LAN but need remote access to it, allows users to gain access to files and print services on the LAN from a remote location. For example, a user who dials into a network form home using an analog modem or an ISDN connection will dial into a remote access server. Once the user is authenticated he can access shared drives and printers as if he were physically connected to the office LAN.

Q15: Which of the following makes use of X.509 certificates? In 2-3 paragraphs, define X.509 certificates and how they are used in your chosen answer.

a) PKI
b) CDC
c) HMAC
d) KDC

The correct answer is answer a (PKI). An X.509 certificate is a digital certificate that uses the widely accepted international X.509 public key infrastructure (PKI, answer a) standard to verify that a public key belongs to the user, computer or service identity contained within the certificate. X.509 certificates are used in most network security applications, including IP security, transport layer security (TLS), and S/MIME.

CDC (Certificate Distribution Center, answer b) is a special purpose name server created to service DASS (Distributed Authentication Security Service) until an X.500 service is available in all of the environments where DASS needs to operate.

HMAC (Hash-based Message Authentication Code, answer c) is a mechanism for message authentication by using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, for example, MD5, SHA-1, in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function.

KDC (Key Distribution Center, answer d) is a type of key center (used in symmetric cryptography) that implements a key distribution protocol to provide keys (usually, session keys) to two (or more) entities that wish to communicate securely.