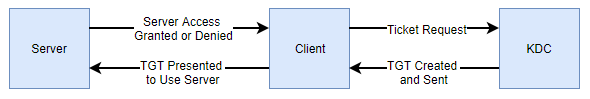
Q1- Q5 (each 8 points)

Answer each question fully and completely. Show your work and state your assumptions where appropriate.

**Q1**

Kerberos provides a central authentication service developed to limit access to servers to only authorized users. Kerberos utilizes symmetric encryption. In Kerberos, a user, or client machine, sends a ticket request to the key distribution center (KDC). The KDC creates a ticket-granting ticket (TGT) for the client, encrypts the ticket and sends it back to the client. The client then decrypts the TGT. If the decryption is successful, the TGT is retained and confirms the user’s identity. The Kerberos system is designed to exchange messages between three types of entities: clients / users, servers and KDCs.

Clients and servers trust Kerberos to handle their authentication needs. As long as the Kerberos implementation is secure, the authentication between clients and servers is secure. Kerberos is secure, reliable, transparent and scalable. Kerberos offers both identify confirmation, data integrity and data privacy. The authentication process described above illustrates the Kerberos approach to identity confirmation. After identity confirmation and authentication is complete, Kerberos uses symmetric key encryption to protect communication along with hash keys to confirm data integrity.



Q1 References

<https://web.mit.edu/kerberos/krb5-1.5/krb5-1.5.4/doc/krb5-install/What-is-Kerberos-and-How-Does-it-Work_003f.html#What-is-Kerberos-and-How-Does-it-Work_003f>

Section 15.3, Course Textbook

<https://www.kerberos.org/software/whykerberos.pdf>

<https://web.mit.edu/kerberos/>

**Q2**

Border Gateway Protocol (BGP) is the routing protocol that essentially drives the internet. The internet can be thought of as a network of computer networks. The computer networks are known as autonomous systems. BGP assists in choosing the path through the internet and between autonomous systems that typically requires the least number of passages through autonomous systems. Once the traffic is correctly routed to the final autonomous system, the work of BGP is complete. The ultimate autonomous system is responsible to assuring the information guided through the internet by BGP arrives at the correct destination within the autonomous network.

There are at least two methods to exploit BGP to fraudulently direct packets destined for a particular IP address not serviced by the ISP to flow through the ISP. The first example is a denial of service attack. In this type of attack, a false route can be injected into the routing tables that point traffic destined for this specific IP address to be directed to a false address. An example of this type of attack occurred when Pakistan Telecom rerouted YouTube traffic to a dead end on the internet by injecting a new route into the routing tables. More broadly BGP hijacking can accomplish this same goal. In BGP hijacking, a router can be reconfigured to announce IP address prefixes not assigned to the router. When the poisoned router begins to broadcast the false information, the routing tables of other adjacent routers can become polluted with this false information. As those routers broadcast the false information, more routers are polluted. The end result is the broader internet can start redirecting traffic to a destination other than the intended end point.

There have been an unknown number of BCP hijacking attacks during the 2014 – 2016 period. One notable BCP Hijacking attack occurred in August of 2014. In this attack the adversary targeted Bitcoin miners. In this attack the Bitcoin bandit redirected internet traffic from at least nineteen ISPs to steal Bitcoins from a group of Bitcoin users. The thief users a staff account at a Canadian ISP to broadcast false routing information that directed traffic to the thief’s server. This enabled the hijacker to collect approximately $83,000 in cryptocurrencies over a two to three month period before being discovered.

Q2 References

<http://www.enterprisenetworkingplanet.com/netsp/article.php/3615896/Networking-101-Understanding-BGP-Routing.htm>

<http://www.ciscopress.com/articles/article.asp?p=1237179&seqNum=2>

<https://www.bishopfox.com/blog/2015/08/an-overview-of-bgp-hijacking/>

<https://www.wired.com/2014/08/isp-bitcoin-theft/>

**Q3**

The five tenets of the ACM Code of Ethics I believe would be used most often to guide one’s career are: Contribute to society and human well-being (1.1), acquire and maintain professional experience (2.2), be honest and trustworth (1.3), accept and provide appropriate professional review (2.4) and honor contracts, agreements and assigned responsibilities (2.6).

General moral imperative 1.1 is “contribute to society and human well-being”. Software should not be developed to target the human rights of any person or group of people. When designing and implementing software care should be taken to assure the product is used in a socially responsible manner and avoids harmful effects to others. In a corporate setting, the focus should be on improving the day-to-day working lives of the end users while complying with rules and regulations.

Professional responsibility 2.2 is “acquire and maintain professional competence”. In order to deliver software solutions which comply with the other imperatives of the ACM code, one’s skills must be up to date and constantly evolving to keep pace with the world of technology. This requires the individual contributor to take responsibility to driving career and skill development, and managers must devote time to understanding the interests of their employees and guide them through a meaningful development path.

General moral imperative 1.3 is “be honest and trustworthy”. A technologist should not deliberately make false or misleading claims. Transparency and disclosure of the risks, issues and defects should be the norm. Often, technology professionals are trusted with sensitive data. Care should be taken to design systems, implement policies and follow those policies to protect information deemed to be sensitive.

Professional responsibility 2.4 is “accept and provide appropriate professional review”. Honest, direct and timely feedback is critical developing the career of yourself of your direct reports. Similarly, remaining open to receiving that feedback allows for the reviewee to internalize and begin to make the necessary changes to improve performance and achieve career growth.

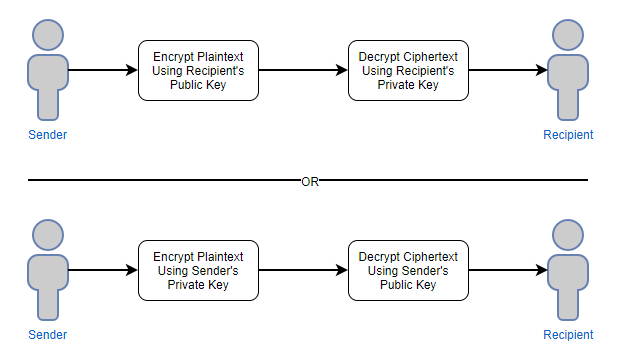
Professional responsibility 2.6 is “honor contracts, agreements and assigned responsibilities”. Honoring agreements is the hallmark to professional responsibility. Delivering software which meets contractual agreements or proactively raises changes to the contract is required to meet the financial and timeline expectations of clients and customers. On a project basis, all reasonable efforts should be made to meet commitments of project deliverables and timelines. Often overlooked, meeting assignment expectations are critical to the efficient operation of projects and departments.

Q3 Resources

<https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct>

**Q4**

Public key cryptosystems are asymmetric and rely public and private keys. One key is used for encryption and the other key is used for decryption. A digital signature serves to uniquely identify the sender of a digital message. Public key encryption effectively offers a digital signature. For example, the sender encrypts a message using his private key. The receiver will then decrypt the message using the sender’s public key. This offers a form of identity confirmation, a digital signature, since only the sender knows his private key. The accurate decryption allows the receiver to verify the digital signature of the sender.



RSA is one of the more widely adopted and utilized security schemes using public key encryption. The RSA security service utilizes digital signatures by applying a sender’s private key to a message to create a digital signature. In contrast to standard public key encryption. The RSA digital signature is not the equivalent to RSA message decryption or encryption. Instead of relying solely on the public and private key encryption algorithms to provide for identify confirmation, RSA employs a cryptographic hash function to digitally sign electronic messages or blocks of electronic messages. This allows RSA to confirm the origin of a message without overloading the size of the encrypted message or encrypted message block itself. This is an important concern as RSA generally struggles to function with messages longer than the encryption key.

A more specific RSA security protocol incorporating digital signatures is the RSA Probabilistic Signature Scheme (RSA-PSS). RSA-PSS was not developed in response to any particular threat or weakness in RSA. RSA-PSS was developed to provide an even more mathematically secure method of providing identity confirmation of an electronic message. Conceptually similar to conventional digital signatures in RSA, RSA-PSS employs the use of a hash function to digitally sign electronic messages. When used to create a digital signature, RSA-PSS produces a single hash key value. This value is used as the digital signature. The RSA parameters are coded to carry the appropriate RSA-PSS parameters. This allows for proper decoding and verification of the hash value to confirm electronic message integrity and identity.

Q4 Resources

Ch 9, Course Textbook

<https://en.wikipedia.org/wiki/Digital_signature>

<https://www.ietf.org/rfc/rfc4056>

<http://www.drdobbs.com/rsa-digital-signatures/184404605>

<https://www.cs.cornell.edu/courses/cs5430/2015sp/notes/rsa_sign_vs_dec.php>

<https://www.ietf.org/rfc/rfc3447.txt>

**Q5**

Worms and viruses are both types of malicious software. Viruses are bit of code or programs attached to any standard and often legitimate program. The virus uses the execution of that program to propagate itself. The virus then spreads by attaching to more and more programs. The virus can be transmitted via email, internet downloads, removable media or just about any other form of digital media. Worms have the ability to copy themselves from one network attached device to another. Worms are often inadvertently downloaded by clicking a disguised link in an email. Once the worm is installed, it quickly reproduces itself over computer networks. Worms can even spread across networks by access email programs on each computer and mailing them themselves to email address book entries.

Viruses and worms can both be effective forms of malware. Both are similar in that they are both forms of software designed for a malicious purpose. The way viruses and worms replicate are very different. Viruses replicate themselves by attaching to a host program. The virus is activated and spread at run time of the infected program. Viruses require the action of a user of the infected program to propagate themselves. This is the primary differences between a worm and a virus. A worm is capable of reproducing itself. Worms can copy themselves to any number of network attached devices with no human assistance. In this sense, worms have greater capacity to invade more computers in a quicker timeframe than a virus. The damage and number of infected devices done by a worm can be achieved at a far greater pace than a virus before being contained.

A recent example of a computer virus from the news is the 2017 “WannaCry” ransomware-based computer virus. The Washington Post and the White House administration reported the virus originated in North Korea. The virus infected more than 230,000 computers in over 150 countries. The “WannaCry” virus spread by exploiting Microsoft file sharing technologies installed on most computers with Windows operating systems. The “WannaCry” virus works by encrypting all data on a computer. A screen then appears requesting money to decrypt all files. If the ransom is not paid, all file will be deleted. The impact could be negligible on a lightly used personal computer to catastrophic for a corporate or government server containing sensitive and/or mission critical data. Interestingly, the fault in Windows operating systems was discovered by the National Security Agency (NSA). Instead of reporting this deficiency to Microsoft, the NSA catalogued it for possible future use to spy on potential targets. This was discovered by hackers and leaked on the internet. North Korea has a recent history of computer virus attacks. In 2014, North Korea effectively targeted Sony Pictures in an attempt to stop the release of a comedic film centering around the North Korean government.

Q5 Resources

<https://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/how-does-a-virus-work.aspx>

<https://computer.howstuffworks.com/virus5.htm>

<https://www.lifewire.com/how-computer-worms-work-816582>

<https://www.pandasecurity.com/mediacenter/malware/worms-vs-viruses-whats-difference/>

<https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html?utm_term=.783b2708872b>

<https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/>

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**

Answer: Transport Layer Security (TLS)

The goals of TLS, as stated in RFC 2246, are cryptographic security, interoperability, extensibility and relative efficiency. To accomplish these goals TLS seeks to deliver the following:

* Cryptographic Security
  + A secure connection between two parties should be used by TLS.
* Interoperability
  + Independent application developers should be able to utilize TLS to exchange cryptographic parameters without knowledge of the applications developed by others.
* Extensibility
  + TLS will provide a framework where new public keys and bulk encryption methods can be incorporated without having to create a new protocol
* Relative Efficiency
  + TLS implements caching to reduce the number of connections that need to be verified and established.

Q6 References

<https://www.ietf.org/rfc/rfc2246.txt>

17.3 Course Textbook

**Q7**

Answer: Firewall

Network access control (NAC) is a general term describing methods for managing and controlling access to a network. Network access enforcement methods are applied to access requestors to control network access. As described in the fill in the blank question, a firewall is a type of network access enforcement method that governs which access requestors external to the enterprise may access the enterprise network. Other types of enforcement methods are IEEE 802.1X, DHCP servers and VLANs.

Q7 Resources

16.1 Course Textbook

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**

Answer: D) IKE

Internet key exchange (IKE) portion of IPsec determines key distribution. The DH key exchange is a method of exchanging keys securely over a public channel. KMP provides a framework for internet key management. Key Exchange Protocol (KEP) is any method of securely exchanging cryptographic keys between two parties. Though there are multiple key exchange protocols, key exchange protocols do not necessarily cover the comprehensive management of keys.

Q8 Resources

Ch20 Course Textbook.

<https://pdfs.semanticscholar.org/e60e/1828ff553bcb348c75b0337bea2e06f5fb8c.pdf>

**Q9**

Answer: B) Transport Mode

IPsec operates in transport and tunnel mode. In tunnel mode, all packets are combined and encrypted. In transport mode, encrypts all packets except for the IP Header. Transport mode is commonly used for end to end communications. For example, the communications between a client and a server is likely to use transport mode. Transport mode focuses on protecting the payload of the message through encryption prior to transmitting the data. The IP payload is then decrypted at the destination. Protecting the IP Payload assures the most sensitive contents of the transmission are protected.

Q9 Resources

<http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html>

Ch 20 Course Textbook

**Q10**

Answer: D) All of the above

IPsec covers authentication, confidentiality and key management. IPsec is a complex IETF specification spanning several RFC documents. Standards, minimal functionality and interoperability between protocols supporting authentication, confidentiality and key management are thoroughly documented by IPSec.

Q10 Resources

CH 20 Course Textbook, p. 630

**Q11**

Answer: C) SA

A Security Association (SA) is a one way relationship between a sender and a receiver that affords security services to the traffic carried on it. The remaining answers describe functions used to facilitate an SA. Security Parameters Index (SPI) is a bit string assigned to the SA. The SA is governed by the interaction of two databases: Security Association Database (SAD) and Security Policy Database (SPD). The contents of the SPD defines a subset of IP traffic and points to a SA for that traffic. Each SPD row is a set of IP and protocol field values called selectors. The contents of the SAD define the parameters associated with each SA.

Q11 Resources

<http://www.idc-online.com/technical_references/pdfs/data_communications/I_Security_Services.pdf>

pp. 633 – 634, Course Textbook

**Q12**

Answer: B) ESP

Encapsulating Security Payload (ESP) consists of an encapsulating header and trailer used to provide encryption or combined encryption and authentication. ESP can be used to provide confidentiality, data origin, authentication, connectionless integrity, and anti-replay service and limited traffic flow confidentiality services. Confidentiality and integrity will typically be employed together with ESP. The anti-replay service can be selected for a security association if the integrity service is also selected. The traffic flow confidentiality service requires the source and destination addresses to be protected to be effective.

Q12 Resources

<https://www.ietf.org/rfc/rfc4303.txt>

**Q13**

Answer: D) Wi-Fi

The term “Wi-Fi” is used for certified 802.11b products. WAP, WEP and WPA are all 802.11 standard protocols for accessing and protecting wireless communications. Wireless Application Protocol (WAP) is a technical standard for accessing information over a wireless network. Wired Equivalent Privacy (WEP) is a common encryption algorithm used to secure information transmitted over a wireless network. Wi-Fi Protected Access (WPA) is another security protocol used to secure wireless computer networks.

Q13 Resources

<https://en.wikipedia.org/wiki/Wireless_Application_Protocol>

<https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy>

<https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access>

**Q14**

Answer: B) NAC

Network access control (NAC) is a general term describing methods for managing and controlling access to a network. A network access server (NAS) functions as an access control point for users in remote locations connecting to an enterprise’s internal network. A remote access server (RAS) is an alternate term for a network access server. Automatic repeat request (ARQ) is a method on controlling data transmission with a network and assuring sent messages are received by the appropriate destination through the use of an acknowledgement response message.

Q14 Resources

<https://en.wikipedia.org/wiki/Automatic_repeat_request>

pp. 496 – 497, course textbook

**Q15**

Answer: A) PKI

Public Key Infrastructure makes use of X.509 certificates. X.509 certificates define a framework for the provision of authentication services by the X.500 directory to its users. Additionally, X.509 defines alternative authentication protocols based on the use of public key certificates. X.509 is based on the use of public key cryptography and digital signatures. The X.509 standard does not specify public key algorithms, but it does recommend RSA.

The core of X.509 functionality is driven the public key certificates associated with each user. Certificates are obtained from a certificate authority and stored locally. To securely transfer information between users, the public key of the receiver is used to encrypt the message. Once received the recipient uses a private key to decrypt and read the message.

Q15 Resources

Section 14.4, Course Textbook