**MSDS 7349 Data and Network Security**

**Exam 2**

**Due End of Class Week 15**

**Name: Andrew Abbott**

**Section: 401**

**Exam 2: Directions**

**This is Exam 2 for MSDS 7349, Data and Network Security. This document contains the questions for the exam.**

**For your answers, create a Word document that clearly identiﬁes every question number and your answer to that question. Name the Word ﬁle containing your answers ‘yourLastNameMSDS7349Exam2.doc’. For example, the Word ﬁle for John Smith would have the name SmithMSDS7349Exam2.doc.**

**Submit your Word ﬁle. Answer each question fully and completely. Show all of your work and state your assumptions where appropriate. Each answer is worth an equal number of points.**

**For each multiple choice question, record the one letter of your chosen answer (1/2 the 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 (1/2 the points). Note that one sentence explanations for any choice except an ‘All of the above’ or ‘None of the above’ choice will receive 0 points even if they are correct.**

**For each ﬁll in the blank question, 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.**

**The questions may have hints embedded within them regarding the answer and what should be written for supporting the chosen answer. Follow these hints as appropriate for full points. Following directions is necessary to achieve the maximum exam grade.**

**Do not copy answers. Always use your own words.**

**Directly under each question list all persons with whom you collaborated and list all resources used in arriving at your answer. Resources include but are not limited to the textbook used for this course, papers read on the topic, and Google search results. Note that Google is not a reference. It is a tool to ﬁnd references. Don’t forget to place your name in the Word document itself.**

**Exam 2: Questions**

**1) 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.**

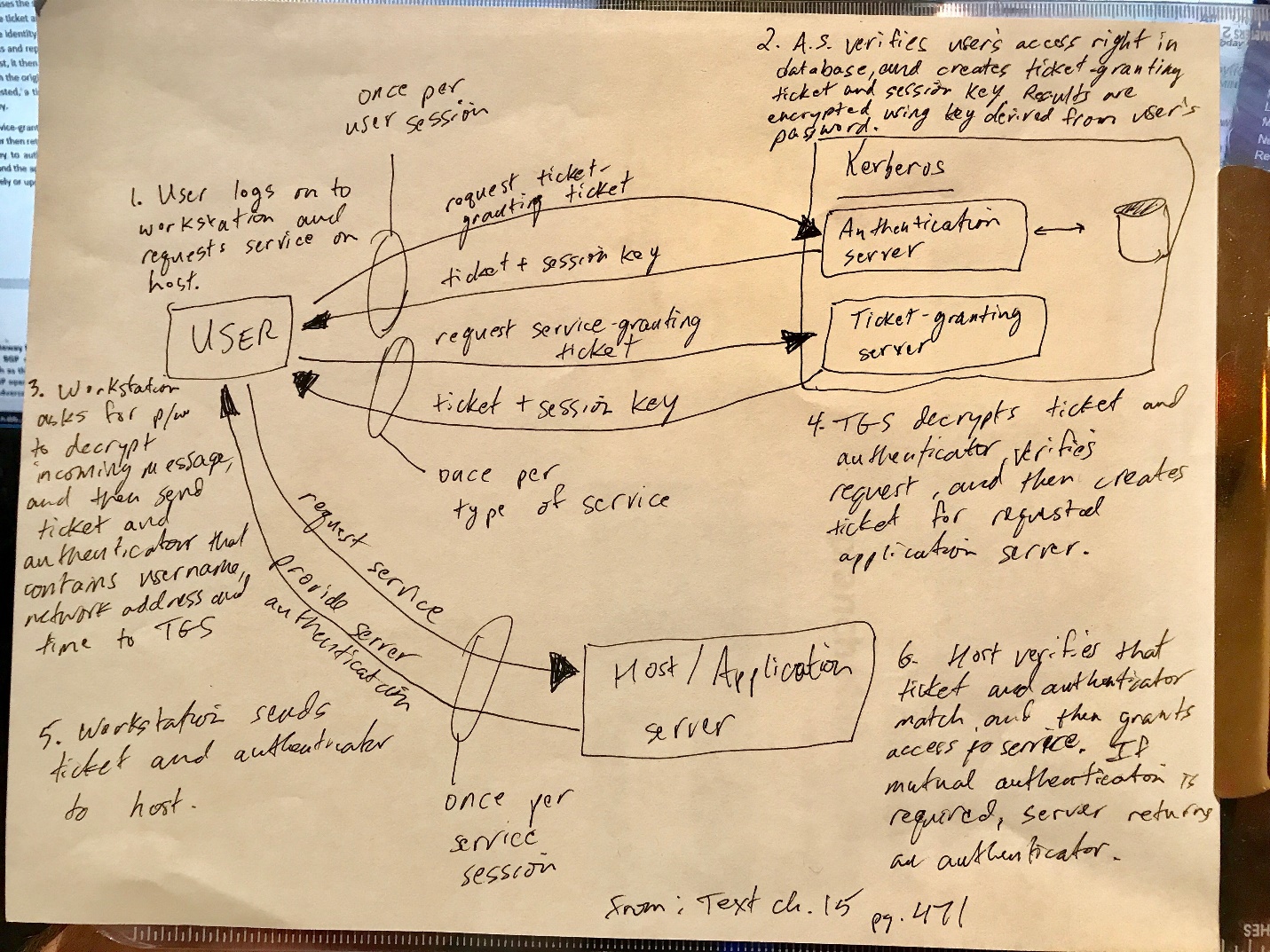
**Collaboration: None**

**References:** William Stallings. 2017. Cryptography and Network Security: Principles and Practice (7th ed.). Pearson Education. Hoboken, NJ USA

Kerberos is an authentication service that provides a centralized authentication server that authenticates two systems to one another. Kerberos uses symmetric key encryption exclusively to provide this function. The method Kerberos uses begins with a user logging on to a workstation to request service from a host. A part of the Kerberos system called the authentication server (AS) verifies the user’s access rights in the Kerberos database and creates a ticket-granting ticket and a session key that are encrypted using a key derived from the user’s password. That password never needed to be sent over the network but is then used by the user to decrypt the incoming message that contains the ticket-granting ticket and session key. This part of the process only needs to be done once per user log on session.

The user’s workstation then sends the ticket-granting ticket along with an authenticator which includes the user’s name, network address and the time, to another part of the Kerberos service called the Ticket-Granting Server (TGS). The ticket-granting ticket contains the session key and can be read by the TGS using a key it shares with the AS, putting both the user and the TGS in possession of the session key. The TGS uses the session key to decrypt the authenticator and then compares it with the information in the ticket and the network address of the incoming request. It is the authenticator that proves the identity of the user and is only valid for a short lifetime, countering threats from stolen tickets and replay attacks. After the TGS decrypts the ticket and authenticator and verifies the request, it then returns a message containing another ticket and a different session key encrypted with the original session key. The message includes the ID of the application server that was requested, a time stamp and the ticket, a service-granting ticket which also contains the session key.

The user now has a reusable service-granting ticket and sends it along with an authenticator to the application server. The server then returns an authenticator with an incremented time-stamp encrypted with the session key to authenticate the server to the user. The result of these exchanges between the user and the application server are that both share a secret session key and can send messages securely or update the session key.



**2) 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.**

**Collaboration:** None

**References**: Course Lesson 12.3, <https://en.wikipedia.org/wiki/Border_Gateway_Protocol>, <https://tools.ietf.org/html/rfc7454> , <https://www.wsj.com/articles/old-internet-flaw-causes-new-problems-1445989248>

Border Gateway Protocol (BGP) is used for routing packets between internet service providers (ISPs). These BGP routers exchange information between ISPs such as the IP addresses served within each ISP. BGP neighbors (peers) are manually established and exchange between neighbors routing tables which contain the routes they should use to send the packets between addresses. Like much of the internet, this system was not designed with security in mind and contains no authentication. This protocol relies on trust between the operators of the routers. One way that this could be exploited is for an intruder to send and propagate different routing maps and BGP does not check to see if the shortest path recommended by its neighbor is truly the shortest path or if that recommendation is even coming from an authorized server.

According to the Wall Street Journal, (https://www.wsj.com/articles/old-internet-flaw-causes-new-problems-1445989248), in the summer of 2015 traffic from Level 3 Communications Inc. was rerouted through Malaysia, disrupting service and that same summer, Two Sigma Investments LLC also discovered that traffic destined for some of its addresses went to Russia instead. “Using BGP flaws to trick carriers into rerouting their clients’ data could let someone steal proprietary information, eavesdrop on confidential traffic or send information into cyber oblivion rendering it unreachable, according to security experts.”

**3) 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.**

**Collaboration:** None

**References:** <http://ethics.acm.org/code-of-ethics>

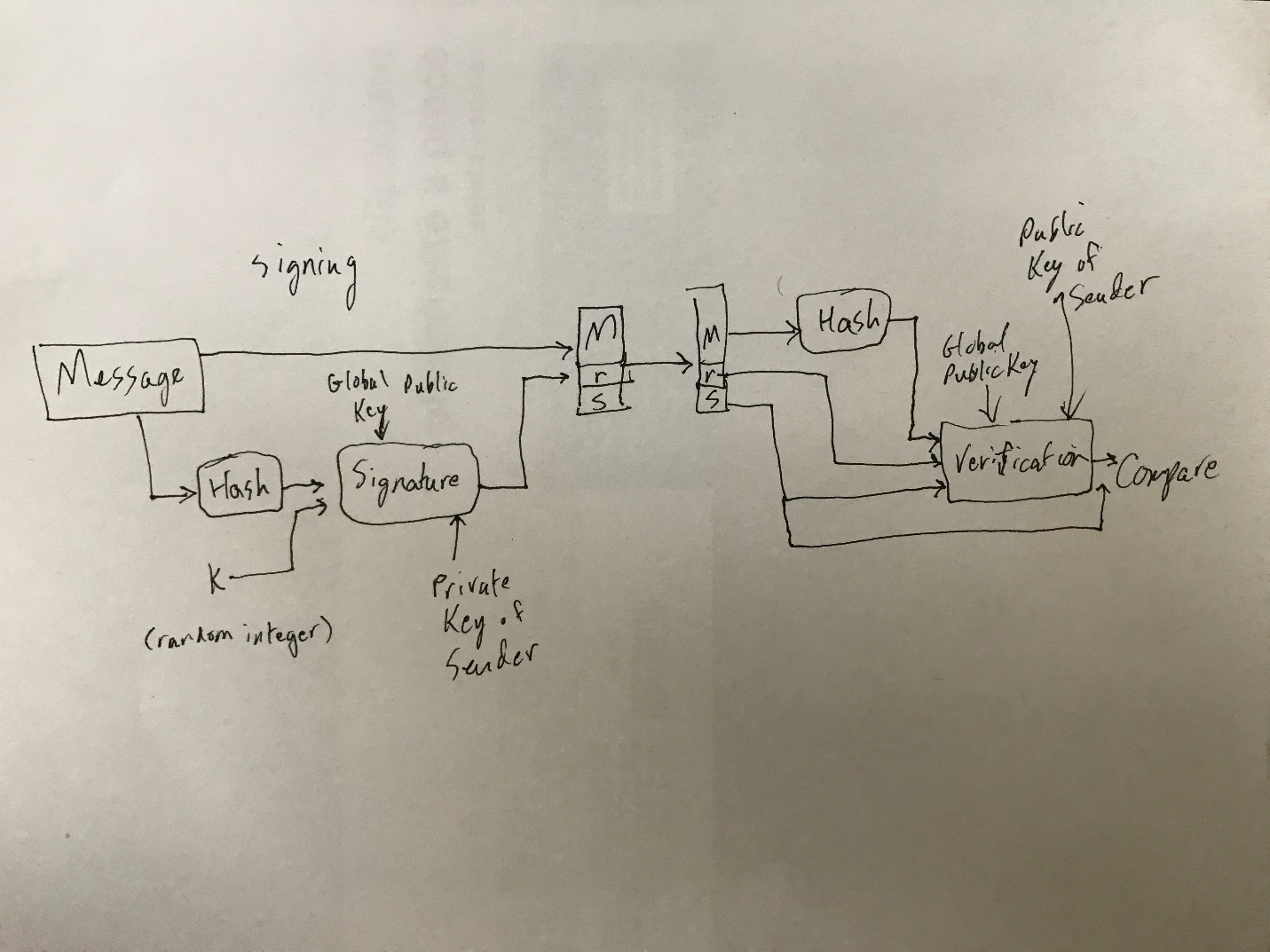
The five primary tenets of the ACM Code of Ethics that would be most used to guide one’s career are:

1. **Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work.** In guiding a career, the goal of achieving high quality work is of course necessary for maintaining that career and advancing within it. High effectiveness is how one makes themselves stand out among their peers and contributes to the product of their employer. High quality and effectiveness together seem to imply another of the tenets, to “acquire and maintain professional competence”. A high level of dignity is also important and somewhat encompasses a few of the other tenets. I think the call for dignity and dignity itself imply a commitment to not harm others and respect the intellectual property rights of others. For me dignity also includes being honest, trustworthy, and fair.
2. **Acquire and maintain professional competence**: As mentioned above, striving to achieve high levels of quality and effectiveness is important. This tenet goes further in striving to improve one’s abilities and knowledge, not just doing the best with what one has. I think that to be successful in any career or endeavor it is necessary to be a lifelong learner. This is especially true in a technology career where the tools and techniques are continually evolving. Our own toolboxes must also continually evolve in order to maintain the professional competence required by the ACM Code of Ethics.
3. **Know and respect existing laws pertaining to professional work:** In my current role as well as all my previous roles, there were large parts of the jobs that required careful following of laws and regulations. In fact, my current title is “Compliance Analyst”. Knowledge of current laws also involves several other of the Code’s tenets. Respecting property rights, respecting intellectual property, not discriminating, respecting privacy and confidentiality, and honoring contracts all have legal ramifications.
4. **Honor contracts, agreements, and assigned responsibilities:** I just mentioned the legal aspects of honoring contracts and this is very important in any career. If you fail to meet the stipulations of your contract you should not be paid. One of those contracts is your employment contract which covers assignments given to you by your supervisor. A quick way to end a career is to fail to complete assigned tasks. A better choice would be to go above and beyond your assigned tasks as well as help your coworkers with their tasks.
5. **Accept and provide appropriate professional review.** I think for work that involves data science, peer review is particularly important. Getting a fresh set of eyes on any problem is a great way to not only improve the product and save the time wasted when a solution does not meet expectations but also the peer review process is a knowledge sharing process. Learning by doing is the best way to learn and that involves making mistakes often. Peer review makes those mistakes productive rather than destructive.

**4) 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.**

**Collaboration:** None

**References:** Textbook, chapter 13

A public key cipher is typically used to provide a digital signature by using a secure hash function to generate a hash value for the message. That hash value and the sender’s private key are used to generate the digital signature. The sender then sends the message with the digital signature attached and the receiver then verifies the sender. To verify the sender of a message sent in this way the receiver first generates a hash for the received message. The using that hash and the sender’s public key, the receiver can verify that the signature is valid. That is because no one else has the private key in combination with the hash created from the message to have been able to send that signature. The following illustration shows the DSA approach to digital signatures.

**5) 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.**

**Collaboration:** None

**References:** <http://www.cisco.com/c/en/us/about/security-center/virus-differences.html>**,** <http://www.gazettextra.com/20160618/city_network_attacked_by_computer_virus>**,** <http://www.thedailybeast.com/articles/2016/07/09/the-terrifying-u-s-israeli-computer-worm-that-could-cause-world-war-iii.html> **,** <http://www.thedailybeast.com/articles/2011/11/16/new-computer-worm-may-presage-another-cyber-attack-potentially-on-iran.html>

A computer virus, like a biological virus, acts by creating copies of itself on or is its host. It then spreads from host to host creating copies of itself as it spreads. A computer virus requires the execution of some executable file to which it is attached. When that file or code is executed, the virus is executed, creating copies of itself and performing its malicious function. The effects of a computer virus can range from silly pranks to deleted data to denial of service.

An example of a computer virus in the news is an attack that occurred in Janesville, Wisconsin. City employees opened an infected email attachment which allowed a virus to infect the city network. The virus disabled the city’s websites and servers as well as disabling a program that digitally connects city services considered the “backbone of the city’s network infrastructure” by the city manager Mark Freitag.

Computer worms are like viruses but they do not require the execution of code to infect their host. They also copy themselves, travel between hosts, and cause a range of possible damages. They spread by either using a weakness in the host system or by tricking the user into executing their code. Once executed, worms use the system transport features to travel to new hosts.

A more well know example of a newsworthy computer worm is the Stuxnet worm. The Stuxnet worm was discovered by a Belarussian security expert on a client in Iran and allegedly created by the US and Israeli. The worm likely originated on a thumb-drive and infected tens of thousands of hosts. It was designed to only target specific kinds of machines at the Iranian Natanz nuclear facility. On every other infected machine, the worm had no function.

**6) Deﬁned as a Proposed Internet Standard in RFC 2246, the TLS Protocol is an IETF standardization initiative whose goal is to produce an Internet standard version of SSL. Identify and explain the goals of your answer.**

**Collaboration:** None

**References:** <https://www.ietf.org/rfc/rfc2246.txt>, <https://www.sans.org/reading-room/whitepapers/protocols/ssl-tls-beginners-guide-1029>

Reading the text of RFC 2246 I find a clear description of the goal and motivation of the TLS protocol. “The current version of SSL is version 3.0, released by Netscape in 1999. The Internet Engineering ask Force (IETF) has created a similar protocol in an attempt to standardize SSL within the Internet community. This protocol, the Transport Layer Security (TLS) protocol, will be discussed later in this paper.” The RFC goes on to describe the details and variations of the TLS protocol.

**7) A Firewall provides a form of NAC by allowing or denying network trafﬁc between an enterprise host and an external user.**

**Collaboration:** None

**References:** Textbook, chapter 16

A Network Access Control (NAC) describes the management of access to a network. A firewall is a form or NAC as it manages access to a network by allowing or denying traffic access between an external user and a host. Firewalls act to separate an internal network from the external internet. They prevent many attacks such as denial of service attacks or illegal access to internal data. The firewall administrators maintain a list of authorized users and IP address.

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

1. **KEP**
2. **DH key exchange**
3. **KMP**
4. **IKE**

**Collaboration:** None

**References:** Textbook, chapter 20

**9) 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.**

1. **Tunnel Mode**
2. **Transport Mode**
3. **Association Mode**
4. **Security Mode**

**Collaboration:** None

**References:** Textbook, chapter 20

Transport mode applies authentication to all the packets except for the IP header. This is secure because while the IP header is not authenticated, confidentiality is provided. For the policy where transport mode is used it is confidentiality that is required. The contents of all the packets are encrypted and decrypted by the end recipient application. The data and TCP headers are also authenticated by the receiver.

Transport mode is typically used in end-to-end communications between two hosts. The protection applies to the payload.

**10) Which of the following are functional areas encompassed by IPsec?**

1. **Authentication:** Authentication is provided by an Authentication Header (AH) or by an Encapsulating Security Payload (ESP). These are described in RFC 4302 and 4303.
2. **Key Management**: Internet Key exchange (IKE) describes a collection of key management schenmes. The main RFC is 7296.
3. **Conﬁdentiality**: There are many documents that describe and define the cryptographic algorithms for encryption, authentication, PRNGs. Two of these are described in RFC 4308.
4. **All of the above**
5. **None of the above**

**Collaboration:** None

**References:** Textbook, chapter 20

**11) 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?**

1. **SAD**: SAD is the Security Association Database. This database defines the parameters associated with each SA.
2. **SPD**: SPD is the Security Policy Database. The means by which IP traffic is related to specific SAs.
3. **SA**: SA is a Security Association. An SA is identified by the SPI, IP destination address, and the Security Protocol Identifier. It is a one-way relationship between a sender and a receiver that affords security services to the traffic carried on it.
4. **SPI**: SPI is the Security Parameters Index. A 32-bit unsigned integer assigned to the SA that allows the receiving system to select the correct SA.

**Collaboration:** None

**References:** Textbook, chapter 20

**12) 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.]**

1. **SPI**: SPI is the Security Parameters Index. A 32-bit unsigned integer assigned to the SA that allows the receiving system to select the correct SA.
2. **ESP**: The definition in the question is a direct quote from the textbook description of ESP. ESP stands for Encapsulating Security Payload.
3. **ISA**: ISA is the Internet Security Association. The ISAKMP provides a framework for internet key management.
4. **IPsec**: IPsec is a set of internet standards. These standards provide tge capability to secure communications across local, private, and public networks.

**Collaboration:** None

**References:** Textbook, chapter 20

**13) What is the term used for certiﬁed 802.11b products?**

1. **WAP**: WAP is wireless access point. A WAP provides access to the system via the wireless medium.
2. **WEP**: WEP is Wired Equivalent Privacy. This is the privacy portion of the 802.11 standard.
3. **WPA**: WPA is Wi-Fi Protected Access. It is a Wi-Fi standard introduced in order to accelerate the introduction of strong security into WLANs.
4. **Wi-Fi**: The WECA, renamed the Wi-Fi alliance created a test suite to certify 802.11b products as Wi-Fi. This has been extended to 802.11g and 802.11a products.

**Collaboration:** None

**References:** Textbook, chapter 18

**14) Which of the following is an umbrella term for managing access to a network?**

1. **NAS**: A Network Access Server’s function is as an access control point for remote users. This is not an umbrella term but a specific component of that system.
2. **NAC**: NAC, or Network Access Control, is an umbrella term for the system that manages access to a network. This system includes Access Requestors, Policy Server, and an NAS described above.
3. **ARQ**: Access requestors are the nodes that attempt to access the network. These may include workstations, servers, printers or other IP-enables devices.
4. **RAS**: A remote access server is another name for an NAS. It is an access control point for remote users of a network.

**Collaboration:** None

**References:** Textbook, chapter 16

**15) 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.**

1. **PKI**
2. **CDC**
3. **HMAC**
4. **KDC**

**Collaboration:** None

**References:** Textbook, chapter 14

X.509 certificates are public-key certificates that have a standardized structure and authentication protocols defined in ITU-T recommendation X.509. X.509 certificates each contain the public-key of a user and are signed with the private-key of a trusted certification authority. The certificates are placed in an X.500 directory for easy location by users.

In PKI, public-key infrastructure, X.509 is the basis for a formal model for deploying the certificate based infrastructure across the internet. The elements of the PKI X.509 model are the end entity (end user), the certificate authority (CA), the registration authority (RA), the CRL issuer (optional), and the repository (the directory).