Spring 2020
CYB 404 – NETWORK SECURITY
MIDTERM EXAM I
COVERSHEET

LAST NAME	MUSKU
FIRST NAME	KRUSHITH REDDY
NAU EMAIL	Km3248@nau.edu

Please only write your name and any other identifying information on this coversheet. This will allow me to grade your exam via a single-blind process.

I confirm that I have completed this exam using my own knowledge and have not committed any acts considered "academic dishonesty" according to the University's Academic Dishonesty Policy.

Krushith reddy
Signature:

2/7/2022
Date:

Instructions: Provide your answer to each question in the box below the question. The provided space should be more than enough for a complete answer. **If you are printing this PDF and writing your answers with pen or pencil, be sure to write very darkly and legibly so the scanned version with your answers appears clearly in Gradescope.**

You must upload your completed exam to BbLearn in a PDF. Failure to do so will result in a zero grade on your exam. You must also ensure that the uploaded PDF has the same page numbers and formatting as the blank exam form you download. Failure to do so will result in half the points from your exam being removed.

Q0. [10 pts] Describe the components of the CIA triad and the function that each plays in designing secure network architectures and protocols.

The CIA Triad is an information security model, which is widely popular. It guides an organization's efforts towards ensuring data security. The three principles—**confidentiality, integrity,** and **availability** which is also the full for CIA in cybersecurity, form the cornerstone of a security infrastructure. In fact, it is ideal to apply these principles to any security program. These core principles help identify problem areas and their security solutions and include:

Confidentiality: This is the principle of keeping sensitive information safe - protecting it from getting in the hands of the wrong people - or anyone who doesn't have permission to access it. It's about privacy and the safe handling of data. When developing information security policies, the confidentiality aspect of the CIA triad needs to define and classify what data needs to be protected, put in place measures to protect it, and manage access levels. Not all data will need to the most stringent protection levels and therefore it will need to be classified according to its' sensitivity and appropriate security and access controls put in place for different classifications.

Integrity: This principle refers to protecting information and data from modification or deletion by unauthorized individuals, and also ensuring that authorized changes made by mistake can be undone. Protecting the integrity of the data. In practical terms this could mean that certain users are able to view data but not modify it, or that some information cannot be modified at all. It also underlines the importance of recovery systems and backups that can allow data to be restored if changes are made inadvertently or rescinded later.

Availability: Finally, data needs to be readily available for those that need it - for business continuity - but at the same time ensuring it is not available for unauthorized users. This means that information security measures must not block authorized access to data; that systems, authentication tools and access channels work effectively. This core principle also applies to the measures taken to keep those channels working when incidents occur, for example a DDoS attack, power outages, and other worst-case scenarios.

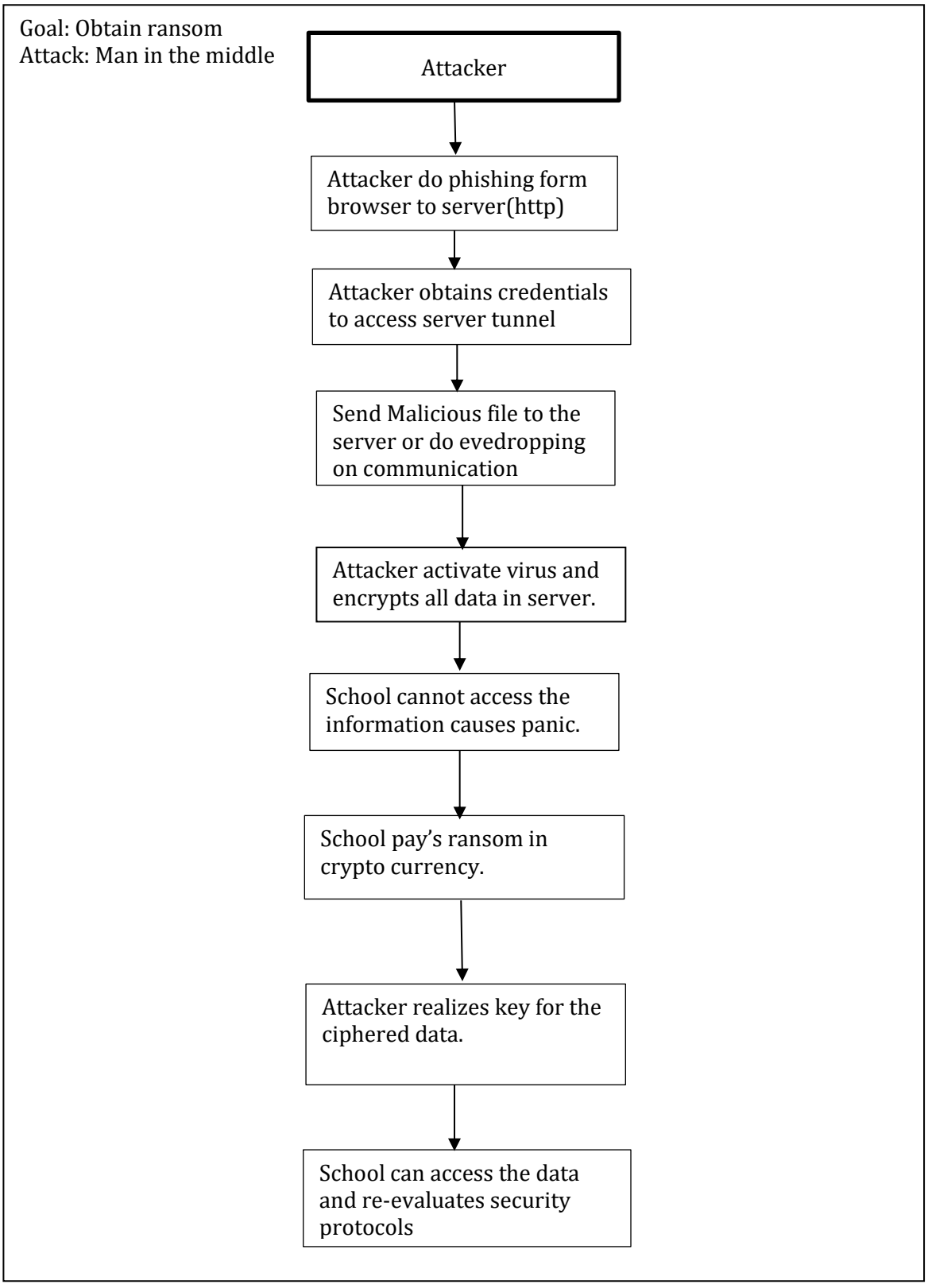
Q1. [5 pts] Why are Authenticity and Accountability added to the CIA triad? What do they add?

The CIA triad is a starting point and is not without limitations. There are a host of other key requirements including **authenticity** and **accountability** that relate to these core principals. However, by using these three core principals to build a secure network architecture the problems of bolting on security solutions later in the development of IT projects can be avoided. These additional concepts add:

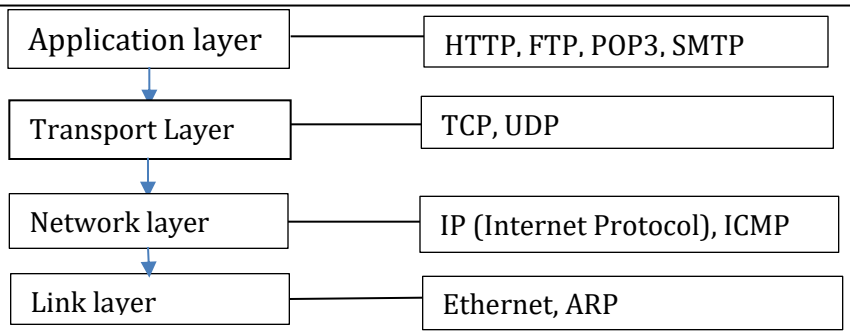
Authenticity - means verifying that users are who they say they are and that each input arriving at destination is from a trusted source. This principle if followed guarantees the valid and genuine message received from a trusted source through a valid transmission. For example, if take above example sender sends the message along with digital signature which was generated using the hash value of message and private key. Now at the receiver side this digital signature is decrypted using the public key generating a hash value and message is again hashed to generate the hash value. If the 2 value matches then it is known as valid transmission with the authentic or we say genuine message received at the recipient side

Accountability - means that it should be possible to trace actions of an entity uniquely to that entity. For example, as we discussed in Integrity section Not every employee should be allowed to do changes in other employees' data. For this there is a separate department in an organization that is responsible for making such changes and when they receive request for a change then that letter must be signed by higher authority for example Director of college and person that is allotted that change will be able to do change after verifying his bio metrics, thus timestamp with the user (doing changes) details get recorded. Thus, we can say if a change goes like this then it will be possible to trace the actions uniquely to an entity.

Q2. [15 points] Control over access to Student Information is a goal for many ransomware attacks on schools. Ransomware attacks usually involve encrypting target information and not releasing the decrypted information until a ransom is paid. Create an attack tree for NAU Student Information below.



Q03. [10 points] Draw and label the TCP/IP layer protocol stack. Describe the purpose of each layer. Discuss the importance of protocols for Internet communication.



The **internetwork layer** provides addressing and routing functions that ensures messages are delivered to their destination. Internet Protocol (IP) is the most important protocol in this layer.

The **link layer** is undefined in some ways, because it may consist of virtually any low-level network technology, including Ethernet, X.25, Point-to-Point Protocol (PPP), or whatever happens to be implemented on a particular network or subnet link. The link layer roughly equates to the data-link and physical layers of the OSI 7-layer reference model, and provides the interface with the underlying network hardware.

The **network layer** provides addressing and routing functions that ensures messages are delivered to their destination. Internet Protocol (IP) is the most important protocol in this layer. It is a connectionless, unreliable protocol that does not provide flow control or error handling, and attempts to deliver datagrams (in the form of IP packets) on a best-effort basis. Network devices called routers forward incoming datagrams according to the destination IP address specified within the IP packet. The internet layer corresponds more or less to the network layer of the OSI model. Other protocols at this layer include Internet Control Messaging Protocol (ICMP) and Internet Group Management Protocol (IGMP).

The **transport layer** oversees the end-to-end transfer of data, and can handle a number of data streams simultaneously. The main transport layer protocol is Transmission Control Protocol (TCP), which provides a reliable, connection-oriented service. User Datagram Protocol (UDP) provides an unreliable, connectionless service (delivery is not guaranteed, but UDP is useful for applications for which speed is more important than reliability). The transport layer roughly corresponds to its namesake in the OSI model.

An **application layer** protocol is specific to a particular type of application (e.g. file transfer, electronic mail, network management etc.) and is sometimes embodied within the application's client software, although it could also be implemented within the operating system software. The interface between an application layer protocol and a transport layer protocol is defined with reference to port numbers and sockets (more about this later). The application layer effectively combines the functionality of the application, presentation and session layers of the OSI model.

Each layer in the TCP/IP model handles a particular set of problems involving some aspect of sending data between distributed user applications, i.e. applications that are running on different computers, and often on different networks. Each of the lower three layers provides services to the layer immediately above it, while the application layer provides an interface between the user application above it and the communication-oriented layers below it. As the raw data moves from the application itself down through the various layers, it is wrapped up (or encapsulated) within protocol data units (PDUs) created by each of the protocols it encounters. The names commonly used to refer to these protocol data units tend to vary. At the internet layer, for example, they are called packets or datagrams. At the link layer, they are more often called frames.

Q04. [15 points] Kerberos was a significant improvement in authorization technologies. Is Kerberos alone sufficient for securing a network against unwanted infiltration? Defend your position, being sure to highlight the strengths and weaknesses of Kerberos.

Kerberos was created as a key distribution and user authentication system in response to three threats: the possibility that a user could gain access to a workstation and pretend to be another user operating from that workstation, the possibility that a user could alter the network from the impersonated workstation, and the possibility that a user could eavesdrop on exchanges and use a reply attack to gain access to a server or disrupt operations. An unauthorized user may be able to obtain access to services and data that he or she is not allowed to access under any of the aforementioned scenarios. Since a result, Kerberos comes in handy here, as it provides a centralized authentication server that authenticates users to servers and servers to users.

Strengths:

It provides various strengths as compared to the traditional authorization technologies E.g. The passwords of the user will never be sent across the network either encrypted to plaintext, mutual authentication of client and server system, reusable and durable authentications, open internet standards-based system.

Weakness:

There is also certain weakness associated with the Kerberos e.g. some versions of Kerberos use DES algorithm for encryption which was strong earlier but can be cracked now. Moreover, it was built for single-user client systems. So, it cannot support multi-user system. Finally, it is vulnerable to brute-force attacks and phishing attacks, so the passwords may be stolen.

Conclusion:

So, keeping in mind the weakness I described above, I believe that alone Kerberos is not enough for securing a network against unwanted infiltration, So, we can observe that multi-factor authentication is being used now for quite some time with Kerberos to protect identities with additional tokens.