UNIT 20: Network Meets Cryptography

Estimated Time in Hours: 5

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
2 Establishing Trust 7 Risk		- Use *traceroute* to discover the number of devices between their computer and a destination website. - Check the domain of the discovered IP addresses to find out who owns them. - Use Wireshark to view plaintext network traffic on non-HTTPS websites. - Make a case for or against the security of the Internet.

Guiding Questions:

- Where does your network traffic go after it leaves your computer? How can you track this?
- Who can see encrypted web traffic?
- Who can see unencrypted web traffic?
- Which parts of the CIA Triad can man-in-the-middle attacks violate?
- How does cryptography protect information on untrusted networks?
- What is the role of certificate authorities?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
7.2.4 LO: Students will be able to explain how the decentralized and dynamic nature of networked systems create the potential for a system to fail or behave incorrectly due a component the designer didn't even know existed.	• Computer, lecture slides, projector, graphic organizers, access to Internet • Windows *tracert* command, access to http://www.arin.net/whois/ , and a tutorial like:	• Ask students where their network traffic goes when they browser to a website. The obvious answer is to the website destination; however, where does it go in-between? • Explain that the Internet is built to facilitate communication. Security has become increasingly important, but it's not always there, and there's plenty of adversaries trying to steal your data.

7.2.4a EK: There are risks and mitigations associated with open systems like the Internet. 7.2.4b EK: Internet communication between a sender and receive relies on a number of systems that are not controlled by the sender or receiver. This can include the hardware and software at the sender and the sender's edge network. It includes a number of supporting systems such as the DNS and certificate authorities, and any number of intermediate networks. It can also include the receiver's edge network as well as the hardware and software at the receiver.	"Lab 1.2.3 Mapping ISP Connectivity Using Traceroute." Cisco | Networking Academy, https://web.nmsu.edu/~jbeasley/Cisco_Discovery_4-1/courses/en0500000000/en0501000000/en0501020000/en0501020300/en0501020303/cm6042232704/lab.pdf	• Let students experience this first-hand using *traceroute* to identify the computers between their system and a destination website.
7.2.4c EK: Incorrect assumptions about the network can result in the loss of confidentiality by sending data to an imposter or sending data over a path where it can be observed.	• Wireshark and access to non-HTTPS website. Lists of these can be found online; however, they are becoming more rare to find – this is a good thing. Websites with unencrypted images make for an excellent use case as students can find	• Explain the dangers of sending traffic over insecure connections. • Have students use Wireshark to visit non-HTTPS websites and observe the plaintext traffic. • Explain or review man-in-the-middle attacks as another method to snoop on traffic.

	the links to those pictures in Wireshark. • Man-in-the-Middle Attack overview: "What Is a Man-in-the-Middle Attack?" *YouTube*, uploaded by Hacksplaining, 4 Mar 2017, https://www.youtube.com/watch?v=DgqID9k83oQ	
7.2.4d EK: Network vulnerabilities can result in the loss of integrity if data is sent to an imposter acting as a "monkey-in-the-middle" or when data is sent over a path where it can be changed.		• Ask students if the man-in-the-middle attack can be used other ways. • A man-in-the-middle who can intercept all web traffic from the victim can then change the traffic mid-transit to violate the integrity.
7.2.4e EK: Network vulnerabilities can result in the loss of availability by directing the sender to an invalid destination or sending data over a path where it can be dropped.	• Man-in-the-Middle availability attack against a drone: "DoS by man-in-the-middle attack." *YouTube*, uploaded by Mehdi Karimi, 3 Mar 2019, https://youtu.be/SrJvO4RwMUQ	• If an adversary can view and alter traffic, what else can they do? They can drop traffic and prevent it from reaching its destination. • Ask students which parts of the CIA Triad a man-in-the-middle attack violates.

7.2.4f EK: Cryptography can be used to prevent imposters and protect data so only authorized entities can view it. 7.2.4g EK: Cryptography can be used to identify the creator of a message and show a message was not modified in transit (hash function).		• Ask students the best way to protect themselves when using the Internet. • Cryptography is the best solution as it prevents any parties in the middle from viewing data. • Asymmetric cryptography can also provide integrity and authentication to prevent man-in-the-middle attacks. • Review protocols secured with cryptography.
7.2.4h EK: Certificate authorities play a role in asserting the identities.	• Certificate Authority explanation and demonstration in the face of man-in-the-middle attacks: Challen, Geoffrey. "What is a certificate authority?" *YouTube*, uploaded by internet-class, 17 Oct 2016, https://youtu.be/8ItJ-VqYo_s	• Review Certificate Authorities as the trusted third-parties who ensure communications are secure. • Explain the importance of a certificate and why they must be legitimized by a certificate authority. • Show the linked YouTube video and use a video viewing guide to assess learning. • Ask students what would happen if a certificate authority was compromised?
7.2.4i EK: Cryptography does not solve operational challenges and cryptography alone is not a solution in a decentralized network.		• Review that cryptography is an important piece of the solution, but not necessarily a catch-all. • The environment's security (e.g., CAs, PKIs) is also paramount.
2.3.6 LO: Students will know that the principle of data hiding is		• Review the principle of data hiding.

about allowing only necessary aspects of a data structure or a record to be observed or accessed. 2.3.6a EK: Data hiding can help prevent users/programmers/processes from updating/changing data in invalid ways or by mistake.		• Ask students to describe how data hiding applies to man-in-the-middle attacks. • Ask students to explain how data hiding applies to certificate authorities. • As an independent assignment, task students with making a case for whether or not the Internet is secure. How can they back up this claim?
8.1.1h EK: Cybersecurity events have led to the development of various cybersecurity career paths and various needs in order to prepare people for these new types of jobs.		• Explore a relevant career, such as cyber operator.