UNIT 15: Network Standards & Protocols

Estimated Time in Hours: 8

Big Idea(s) 2 Establishing Trust 3 Ubiquitous Connectivity	Enduring Understandings	Projects & Major Assignments - Use nslookup to test their understanding of DNS. - Research, identify, and categorize open-source and proprietary protocols.

Guiding Questions:

- How are protocols different from standards?
- What is the purpose of DNS?
- What is the value of open-source protocols?
- Are proprietary protocols necessarily more secure?
- What is security by obscurity? Is it effective?
- How do protocols implement minimization?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
3.1.2 LO: Students will explain how network standards and protocols allow different types of devices to communicate.	• Computer, lecture slides, projector, graphic organizers, access to Internet • Reference comparison between protocol and standard: • Rusev, Emanuil. “What’s the difference between the terms ‘protocol’ and ‘standard’?” Stack Exchange | Software Engineering,	• Differentiate standards vs protocols here. Protocols are like languages, while standards are like dictionaries.

	StackExchange.com, 2 Sept 2011, https://softwareengineering.stackexchange.com/questions/105449/whats-the-difference-between-the-terms-protocol-and-standard	
3.1.2a EK: Communication protocols define the rules, types, and formats of messages exchanged between devices and are necessary to allow devices to communicate with each other.	• Simple protocol explanation: "Computer Networking Tutorial – 10 – What is a Protocol?" *YouTube*, uploaded by thenewboston, 11 Dec 2012, https://youtu.be/VlKksZhI0	• Ask students to list protocols they know about: TCP, UDP, HTTP, HTTPS etc. • The YouTube video linked to the left is a simple explanation of how a protocol works.
3.1.2b EK: Protocols like the Domain Name System (DNS) provide a mechanism to map names like "www.example.com" into numbers (IP addresses), similar to a phonebook that maps names to phone numbers.	• DNS overview: "How a DNS Server (Domain Name System) works." *YouTube*, uploaded by PowerCert Animated Videos, 26 May 2016, https://youtu.be/mpQZVYPuDGU • Activity: use the command window tool	• Explain how DNS is a useful protocol used for navigating to websites without knowing its IP address. • Show the YouTube video linked to the left and use a video viewing guide to assess learning. • Challenge students by having them use *nslookup* to identify domain names or their corresponding IP addresses.

	nslookup to check the DNS-mapped IP addresses of domain names. Examples: "Using Nslookup." Get Certified Get Ahead, *gcgapremium.com*, https://gcgapremium.com/using-nslookup/	
3.1.2c EK: Some protocols are proprietary and are available only to authorized users while other protocols are published as formal standards and allow devices from any manufacturer to communicate with each other. 3.1.2d EK: Some standards are open standards where the packet format and message exchange rules are available to everyone. In other standards called proprietary standards, the message formats and message exchange rules are only provided to authorized entities.		• Contrast open-source vs proprietary software. • Open-source software gets a larger pool of supporters who can review and suggest changes to the source code. Ask students if this is a good thing or bad thing. Does it enhance security? • Explain how open-source protocols are often more popular because they can be implemented freely and often more easily than proprietary counterparts. • As a research project, have students identify protocols that are open-source and proprietary.
3.1.2e EK: When designers rely on secrecy, assuming an adversary cannot compromise the system because the adversary cannot determine how	• Security by obscurity analogy: "Security via Obscurity Is a Bad Idea." *YouTube*,	• Explain the misconception of "security by obscurity." For example, you may be tempted to hide an insecure service by changing its port number; however, adversaries can

the system works is known as security through obscurity. It is widely accepted that security through obscurity should never be your only security mechanism.	uploaded by Phil Koopman, 10 Nov 2018, https://youtu.be/FR9YZlmeojY	still detect the actual service running on the misleading port number. • Ask students if leaving a key under your doormat is secure. Adversaries know how to check there, but in cyberspace they also have the capability to write a script to check under door mats for them. See the video for a full explanation of this analogy.
3.1.2f EK: Cryptographic algorithms are either publicly known or proprietary. The use of proprietary cryptographic algorithms is largely discredited, as evidenced by organizations like NIST, which encourages public review of algorithms.		• Ask students if cryptographic algorithms should be public or private knowledge. • Explain the security of cryptography lies in the power of the algorithm, not its secrecy. The process of encryption is not secret, only the key and plaintext should be secret.
3.1.2g EK: Through experiments, an adversary can often learn how proprietary protocols or algorithms work even though the adversary is not an authorized user.		• Why does it not help to keep the protocol/algorithm secret? • Adversaries can use the tactic of reverse engineering to discover how the algorithms function. Keeping it secret does not protect it. • Note that when software is open-source or public, the community's feedback can help make it more secure or reveal its flaws for patching.
2.2.3 LO: Students will apply the principle of minimization by decreasing the number of ways		• Ask students why there are so many protocols.

in which attackers can exploit a program or device. 2.2.3a EK: The attack surface of a software environment is the sum of the different points where an unauthorized user can try to enter data or to extract data from an environment. 2.2.3b EK: Minimizing the attack surface decreases the opportunity to find an exploitable vulnerability in the system. 2.2.3c EK: The human interface should be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. 2.2.3d EK: Common mechanisms and access should be minimized.		• Protocols should be fairly narrow-focused to follow the principles of minimization. By following rules and a narrow use-case, minimization allows protocols to lower possible attack vectors. • Review the principle of minimization. • What is the purpose of HTTP? To provide web pages. • What is the purpose of FTP? To transfer files. • What is the purpose of RDP? Command and control a computer remotely. • Explain how in the case of complicated protocols, they often borrow features from other protocols. For example, HTTPS uses the SSL/TLS protocol to provide security for web browsing.
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 defense incident responder.