UNIT 11: Authentication and Identity Management

Estimated Time in Hours: 7

Big Idea(s)	Enduring Understandings	Projects & Major Assignments
4 Data Security 6 Adversarial Thinking 2 Establishing Trust	4.2	- Research the pros and cons of biometrics. - Examine where browsers store passwords. - Research password managers. - Explore user permissions on a Windows system.

Guiding Questions:

- What is identity and access management?
- Why should passwords be complex?
- What are the types of biometrics?
- What is multi factor authentication?
- What are single sign-on, federation, and transitive trust?
- Where are passwords stored?
- What are different types of access control?
- What is least privilege?
- What are groups, roles, privileges, & permissions?
- What are some dangers of social engineering?

Learning Objectives & Respective Essential Knowledge Statements	Materials	Instructional Activities and Classroom Assessments
4.2.3d EK: Identity management includes authentication, access control, sometimes coordination across different domains, and management of the credentials throughout the lifecycle.	• Computer, lecture slides, projector, graphic organizers, access to Internet	• Provide the definition of identity management. Include identification, authentication, authorization, and accountability. A graphic organizer to help students differentiate among the terms is suggested, as these are terms students often confuse. • Take time to discuss each term and provide examples.
4.2.3a EK: Authentication is a process by which you verify that	• "Complex Passwords Harder to Crack, but It May Not Matter."	• Explain how passwords are a form of authentication. Discuss with students the characteristics of good passwords.

someone is who they claim they are. 4.2.3f EK: The strength of a password is a function of length, complexity, and unpredictability.	InetSolution blog, *inetsolution.com*, https://www.inetsolution.com/blog/june-2012/complex-passwords-harder-to-crack,-but-it-may-not • *How Secure Is My Password?* https://howsecureismypassword.net/	• Show students how easily passwords can be cracked. This can be by using a password cracker that you demo or using a chart like the one linked to the left. • Explain why password length matters (search space). • Discuss dictionary attacks. • Using How Secure Is My Password (linked on the left). Have students craft their own strong passwords.
6.1.4a EK: Human users of the system have their own conscious and unconscious objectives that can undermine cybersecurity protections and policies.	• "Password Minder Infomercial featured on Ellen." *YouTube*, uploaded by Consumer Affinity, Inc., 2 Jan 2019, https://www.youtube.com/watch?v=2HYmojdDweI&feature=emb_logo	• Show the video linked left about the Password Minder. Explain that this was a real product. Ask students their thoughts. Is it a good or bad idea? Why? • Have students list (or research) bad password habits that weaken security.
4.2.3c EK: Authentication can be done using multiple factors, something you have, something you know, something you do, & something you are. (E.g., have = card, know=password, do=sign, walk, are=fingerprint, retina)		• After discussing biometrics as a way to authenticate, have students research different types of biometric authentication. How does this strategy compare to passwords? • Discuss biometric related errors. • Discuss how users can authenticate using something they have.

		• Review authentication strategies something you know, are, or have. • Discuss multi factor authentication.
4.2.3 LO: Students will evaluate and recommend technical controls that can be used to secure data. 6.1.4 LO: Students will understand how social behaviors and human factors impact the cybersecurity of a system design	• Teravainen, Taina and Rouse, Margaret. "single sign-on (SSO)." TechTarget|SearchSecurity, *SearchSecurity.com*, https://searchsecurity.techtarget.com/definition/single-sign-on • Sheldon, Robert. "Explore the pros and cons of identity federation management." TechTarget|SearchMobileComputing, *SearchMobileComputing.com*, 23 Feb 2018 https://searchmobilecomputing.techtarget.com/tip/Explore-the-pros-and-cons-of-identity-federation-management • "QTNA #19: Transitive Trust." *YouTube*,	• Explain single sign-on to students. Ask students if they have ever used single sign-on. Have them list the advantages and disadvantages (see article linked left). • Contrast single sign-on with federation. Have students provide examples of federated accounts. Have students research the advantages and disadvantages to account federation (see source linked left). • Discuss transitive trust. The video linked left may help with this.

	uploaded by CyberVista, 20 June 2018, https://www.youtube.com/watch?v=uWifmuVOcLw&feature=emb_logo	
4.2.3b EK: Authentication requires a database of information.		• Ask students where passwords are stored. Explain that passwords have to be stored in a database somewhere. How can this be a vulnerability? • Have students investigate where browsers and Windows store passwords.
4.2.3g EK: Authorization is the process of establishing if the authenticated user, is permitted to have access to and/or act on a resource.		• Explain the concept of authorization. Compare it to their household. Does everyone in the house have the same authority (rights and privileges)? • Authorization is what you are allowed to do.
4.2.3i EK: Access Control is the process of enforcing the required security for a particular resource.		• Have students review the types of access controls from the previous units (MAC, DAC, RBAC, RuBAC). Review nondiscretionary and discretionary.
2.3.4a EK: A privilege is a right for the user to act on managed computer resources.	• "Unix / Linux – File Permission / Access Modes." tutorialspoint, *tutorialspoint.com*, https://www.tutorialspoint.com/unix/unix-file-permission.htm	• Review types of user privileges. The article linked left may help with this.
2.3.4 LO: Students will explore the principle of least privilege, which is about differentiating	• "What Is Privilege Escalation?" *YouTube*,	• Explain the concept of least privilege. Why is it important? Have students think of situations when least

among types of access control (mandatory, role-based, discretionary, and rule-based access controls) and analyzing which to use for selective restriction of access to a place or other resource. 2.3.4b EK: Least privilege is the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities.	uploaded by Netwrix, 10 Jul 2018, https://www.youtube.com/watch?v=7PpYavvu-6k	privilege should be used. The video linked left is a resource for this concept.
4.2.3h EK: Groups, Roles, Privileges and Permissions are used to manage authorization.		• Explain groups, roles, privileges, and permissions. It is a good idea to map out how they relate.
4.2.3j EK: Failure to protect data can be due to faulty authentication, faculty authorization, and/or faulty access control.		• Discuss with students that these measures can fail. Have them use a Windows system to explore authorization.
2.3.4c EK: Granting only those privileges necessary for a user to accomplish assigned duties improves accountability and limits accidental misuse.		• Have students think back to their home. What happens if they do not do their chores? This is called accountability. Ask students how misuse can be spotted on a computer system. Discuss logging.

6.1.4b EK: Social engineering is one of the most widely used techniques in which an adversary compromises a system by convincing a human to violate the security policies in a way that enables the adversary to gain an advantage.	• "How to Spot a Phishing Email Attack – 5 key steps for 2020. SpamTitan from TitanHQ." *YouTube*, uploaded by TitanHQ Email Security and Web Security., 4 Dec 2019, https://www.youtube.com/watch?time_continue=34&v=P2TQmCcfD7Q&feature=emb_logo • @stewy6. "So I'm using Instagram's Question Stickers to ask ppl common password recovery questions, and most are actually responding #privacy @CryptoAustralia." *Twitter*, 23 July 2018, 2:03 a.m., https://twitter.com/stewy6/status/1017650779044265986	• No matter what controls are in place, a system is still vulnerable to social engineering. Discuss phishing and other techniques with students. Use the video linked on the left to guide discussion. • Show students the Tweet linked left. How does this link to passwords/password recovery?
8.1.1h EK: Cybersecurity events have led to the development of various cybersecurity career paths and various needs in order		• Discuss a potential related career path with students. Perhaps systems administrator.

to prepare people for these new types of jobs.		