IDENTITY, AUTHENTICATION, AND AUTHORIZATION

Nancy Stevens, First Flight High School, Kill Devil Hills, NC

This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.

Additional materials may be found at www.ncyte.net

IDENTITY, AUTHENTICATION AND AUTHORIZATION

Students will:

1) explain concepts of identity, authentication, and authorization,
2) describe ways in which attackers gain unauthorized access to systems and data, and
3) identify aspects of for passwords, multifactor authentication, and the concept of least privilege as security controls for protecting information assets and computing resources.

OVERVIEW

Prerequisite Knowledge: Students should be familiar with phishing and the concepts of confidentiality, integrity, availability (CIA Triad).

Length of Completion: The CCL is designed to take approximately 100-150 minutes.

Learning Setting: Traditional face-to-face setting or a blended classroom.

Lab Environment: Students need access to several websites for exploration and research.

Activity/Lab Tasks: Students investigate the scope of credential-based attacks in the first lesson. They conduct online research and investigate methods used to gain unauthorized access to data and devices. The second lesson explores authentication and authorization measures. Password selection, password strength, and multifactor authentication are examined. The concept of least privilege is introduced. Students create a digital artifact to illustrate their understanding of password security.

1) IdentificationAuthenticationAuthorization_Overview.docx
2) IdentityAuthenticationAuthorization_Presentation.pptx
3) IdentityAuthenticationAuthorization_IdentityCrisis_Activity.docx
4) IdentityAuthenticationAuthorization_IdentityCrisis_Activity_Solutions.docx
5) IdentityAuthenticationAuthorization_LetMeIn_Activity.docx

LEARNING OBJECTIVES AND AP CSP ALIGNMENT

LESSON LEARNING OBJECTIVES

Students will

1) understand ways in which attackers gain unauthorized access to systems and data
2) understand ways to protect devices and data
3) distinguish between authentication and authorization
4) identify three types of Multifactor authentication (knowledge, possession, inheritance)
5) describe what defines a strong password

ASSOCIATED AP CSP SUB LEARNING OBJECTIVES

AP COMPUTER SCIENCE PRINCIPLES COURSE, BIG IDEA 5: IMPACT OF COMPUTING

LO IOC-2.B Explain how computing resources can be protected and can be misused.

- IOC-2.B.1 Authentication measures protect devices and information from unauthorized access. Examples of authentication measures include strong passwords and multifactor authentication.
- OC-2.B.2 A strong password is something that is easy for a user to remember but would be difficult for someone else to guess based on knowledge of that user.
- IOC-2.B.3 Multifactor authentication is a method of computer access control in which a user is only granted access after successfully presenting several separate pieces of evidence to an authentication mechanism, typically in at least two of the following categories: knowledge, possession, and inheritance.
- IOC-2.B.4 Multifactor authentication requires at least two steps to unlock protected information; each step adds a new layer of security that must be broken to gain unauthorized access.

LO IOC-2.C Explain how unauthorized access to computing resources is gained.

- IOC-2.C.2 Keylogging is the use of a program to record every keystroke made by a computer user in order to gain fraudulent access to passwords and other confidential information.
- OC-2.C.3 Data sent over public networks can be intercepted, analyzed, and modified. One way that this can happen is through a rogue access point.
- IOC-2.C.4 A rogue access point is a wireless access point that gives unauthorized access to secure networks.

- IOC-2.C.5 A malicious link can be disguised on a web page or in an email message.
- IOC-2.C.6 Unsolicited emails, attachments, links, and forms in emails can be used to compromise the security of a computing system. These can come from unknown senders or from known senders whose security has been compromised.

LESSON DETAILS

Overview of Lessons: There are two lessons.

- Lesson 1 Identity Crisis
- Lesson 2 Let Me In

LESSON 1 IDENTITY CRISIS

- 2) IdentityAuthenticationAuthorization_Presentation.pptx
- 3) IdentityAuthenticationAuthorization_IdentityCrisis_Activity.docx
- 4) IdentityAuthenticationAuthorization_IdentityCrisis_Activity_Solutions.docx

Upon completion of this lesson: Students will understand ways in which attackers gain unauthorized access to systems and data.

The PowerPoint slides guide the lesson as it progresses from the warmup activity to a research activity. Students explore identification, authentication, and authorization. They explore how credential-based attacks are used to gain unauthorized access to systems and data.

Warm Up: Students will think to themselves and answer three questions: How do people know who you are? How do you prove who you are? What are some examples of access based upon proving your identity? Provide students with a few moments to think about these questions and then ask students to share. The warmup prompts explore the concepts of identification, authentication, and authorization. Spend only about 10 minutes on this activity.

Lesson: The first lesson explores the concepts of identification, authentication, and authorization. Examples and statistics on data breaches are provided in the PowerPoint slides to help students understand the scope of credential-based attacks. The learning activities include checking whether student email accounts have been involved in a data breach and examining a timeline visualization of major data breaches. A research activity explores the means used to gain unauthorized access to devices and data. Additionally, students will read an article on password sharing and discuss (whole group, small group, think/pair share, or journal) questions regarding cyber ethics.

Active Learning Activity: There are three learning activities in this lesson. All of the activities require access to websites for exploration or research. Students can

check their email accounts on the website, https://haveibeenpwned.com/, to see if they have been involved in a data breach. The website, https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/, provides a timeline and visualization of major data breaches. The third activity requires students to research definitions of some of the methods used to gain unauthorized access to data and devices.

LESSON 2 LET ME IN

- 02.IdentityAuthenticationAuthorization_Presentation.pptx
- 05.IdentityAuthenticationandAuthorization_LetMeIn_Activity.docx

Upon completion of this lesson, students will:

1) understand ways to protect devices and data;
2) distinguish between authentication and authorization
3) identify three types of Multifactor authentication (knowledge, possession, inheritance)
4) describe what defines a strong password

Following the first lesson's exploration of identification, authentication, and authorization, students will explore password selection and multifactor authentication. Control measures are investigated as a means of protection.

Warm Up: Students construct the meaning of authenticity by defining the term, authentic, and then listing synonyms and antonyms.

Lesson: The second lesson explores authentication, authorization, and protection measures. Multifactor authentication is introduced as authentication by knowledge, possession, or inherence. The concept of least privilege provides a means to limit attackers.

Active Learning Activity: This Federal Trade Commission website (https://www.consumer.gov/articles/1015-avoiding-identity-theft) is included in the slide deck for students to explore security controls for identity theft.

Active Learning Activity: The learning activities focus on the concepts of authentication, authorization, least privilege, and protective measures. The NIST guidelines for passwords are examined. Students will need access to these websites:

- https://www.random.org/passwords/
- https://howsecureismypassword.net/
- http://www.passwordmeter.com/
- https://www.us-cert.gov/ncas/tips/ST04-002

Students will create a digital artifact using a one-pager template to demonstrate their understanding of password security.

ACKNOWLEDGEMENTS

 This material is based upon work supported by the **National Science Foundation** under Grant No.1548315.