Fundamentals of Information Security Series

C836

Instructor: Arthur Moore

Event time: Every Thursday at 6:00PM MST

WESTERN GOVERNORS UNIVERSITY

ONLINE. ACCELERATED. AFFORDABLE. ACCREDITED.

Instructor intro

- Contact info: Arthur.Moore@wgu.edu
- Number: 1-877-435-7948 Ext. 1554
- Office Hours:
- Monday: 8AM-5PM
- Tuesday: 8AM-5PM
- Wednesday: 8AM-5PM
- Thursday: 8AM-12PM AND 7PM-10PM
- Sunday: 6PM-10PM

As a reminder

- This web series is only to enhance/supplement the course material not to replace it please follow the guidelines as posted below.
- ***It's Highly recommended that you Don't schedule the first assessment until all the materials are covered***.
- -take the preassessment until constantly passing
- -review lessons 1-14 readings (pay close attention to chapters 1 – 6.)
- -complete lessons 1-14 quizzes.
- -complete lessons 1-14 exercises (pay close attention to chapters 1 – 6)
- -watch the videos that are posted in the course tips
- -go over the PowerPoints that are posted in the course tips

Identify and Authenticate

- Identity is who or what we claim to be.
- Authentication is the act of providing who or what we claim to be.
- Example a username is an Identity claim and the password authenticates that user and allows access.
- Identity verification is the half step between Identity and Authentication.
- Think of Identity verification as showing 2 forms of ID for a service.

Authentication

- Authentication comes in 5 different types.
- Something you know: Username/Password/Pin
- Something you have: ID badge/swipe card/OTP
- Something you are: Fingerprint/Iris/Retina scan
- Somewhere you are: Geolocation
- Something you do: handwriting/typing/walking

Authentication Continued

- Single/Dual/Multifactor and the examples of mixing the various types of Authentication.
- Single factor: one factor
- Dual factor: two different factors (2 of the same factor does not count)
- Multifactor: three or more factors (2 of the same factor does not count)

Mutual Authentication

- Mutual Authentication: is not the same as multifactor authentication.
- Mutual Authentication is the process where the session is authenticated on both ends and just one end. The event prevents man in the middle attacks.
- Example both the PC and server authenticate each other before data is sent in either direction.
- The man in the middle attack is where the attacker inserts themselves into the traffic flow.

Passwords (Something you know)

- Passwords are the most common form of Authentication.
- Passwords are very vulnerable if created without complexity requirements.
- Complexity requirements include numbers, letters capital/lower case, and special characters.
- Brute force attacks against passwords are when all possible combinations are used to guess the password.
- Password managers are programs that store all of the user’s passwords with a master password.
- Manual password synchronization is when a user synced passwords from different systems without a software application.

Biometrics (Something that you are)

- Biometrics are Authentication factors that uses physical features.
- Biometrics are defined by 7 features universality, uniqueness, permanence, collectability, performance, acceptability, and circumvention
- Universality: stipulates that we should be able to find our chosen biometric characteristic in the majority of people we expect to enroll in the system.
- Uniqueness: is a measure of how unique a particular characteristic is among individuals.
- Permanence: tests show how well a particular characteristic resists change over time and with advancing age.
- Collectability: measures how easy it is to acquire a characteristic with which we can later authenticate a user.
- Performance: is a set of metrics that judge how well a given system functions.
- Acceptability: is a measure of how acceptable the particular characteristic is to the users of the system.
- Circumvention: describes the ease with which a system can be tricked by a falsified biometric identifier.

Hardware Tokens (Something that you have)

- Hardware tokens: Physical devices that generate a one-time password (OTP)
- Software tokens: Applications that generate OTP.
- One Time Passwords: Passwords that expire after a time frame or after one-time usage.