Access Control

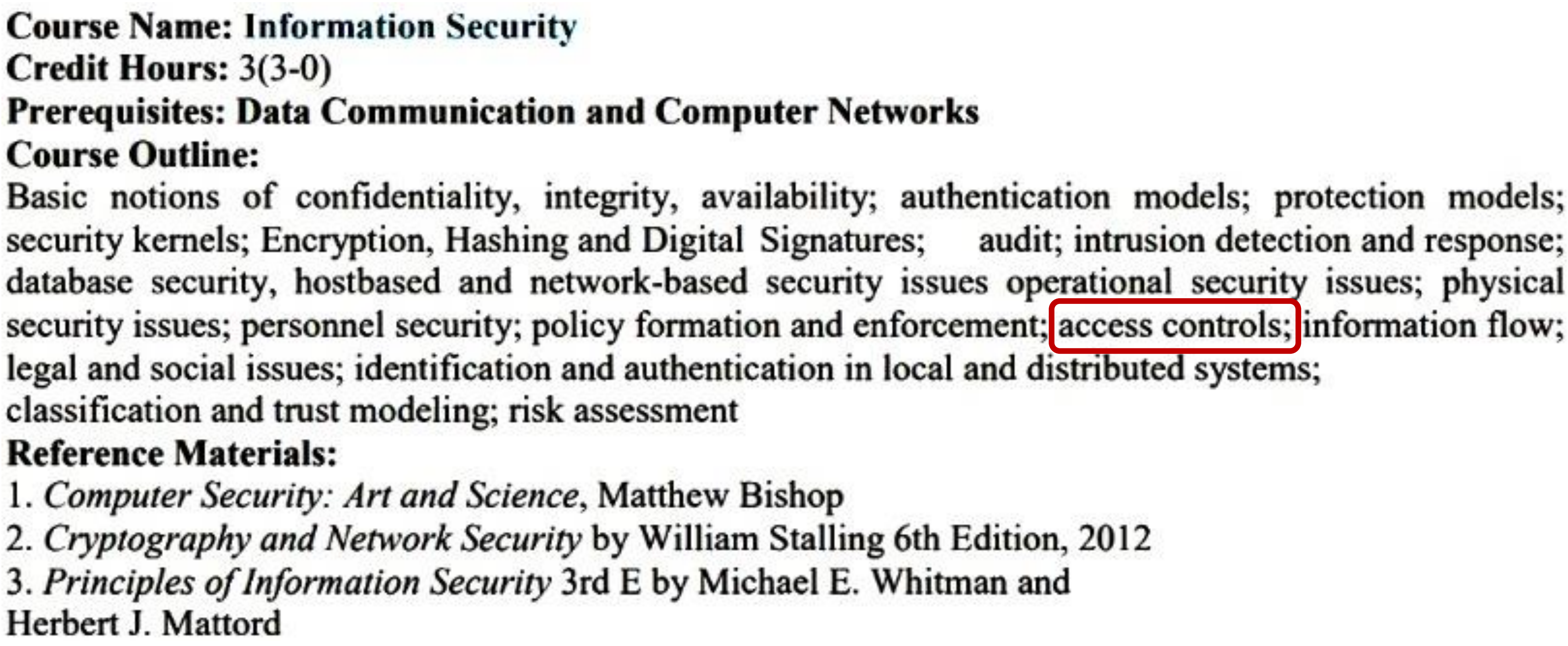
CSI-604 - Information Security

ArfanShahzadTech

WhatsApp-Contact Us
0345-5922495

ArfanShahzad.com

Course Outline



Course Name: Information Security
Credit Hours: 3(3-0)
Prerequisites: Data Communication and Computer Networks
Course Outline:

Basic notions of confidentiality, integrity, availability; authentication models; protection models; security kernels; Encryption, Hashing and Digital Signatures; audit; intrusion detection and response; database security, hostbased and network-based security issues operational security issues; physical security issues; personnel security; policy formation and enforcement; access controls; information flow; legal and social issues; identification and authentication in local and distributed systems; classification and trust modeling; risk assessment

Reference Materials:

1. *Computer Security: Art and Science*, Matthew Bishop
2. *Cryptography and Network Security* by William Stalling 6th Edition, 2012
3. *Principles of Information Security* 3rd E by Michael E. Whitman and Herbert J. Mattord

Access Control

- Access control is a ***critical component*** of **information security** that governs ***who is allowed to access*** specific ***resources***, ***systems***, or ***data*** within an organization.
- It **encompasses** a set of ***policies***, ***procedures***, ***technologies***, and ***practices*** that **regulate** and **restrict** ***access*** to ***protect sensitive information***, ***prevent unauthorized activities***, and **maintain** the ***confidentiality***, ***integrity***, and ***availability*** of data.

Access Control cont…

- Access control is a fundamental concept in cybersecurity and plays a vital role in safeguarding an organization's digital assets.
- Here are key aspects of access control:

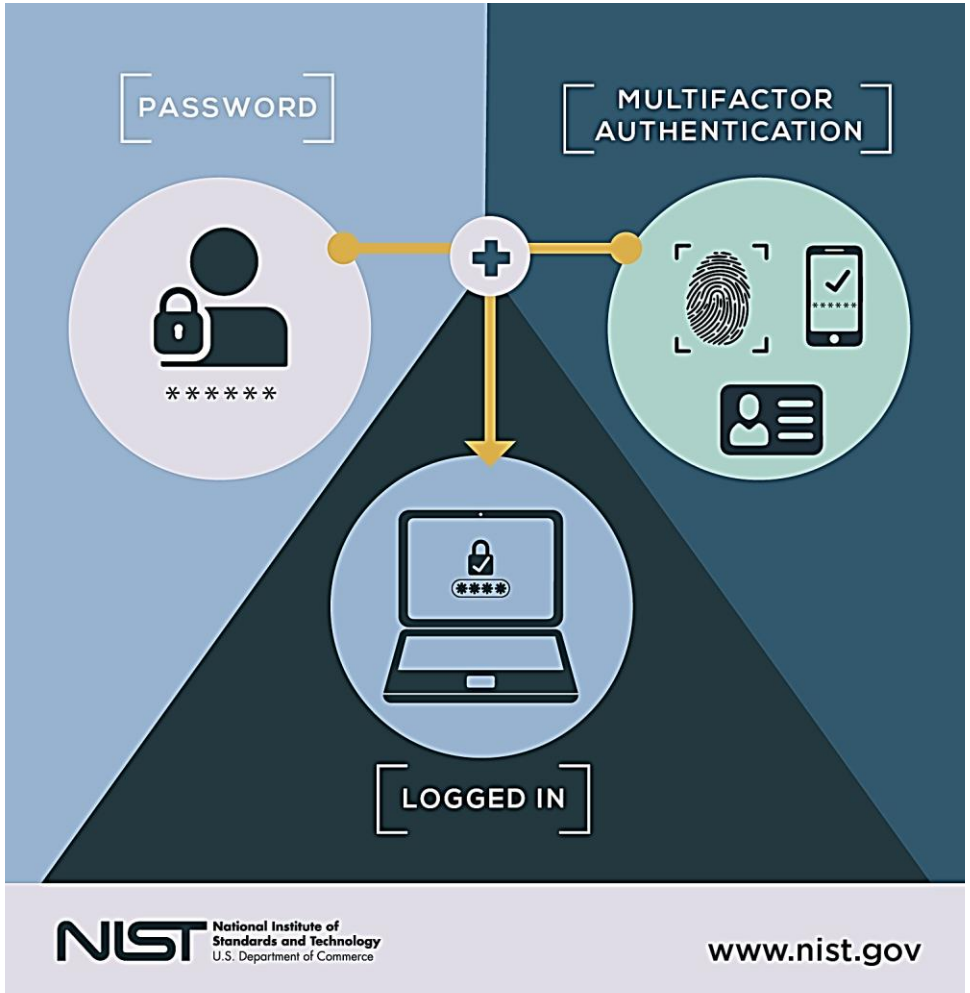
Access Control cont…

- **Identification:** Access control starts with the **identification** of ***users*** or ***entities*** ***seeking access*** to a ***system*** or ***resource***.
- This process typically involves the use of unique identifiers such as ***usernames***, ***employee IDs***, or ***biometric data*** (e.g., fingerprint or facial recognition).

Access Control cont…

- **Authentication:** Once **identified**, users must ***prove their identity*** through ***authentication methods***.
- Common authentication factors include:
- Something you know (passwords),
- Something you have (smartcards or tokens), or
- Something you are (biometrics).

Access Control cont…


PASSWORD
******
MULTIFACTOR AUTHENTICATION
LOGGED IN
NIST National Institute of Standards and Technology U.S. Department of Commerce
www.nist.gov

Access Control cont…

- **Authorization:** After authentication, the system determines **what *actions*** or ***resources the authenticated user is allowed to access***.
- Authorization is based on **predefined policies** and **permissions**.
- ***Role-based access control*** (RBAC) and ***attribute-based access control*** (ABAC) are common models used for authorization.

Access Control cont…

- **Access Control Models:** Different access control models define how permissions are granted and managed.
- The most common models are ***discretionary access control*** (DAC), where resource owners determine access, and ***mandatory access control*** (MAC), where access is determined by system administrators based on classification levels.

Access Control cont…

- **Access Control Lists (ACLs):** ACLs are lists associated with resources, specifying the users or groups allowed or denied access and the type of access they have (read, write, execute).
- They are commonly used in file systems, network devices, and databases.

Access Control cont…

- **Access Control Policies:** Organizations define access control policies to determine how access is granted or denied based on rules and conditions.
- Policies consider factors like user roles, data sensitivity, and the context of access attempts.

Access Control cont…

- **Access Control Mechanisms:** Technologies like firewalls, IDS, IPS, etc. enforce access control by monitoring and filtering network traffic based on predefined rules.
- **Physical Access Control:** Physical access control restricts entry to buildings, rooms, and facilities.

Access Control cont…

- **<u>Privilege Escalation:</u>** Ensuring that users cannot escalate their privileges beyond what is necessary for their tasks is crucial.
- This prevents unauthorized access and potential abuse.

Access Control cont…

- **Continuous Monitoring:** Regularly monitoring access attempts and permissions helps detect anomalies or unauthorized access.
- Logging and auditing access events contribute to accountability and security incident investigation.