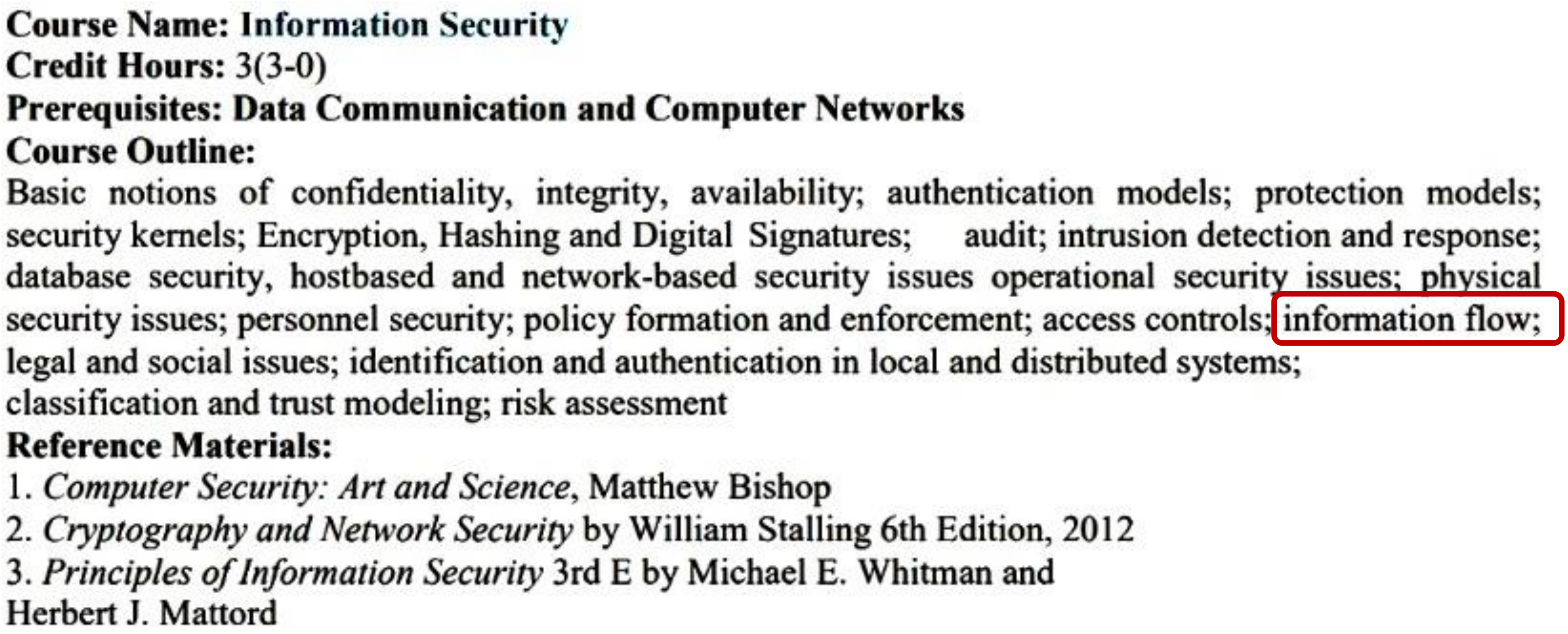
Classification & Trust Modelling

CSI-604 - Information Security

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

Classification and Trust Modelling

- Classification and trust modeling play crucial roles in information security, helping organizations make informed decisions about access control, threat detection, and overall security posture.
- Let's explore how these concepts are applied in information security:

Classification and Trust Modelling cont…

Classification in Information Security

- **Access Control:** Classification is often used to categorize users, devices, or processes into different security clearance levels or roles.
- This allows organizations to control access to sensitive resources based on the classification of entities.
- For example, in military or government contexts, information is often classified as "***Top Secret***," "***Secret***," or "***Unclassified***," and access is restricted accordingly.

Classification and Trust Modelling cont…

Classification in Information Security

- **<u>Data Protection:</u>** Data classification helps organizations identify and protect their most sensitive information.
- Data can be categorized into different classes based on its sensitivity, and security measures are then applied accordingly.
- For instance, medical records might be classified as "***Highly Sensitive***" while publicly available product information is "***Public***".

Classification and Trust Modelling cont…

Classification in Information Security

- **Threat Detection:** Classification models are used to identify and categorize potential security threats and incidents.
- Different algorithms can classify network traffic, log data, or user behavior as normal or suspicious, enabling rapid threat detection and response.

Classification and Trust Modelling cont…

Trust Modelling in Information Security

- **User Authentication:** Trust models are employed in user authentication systems to assess the trustworthiness of users based on their credentials, behavior, and past interactions with the system.
- Users with high trust scores may be granted privileged access.

Classification and Trust Modelling cont…

Trust Modelling in Information Security

- **Device Trustworthiness:** In the context of the Internet of Things (IoT) and device security, trust models are used to evaluate the trustworthiness of IoT devices.
- Suspicious or compromised devices can be isolated or denied access to the network.

Classification and Trust Modelling cont…

Trust Modelling in Information Security

- **Software and Application Trust:** Trust models can assess the trustworthiness of software applications and updates.
- For example, digital signatures and reputation systems are used to determine whether software updates or downloads are from trusted sources.

Classification and Trust Modelling cont…

Trust Modelling in Information Security

- **Access Control:** Trust models are often integrated into access control mechanisms.
- Access decisions can be based not only on user credentials but also on the trust level assigned to a user or device.
- Users with higher trust may be granted more extensive access privileges.

Classification and Trust Modelling cont…

Trust Modelling in Information Security

- **Behavior-Based Trust:** Behavioral analysis models assess the trustworthiness of users based on their behavior within the system.
- Suspicious activities or deviations from normal behavior can trigger alerts or security actions.

Classification and Trust Modelling cont…

- The interconnection between classification and trust modeling in information security is evident in scenarios where entities are categorized based on their attributes and behavior:

Classification and Trust Modelling cont…

- **User and Entity Behavior Analytics (UEBA):** UEBA solutions combine classification techniques with trust modeling to identify abnormal user and entity behavior.
- For example, UEBA systems classify user activities as normal or suspicious based on historical data and trust scores, allowing for real-time threat detection.

Classification and Trust Modelling cont…

- **Data Loss Prevention (DLP):** In DLP solutions, data is classified based on its sensitivity.
- Trust models are then applied to users or processes accessing this data, considering their trustworthiness.
- For instance, sensitive data may only be accessible by highly trusted users.

Classification and Trust Modelling cont…

- **Access Control Policies:** Access control policies often take into account the classification of users and resources.
- Trust models inform these policies, helping organizations enforce fine-grained access control.