Introduction To Information Security

Syllabus Information

IY 2760 - Introduction to Information Security

Associated Term: 2022/23 Academic Session
Learning Objectives:

Introduction: What is security (covering notions of Confidentiality, Integrity, and Availability)? Security threats and risks. Security management (ISO 27000 series). Data Protection legislation.- Introduction to the elements of cryptography: Ciphers (stream, block, e.g. DES/3DES/AES). Message Authentication codes (MACs). Public key ciphers and digital signatures (e.g. RSA). Identity verification: use and storage of conventional passwords. Dynamic password schemes. Biometric techniques. Use of tokens (dumb and intelligent), including the use of secure elements such as smart cards and trusted execution environments (TEEs) Access control: Access Control Lists, capabilities, security labels (MAC and DAC), and role-based access control. CASE STUDY I: a case study in information security. Network security concepts and examples: the concepts of security services and security mechanisms (as in ISO 7498-2). An introduction to firewalls, intrusion detection systems and virtual private networks. Computer security concepts and examples: hardware and operating system concepts, malware e.g. viruses, spyware, ransomware etc., restricting access. Authentication and key distribution: The importance and relatedness of the concepts of key management and entity authentication in a network. Objectives of an entity authentication protocol. Some fundamental protocols (e.g. Kerberos). Using authentication protocols for key distribution, and other approaches to key establishment (including public key certificates and X.509). Cyber Physical security, Examine the security provisions, strengths and weaknesses of existing embedded systems/platforms/smart cards and operating systems. CASE STUDY II: a case study in information security. **Learning Outcomes:** 1. Identify, through the case studies how information security may be influenced by real world design and implementation decisions. 2. Appreciate the different cryptographic algorithms, their use, advantages and disadvantages 3. Apply the above identified cryptographic primitives in the review and evaluation of cryptographic protocols. 4. Appreciate the rational decisions made in the design of some secure systems and security protocols, examples such as authentication protocols, key management protocols, access control, tokens and secure elements, etc
Required Materials: Click here for the reading list system
Technical Requirements: The total number of notional learning hours associated with course are 150. **These will normally be broken down as follows:** 33 hour(s) of Lectures across 11 week(s) 117 hour(s) of Guided Independent Study **Formative Assessment:** In

class feedback **Summative Assessment:** Examination (2 hours) - 60% Set exercises (40 hours) - 40%