INFO 3001 COMPUTER SECURITY

Credit Points 10

Legacy Code 300569

Coordinator Tomas Trescak (https://directory.westernsydney.edu.au/search/name/Tomas Trescak/)

Description This subject aims in particular at, but is not limited to, the implementation and management of security and privacy policies of organisations within the standards and legal framework that is also applicable to the Australian standards.

School Computer, Data & Math Sciences

Discipline Security Science

Student Contribution Band HECS Band 2 10cp

Check your fees via the Fees (https://www.westernsydney.edu.au/currentstudents/current_students/fees/) page.

Level Undergraduate Level 3 subject

Assumed Knowledge

Students are expected to have general understanding on computer systems; computer fundamentals, databases, and web technologies.

Learning Outcomes

On successful completion of this subject, students should be able to:

1. Explain fundamental theories related to computer security, and apply them to computer systems and organisations.
2. Describe the modern authentication, authorisation and access control mechanisms used in computer systems; and look at a few methods of access operations and ownership issues.
3. Explain basic concepts in encryption and cryptography and describe application of various cryptographic techniques and algorithms in accomplishing security.
4. Examine security issues within various hardware systems, operating systems and application software and present the general causes that lead to system security failures.
5. Analyse the security issues specific to databases, and understand how to protect sensitive information and statistical systems within an organisation.
6. Identify security threats and risks associated with web and related technologies; and the capacity to make corrective and preventative measures against these threats and risks in organisations.
7. Describe the relevant standards and the legal framework related to security and privacy; and implement security and privacy policies in organizations.

Subject Content

- Introduction to fundamentals of computer security;
- Identification and authentication: System Security, Managing passwords, Online Verification Requirements, PKI, Key establishment, authentication and protocols;
- Access Control: Access operations, Ownership, Access control structure;
- Security in hardware and software: Data and Code, Memory management, Race conditions, Java Security, .NET security framework;
- Operating system security: Windows/Unix security,
- Cryptography: Symmetric/Asymmetric key Encryption, Digital signature, Hashing, Algorithms;
- Web security: IP security, SSL/TLS, DNS, Firewalls, cookies, Intrusion, Digital identification techniques, Client-side Digital Certificates, Certification Authorities, Sever side security, privacy;
- database security: SQL security model, statistical database security, integrated security, data privacy.
- Security policies and legal framework: Organizational policies, standards and legal framework for security and privacy;

1. Describe the complexities of working in the Cyber Security Industry
2. Identify legal and ethical issues of working in cyber environment
3. Differentiate between threats, vulnerabilities, and exploits
4. Identify network architectures and recognise their potential vulnerabilities
5. Apply reconnaissance methodologies to discover weaknesses in computing environment
6. Explain the differences between vulnerability management policies and vulnerability management maturity models
7. Apply concepts of exploiting vulnerabilities to hack into a system using common penetration testing tools and frameworks
8. Explain the principles of symmetric and asymmetric cryptography, and public key infrastructure
9. Identify data classification levels and email marking standards associated with the dissemination of sensitive and classified information
10. Identify data classification levels and email marking standards associated with the dissemination of sensitive and classified information
11. Identify threats in social networks via Open Source Intelligence (OSINT) Methodologies and demonstrate the capturing of Personally Identifiable Information (PII) using OSINT
12. Demonstrate usage of website security assessment tools to identify weaknesses and potential web attack vectors
13. Identify the types of forensic investigations from a cybersecurity perspective, differentiating between software and hardware digital forensic tools
14. Identify the resources required to navigate the cybersecurity landscape as a potential cybersecurity professional

Assessment

The following table summarises the standard assessment tasks for this subject. Please note this is a guide only. Assessment tasks are regularly updated, where there is a difference your Learning Guide takes precedence.

Type	Length	Percent	Threshold	Individual/ Group Task	Mandatory
Quiz	30 minutes (Weekly from Week 2)	40	N	Individual	N
Quiz	60 minutes	20	N	Individual	Y
Final Exam	2 hours	40	N	Individual	Y

Prescribed Texts

- Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). Security in computing (5th ed.). Upper Saddle River, NJ: Prentice Hall.

Teaching Periods

WSU Online TRI-1 (2025)

Wsu Online

Online

Subject Contact Tomas Trescak (https://directory.westernsydney.edu.au/search/name/Tomas Trescak/)

View timetable (https://classregistration.westernsydney.edu.au/odd/timetable/?subject_code=INFO3001_25-OT1_OW_2#subjects)