

School / Faculty: Faculty of Science and Technology

Course Title: MOBILE SECURITY AND PRIVACY

Course ID: ITECH3300

Credit Points: 15.00

Prerequisite(s): ITECH 3215 or ITECH1102

Co-requisite(s): Nil

Exclusion(s): ITECH3100

ASCED Code: 029901

Grading Scheme: Graded (HD, D, C, etc.)

Program Level:

AQF Level of Program						
	5	6	7	8	9	10
Level						
Introductory	■	■	■	■	■	■
Intermediate	■	■	■	■	■	■
Advanced	■	■	✓	■	■	■

Learning Outcomes:

Knowledge:

- K1.** Describe OSI security architecture.
- K2.** Identify common risks and security requirements, especially for wireless and mobile environments.
- K3.** Develop an understanding of the need for cloud and mobile data security management.
- K4.** Understand the complexities of threat models and the trust in mobile cloud computing.
- K5.** Discuss and reflect on various trust properties in mobile cloud.
- K6.** Identify the security threats in cloud systems and their countermeasures.
- K7.** Develop an understanding of agent-based trustworthy infrastructure for mobile cloud computing.
- K8.** Describe policies prescribed for the protection of information privacy.

Skills:

- S1.** Critically evaluate various types of trust in mobile cloud computing.
- S2.** Distinguish different levels of security for mobile cloud computing.
- S3.** Analyse simulations of security scenarios, identify potential risks and assess solution alternatives.
- S4.** Research emerging trends of mobile cloud.

Application of knowledge and skills:

Course Outline (Higher Education)

ITECH3300 MOBILE SECURITY AND PRIVACY

- A1.** Synthesise knowledge from various sources, including in-depth analysis of theory and simulations, to produce a detailed report involving security risks and threats and to develop technology solutions.
- A2.** Audit different security threats involved in mobile cloud.
- A3.** Communicate professionally to list security policies for mobile cloud computing.

Course Content:

Privacy breaches and countermeasures.

Topics may include:

- Security risks and threats, especially in relation to mobile devices and mobile communications platform.
- OSI security architecture.
- Symmetric and asymmetric encryption techniques, message authentication codes, digital signature, certification authority and public key management.
- Mobile Cloud Computing (MCC) Architecture, Platforms, Technologies and Augmentation approaches.
- Security and data protection in cloud environment - risks and countermeasures.
- Security Issues in Mobile Computing including Application Security and Authentication Issues.
- System security - intrusion detection, malicious software, firewalls.
- Privacy breaches and countermeasures.
- Security Issues with Mobile Cloud Computing.
- Levels for Securing Mobile Cloud Computing.
- Trust and Various Aspects of Trust in Mobile Cloud Computing.

Values and Graduate Attributes:

Values:

- V1.** Develop a professional approach to safeguarding information stored and accessed by mobile devices.
- V2.** Appreciate the role of security and privacy policies in mobile cloud.

Graduate Attributes:

FedUni graduate attributes statement. To have graduates with knowledge, skills and competence that enable them to stand out as critical, creative and enquiring learners who are capable, flexible and work ready, and responsible, ethical and engaged citizens.

Attribute	Brief Description	Focus
Knowledge, skills and competence	Students will be given the foundational knowledge with respect to mobile information security that builds upon their knowledge of software systems, in particular mobile systems.	Medium
Critical, creative and enquiring learners	Students will participate in a self-directed and collaborative learning environment to develop their theoretical and technical expertise in the field of mobile security.	High
Capable, flexible and work ready	Students will investigate technologies to ensure security within mobile information security and develop skills to apply these policies in practice.	Medium

Course Outline (Higher Education)

ITECH3300 MOBILE SECURITY AND PRIVACY

Attribute	Brief Description	Focus
Responsible, ethical and engaged citizens	Students will investigate a variety of security technologies and standards used within industry.	Medium

Learning Task and Assessment:

Learning Outcomes Assessed	Assessment Task	Assessment Type	Weighting
K1, K3 - K7, S1 - S3, A1	The tasks will develop skills in the analysis and practical application of content introduced.	Tutorials/Assignments	10-20%
K2, K4 - K8, S2, A2.	Participate in lectures and labs/tutorials, read and summarise theoretical and practical aspects of the course.	Examinations/Tests	50-60%
S3,S4,A2,A3,K2,K4,K6	The task will develop professional communication skills in delivering a presentation about the recent developments in the content introduced.	Presentation(s)	10-20%

Adopted Reference Style:

APA