FIT5037: Network Security
Unit Information

Faculty of Information Technology
Monash University

People Involved

Chief Examiner
Dr Ron Steinfeld
Email: Ron.Steinfeld@monash.edu

Lecturer
Apostolos Fournaris
Dr. Apostolos.Fournaris@monash.edu
Lecture Consultations Thursday 11:00-12:00

Tutors

- Thalerngsak Kijthaweesinpoon (Guy)
- Ahsan Aziz
- Mohammad Goudarzi
- Aayush Gupta

Unit Objectives

- Explain the fundamentals of wired and wireless network security;
- Learn principles and practices of network security standards and protocols;
- Use practical skills to identify computer system vulnerabilities and carry out penetration testing;
- Identify important network security components, and design then implement defence systems.

Learnig Outcomes

Students should be able to:

- apply common security standards and protocols for network security at different layers e.g. Application, Transport, Network etc.
- understand cryptographic primitives applied to information to ensure its integrity, confidentiality and authenticity during transmission over the network;
- critically assess threats, find vulnerabilities and risks to an organisations information assets and propose control technologies and techniques which can be applied to reduce the security risk;
- →

Learning Outcomes

- ←
- implement cryptographic algorithms and security protocols to provide security over networks and the Internet;
- design system security against intruders and malicious software;
- apply security configurations to computer and network based applications;
- demonstrate proactive vulnerability scanning and penetration testing against hypothetical assets.

Teaching Approach

- Lectures
  - theoretical concepts
    - underlying primitives such as cryptography
    - classes of security problems/solutions
      e.g. vulnerabilities/countermeasures
  - protocols
  - best practices
- Tutorials/Labs
  - practical exercises on the underlying primitives
    - Linux command line and tools
    - python
    - Linux containers
  - exercises on protocols and best practices

Resources

- Moodle
- References and lecture notes
  - **Common Reference: NIST Special Publications**
  - IETF Request for Comments (RFC) documents
  - Other publicly available publications and standard documents
  - Documents freely available through Monash Library
- Laboratory exercises
- Assignment specifications
- Newsgroups/discussion areas
- **Textbook: There isn't any!**
- **Excellent Applied Crypto Reference**
  - Handbook of Applied Cryptography by *Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone*
- Some other useful books:
  - "Network Security Essentials-Application Standards", 5th Edition by William Stallings
  - "Cryptography and Network Security Principles and Practice", 5th Edition by William Stallings

Resources: Software

- Virtualization (VirtualBox)
- Core Network Emulator
- Linux (Ubuntu) open source security tools
- Linux containers (Ubuntu)
- Python programming language and libraries (version 3)

Unit Structure

Lecture Topics:

- Symmetric key cryptography
- Asymmetric key cryptography
- Pseudorandom Number Generators and hash functions
- Authentication Methods and AAA protocols
- Security at Network layer
- Security at Network layer (continued)
- Security at Transport layer
- Security at Application layer
- Computer system security and malicious code
- Computer system vulnerabilities and penetration testing
- Intrusion detection
- Denial of Service Attacks and Countermeasures / Revision

Workload

- **Lecture:** 2 hours per session
- **Tutorial:** 2 hours per session
- **Self Study:** 8 hours of weekly self study (provided that you have mastered the networking part of Network Security)

Recomendations

- Use the Forum to collaborate
- Read each week's laboratory notes and prepare **before** coming to the actual laboratory
- We can help you during tutorial/lecture consultation

Assessment

In-semester:

Three components:

- Assignment 1: due **Monday 16th September 2019 8:00 AM** 30%
  - Monday beginning of Week 8
  - Interviews during Week 8
- Assignment 2: due **Monday 21st October 2019 8:00 AM** 20%
  - Monday beginning of Week 12
  - Interviews during Week 12
- Lab Tasks Assessments: conducted during tutorial sessions in weeks 5 and 10, 20%

In-semester Hurdle: 40% of in-semester assessments

Final Exam:

- A 2-hour closed-book examination, 30% of unit mark

Final Exam Hurdle: 40% of the final exam mark

Assessment: Unit Hurdle

- The overall unit mark must not be less than 50%.
- Failure to meet a hurdle (40% of in-semester or 40% of final exam) will result in a maximum mark of 49N even if the total sum (of in-semester assessments and final exam marks) is greater than 50%.