

Introduction

COMP90043
CRYPTOGRAPHY AND SECURITY

Udaya Parampalli

Introduction

- About me
- About you
- About the subject

A little bit of myself

- Udaya Paramplli, Associate Professor and Reader
- Research Interests:
 - Cryptography
 - Sequences for Communication and Security
 - Network Security
 - Codes for Distributed Storage
- Publications:
<http://people.eng.unimelb.edu.au/udaya/>

Research Interests

- Distributed Storage Codes: Developed novel erasure codes used to build distributed data storage solution on a wide geographically distributed cluster.
- Identity based cryptographic schemes using pairings: We have built cryptographic software for efficient implementation of elliptic curve group operations and pairings
- Sequence design for Radar and Communications. We have developed sequences with low correlations useful in variety of communication and radar applications.

Research Interests

- Cyber Security: Multi-dimensional privacy preserving security data analytics: Developing a privacy preserving analytics using correlation of collected n -dimensional data in a cloud based infrastructure.
- Secure Storage using Erasure codes: Developing secure data storage based on information theoretic principles using erasure codes. This approach has a sound practical context whereby an adversary who can only control some part of the system will not be able to compromise the whole system.
- Steganography for Medical Images and Scans: Developing new information hiding techniques focusing on security and authentication of medical scans and images.

How to contact me?

- Preferably at the end of lectures
- Email: udaya@unimelb.edu.au (Include the word COMP90043 in subject field)
- Expect 48 hours turn around on occasions!
- Office: 7.04, Doug McDonnell Building (Building 168)
- Consultation: Times will be announced on LMS and also by appointment.

Tutors

- Patrick Vicky <pvicky@student.unimelb.edu.au> Head Tutor
- Kim Ramchen <k.ramchen@student.unimelb.edu.au>
- Rahul Sharma <sharma1@student.unimelb.edu.au >

Subject Structure for 2016

- 12 Weeks of Lectures
 - 2 hours of teaching + 1 hour of tutorial (We have three tutors and many parallel sessions)
- Assessment:
- 60% Project/Assignment
 - 2 Assignments (7.5% each individual work)
 - Mid-Semester Test (10%)[Tentative date: Week 8]
 - 1 research project (35% Total) **a group project-details will be released soon)**
 - Part A: Presentation in Week 12 (7%)
 - Part B: Research Report (28%)
- 40% Final examination
 - 2 Hour Final examination

Hurdle Requirements

- **Hurdle requirement:** To pass the subject, students must obtain at least:
- 50% overall.
- 50% in the homework assignments
- 50% in the research project
- 50% in the end-of-semester written examination

Intended Learning Outcomes (ILO)

- ILO1: Identify security issues and objectives in computer systems and networks.
- ILO2: Apply various security mechanisms derived from cryptography to computers and computer networks.
- ILO3: Explain the workings of fundamental public key and symmetric key cryptographic algorithms including RSA, ElGamal, Diffie-Hellman schemes and stream ciphers.
- ILO4: Explain the protocols which ensure security in contemporary networked computer systems.
- ILO5: Describe the interaction between the underlying theory and working computer security infrastructure.
- ILO6: Analyze security of network protocols and systems.

Lecture Times

- **COMP90043: Cryptography and Security**

Two hours per week

- Tuesday 10-11, Venue: See Timetable
- Wednesday 2.15-3.15m, Venue: See Timetable

Additional Extra Lecture

- Tuesday?

See Timetable for workshops.

Note that in the subject you are expected to work on programs on departmental servers. There will not be any official laboratory workshops. You will need to work yourselves. We will provide consultations.

Subject Resources

- **Textbook:** Cryptography and Network Security: Principles and Practice, 6/E by William Stallings
- **References:**
 - ❑ Douglas R Stinson, Cryptography, Theory and Practice, Chapman & Hall/CRC, 2006.
 - ❑ Richard E. Smith, INTERNET CRYPTOGRAPHY, ADDISON WESLEY, 1997.
 - ❑ Andrew S. Tanenbaum , COMPUTER NETWORKS, Fourth Edition, Prentice-Hall International, Inc, 2002.
 - ❑ Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, October 1996.
 - ❑ Wenbo Mao, ``Modern cryptography Theory and Practice'',www.hp.com/hpbooks, Pearson Education, Prentice Hall, 2004.
 - ❑ Articles from Lecture Notes in Computer Science series covering security and cryptography.

Subject Outline

- This subject covers fundamental concepts in information security on the basis of methods from modern cryptography. We will concentrate on topics which are of current interest as well as the more `classic' topics which underlay this discipline.
- Topics drawn from:
 - ❑ symmetric key and public key cryptosystems,
 - ❑ hash functions,
 - ❑ authentication
 - ❑ secret sharing
 - ❑ Protocols
 - ❑ Key Management
- There will be some guest lectures in specialized topics.

Subject Description

- The objective of this subject is for students
- to understand the fundamentals of security principles in modern networks and computer systems,
- to be able to explain the protocols which ensure security in contemporary networked computer systems;
- to study various cryptographic primitives like encryption, hashing and signature functions which are used in theory and practice of network security.

Course Plan (Dates to be Confirmed)

- Topics by week:
 - ❑ 1. Introduction to Security (Ch 1)
 - ❑ 2. Symmetric Ciphers, Block and Stream Ciphers (Ch 2,3,6,7) (Assignment 1 handed out)
 - ❑ 3. Basics from Number Theory (Ch 8) (Group Formation)
 - ❑ 4. Public Key Cryptography and RSA (Ch 9) (Assignment 1 due on Mon)
 - ❑ 5. Hash functions (Ch 11) (Project topics confirmation)(Assignment 2 handed out)
 - ❑ 6. Message Authentication Codes (Ch 12)
 - ❑ 7. Digital Signatures (Ch 13) (Assignment 2 due)
 - ❑ 8. Key management, (Mid Semester Test)
 - ❑ 9. Key management cont., Secret Sharing (Ch 14)
 - ❑ 10. Application/Advanced Topics (Part 5)
 - ❑ 11 Guest Lecture/Preparation for Project Presentations
 - ❑ 12. Review, Project presentations/ Report Due

Generic Skills

- GS1: Ability to undertake problem identification, formulation, and solution.
- GS2: Ability to utilise a systems approach to solving complex problems and to design for operational performance
- GS3: Ability to manage information and documentation
- GS4: Capacity for creativity and innovation
- GS5: Ability to communicate effectively, with the engineering team and with the community at large