Introduction to CSS 322 – Security and Cryptography

Dr Steve Gordon
ICT, SIIT
Welcome

• To a first course on the theory and technologies that provide secure computers and networks

• A 3rd year course for computer scientists

• Course website available from http://ict.siit.tu.ac.th/drupal/css322
Who Am I?

• Steve Gordon

• Contact details:
  – Email: steve@siit.tu.ac.th
  – Office: 2304-7, Bangkadi (IT&MT Building)
  – Phone: ext 2014
  – Mobile: 0817227288
  – Windows Live Messenger: stevengordon07@hotmail.com
  – Google Talk: steve.siit@gmail.com

• When can you contact me?
  – Anytime …
Prerequisites

• There are no formal prerequisites, but I assume you know:
  – Discrete mathematics (logic, prime numbers, …)
  – Basics of data communications (OSI 7-layers)
  – Operating system concepts (processes, RPC, …)
  – Software design principles (divide-and-conquer, functions, …)
  – Programming languages (e.g. C, C++, Java or similar)
What will you learn in CSS 322?

• The role of security in computers and networks
• Theory and concepts behind secure systems
  – Cryptography
• Details of important and popular algorithms
  – DES, AES, RSA, Digital Signatures, …
• Internet security techniques and attacks
  – Layered security, viruses, spyware, …
• Details of Internet security protocols
  – IPsec, SSL/TLS, PGP, …
• Legal and ethical issues and current trends
Topics

- Introduction to Security
- Classical Encryption Techniques
- Block Ciphers and DES
- Advanced Encryption Standard
- More on Symmetric Ciphers
- Confidentiality using Symmetric Key Encryption
- Introduction to Number Theory
- Public Key Cryptography
- Public Key Management
- Authentication and Hash Functions
- Authentication Applications
- Internet Security
- Firewalls
- Malicious Software
- Web and Other Security Issues
Why is CSS 322 Useful?

• It will help you get a job!
  – Designing and writing secure applications
  – Designing and managing secure systems (networks, computers)

  – Security certifications (e.g. CISSP, GIAC) are much more valuable than networking/computer certifications (e.g. Microsoft, Cisco)

• You will have an understanding of:
  – The concepts behind most of today’s security protocols
  – Details of popular Internet security protocols and systems
  – Techniques for attacking and defending networks
  – Legal and ethical issues that arise in computer security
Course Structure

• Lectures
  – 3 hours per week

• Self study
  – At least 6 hours per week
  – Browsing lecture notes BEFORE and AFTER class, reading the textbook and other materials, studying for quizzes and exams, preparing assignments, consultations, group discussions, ...

• Assessment
Assessment

• Quizzes
  – 10 minute quizzes at the beginning of selected lectures
  – Cover the topics since the last quiz
  – Test your understanding of lectures, reading materials and homework problems
  – Closed book
  – 7 quizzes; 5 best marks will count
  – 20% total (4% each)

• Assignment
  – Set of problems for you to complete over a number of weeks
  – Test your in-depth understanding of concepts and protocols
  – Open book
  – 20%
Assessment

- **Mid-term Exam**
  - Closed book
  - 30%

- **Final Exam**
  - Closed book
  - 30%

- **For advice:**
  - Closed book assessment is not a memory test (e.g. I won’t test your ability to remember S-boxes) – it’s a test of understanding
  - We will discuss types of questions and topics before exam
Academic Misconduct

• What is it?
  – Plagiarism, cheating, copying, “lending”, …

• Examples
  – Copying assignment answers from friend (verbal or written)
  – Giving your assignment (or some answers) to a friend
  – Looking at neighbours answers during quiz/exam
  – Copying sentences/paragraphs/code from textbooks/Internet without acknowledgement

• Results
  – If detected, questions or entire assessment item may get 0 marks

• Discussion with friends is encouraged; telling your friends answers is not!
Learning Materials

• Lectures
  – Attend, listen and ask questions!
  – Will include examples and demonstrations

• Lecture notes
  – PDF of Powerpoint slides
  – Available on website and from document services
  – Aim to have available 1 day before lecture
  – Make your own notes

• Recommended Textbook
  – “Cryptography and Network Security” by Stallings
  – 4th Edition (90% of my content is based on this)

• Other Useful Textbooks
  – Earlier editions of Stallings textbook
  – “Network Security” by Kaufman, Perlman, Speciner
  – These other textbooks should only be used as supplementary readings
Learning Materials

• **Recommended Readings**
  - For selected topics I will list papers/chapters/websites/standards that should be read
  - These will be publicly available on the Internet or available through the Library (electronic or hardcopy)

• **Course Website**
  - All materials will be available from the website
  - Announcements, selected solutions will be on the website

• **Mailing list (access via course website)**
  - You must subscribe (as will be used for announcements)
Is This Course Difficult?

• Computer and network security looks very hard!
  – Theory of computer security includes lot of mathematics
    • Example: Stallings textbook contains details of many algorithms
  – Network security protocols can be very complex
    • Example: IPsec (and associated IKE) – 200+ pages of standards

• I will try to make it look easy!
  – Not all mathematical details will be covered
  – Go through algorithms S L O W L Y, using examples
  – Combine technical details of protocols/algorithms with demonstrations of real systems
  – Cover only selected (interesting!) protocols
  – May adapt topics based on your feedback (including quiz results)