Security (CS4028)

Lecture 1a. Course Overview

Chunyan Mu

chunyan.mu@abdn.ac.uk

The School of Natural and Computing Sciences

Schedule

Week	Lecture 1	Lecture 2	Tutorial
⇒ 1	Intro to course & security	Intro to Crypto	-
2	Symmetric Crypto	Hash	Math for crypto
3	Asymmetric Crypto-1	Asymmetric Crypto-2	Symmetric Crypto
4	Signatures	Zero Knowledge Proof	Asymmetric Crypto
5	Certificates	Authentication	Signature & certificates
6	Access Control	AC models	Authentication
7	Information flow	Information flow	Access control
8	Security management	Protocols	Concepts & management
9	Network security	Network security	Protocols and communications
10	Advanced Topic	Advanced Topic	Network
11	Revision		

Course Introduction

The purpose of this course

- This introductory course is in relation to information and network security
- It covers a diverse set of topics related to information and network security (e.g., cryptographic methods, security protocols).
- Recap and build a solid foundation for advanced security.

Course Introduction

Teaching team

- Chunyan Mu (CM), Chunyan.Mu@abdn.ac.uk

When are we?

- This session is Lecture 01 in Week 1 of the course
- There are 11 weeks of teaching, 2 weeks after that in which the final exam can be scheduled.
- Tutorials begin in the second week of teaching.
- University official Week Numbers start at 1 from 1st August, so the number is offset from our course weeks.
  `http://www.abdn.ac.uk/infohub/study/week-numbers-634.php`

Course Introduction

myAberdeen

`http://www.abdn.ac.uk/myaberdeen`

- myAberdeen for this course will have:
  - All lecture notes (that we give).
  - Material for tutorials.
  - The coursework and marking/feedback template
  - Continuous assessment submissions
- All documents in one place

Course Introduction

Lectures

- You should attend **all** lectures in order to be properly aware of what to expect in the examination.
- Lecture notes are available on myAberdeen, but it may be necessary for you also to take your own notes during lectures.
- If there is time, then there will be a revision lecture.
  - This will be decided closer to the time.

Course Introduction

Tutorials

- This course has "*tutorials*".
  - Sometimes we call them "*practicals*" but there is no difference.
- Tutorials begin in the second week of teaching .
- You must attend tutorials for attendance monitoring.
  - This is a University requirement.
- Do not forge signatures or ask others to do so on your behalf.
  - This is fraud.
  - Similar remarks apply to scanned codes.

Course Introduction

Tutorials

- Tutorials will be used to provide support your learning.
  - **You** should make use of tutorials.
  - They help to prepare you for the exam!
- Each week there will be a series of questions to answer.
- You should consider these **before** each tutorial.
- There are often too many to be able to work through during each tutorial, and some of them are quite hard or open-ended.

Course Introduction

Assessment

- **First Attempt**
  - 1 two-hour written examination (75%)
  - continuous assessment/coursework (25%, Due Date 23:59 30/10/2025)
- **Resit**
  - Candidates only resit those components (written examination,continuous assessment)
    - which they failed at first attempt.
  - Written examination at resit is 1 two-hour paper.

Course Introduction

Exam Logistics

- Invigilated, and
- In-person, and
- Closed-book.

Course Introduction

Exam Logistics

- Invigilated, and
- In-person, and
- Closed-book.

Exam

- You need to memorize stuff for the exam.
- You need to be able to do stuff without looking up how during the exam.
- You need to be able to do the exam in a short time-frame.

Course Introduction

Exam cont.

- You need to show up on time.
- You will be denied entry if you are late.
- You need at least one blue or black pen.
  - You should carry at least one spare.
- You need your University ID card.

Course Introduction

Exam Feedback

- The mark is returned after the exam board via the relevant University information system for students.
- The exam board happens around the end of January.
- Exam feedback is provided via an in-person meeting, where requested.
- These are the standard University practices.

Course Introduction

Coursework (25%)

- Coursework = continuous assessment
- This lecture contains basic information about your coursework, but the details including hand-in deadline is on myAberdeen.
- You need to go and look at that very soon.
- Extensions are unlikely to be granted for frivolous reasons.
- If you don't make the hand-in deadline, we will be unable to return marks on the deadline intended.

Course Introduction

Coursework (25%) cont.

- There will be ONE component.
- It consists of a report (with associated code submission) documenting code you have written for a security task.
- This is a Level 4 assessment. It is open-ended. You must do more impressive work to get a higher grade.

Course Introduction

Coursework (25%) cont.

- This is an individual assignment.
- You must write your own code.
- You must write a readable report.

Course Introduction

Coursework (25%) cont.

- All text must be your own writing, with sources and quotations clearly stated.
- Any standard style of giving references is acceptable. Please look at a few books to decide how you'd like to do it.
- Clear, unambiguous English is expected.
- Significant deviations from these requirements will be penalized. If in doubt, ask at a tutorial.

Course Introduction

Coursework Feedback

- The University asks us to give you feedback for normal continuous assessments during term, *normally* in TWO **working** weeks. We will try to do it faster.
- Rapid turnaround of feedback places constraints on how much feedback can be given.
- Marking rubric to be used will be made available on blackboard.

Course Introduction

How to fail the course

- Start by cheating on the coursework.
- Very few people have failed this course. All, or almost all, were caught cheating.
- " *... what I do have are a very particular set of skills. Skills I have acquired over a very long career. Skills that make me a nightmare for people like you. ... I will find you ...*"

  - Taken, 2008, 20th Century Fox

Course Introduction

Misconduct: Plagiarism

- "*The practice of taking someone else's work or ideas and passing them of as one's own*" - Oxford Dictionaries
- Most common way to fail this course is to start by plagiarising in the continuous assessment.
- `https://www.abdn.ac.uk/toolkit/skills/referencing/`

Course Introduction

Code Plagiarism

- You **must** acknowledge any code borrowed from anywhere else.
- This includes open-source code.

Course Introduction

Code Plagiarism

- You **must** acknowledge any code borrowed from anywhere else.
- This includes open-source code.

Other Misconduct

- Collusion: working with others
- Contract cheating: getting someone else to do your work for you, whether-or-not you pay them.

Course Introduction

C6s

- You get a C6 'at risk' warning if any of the following apply
  (i) Absence for a continuous period of 10 working days or 25% of a course (whichever is less) without good cause being reported;
  (ii) Absence from two tutorials
  (iii) Failure to submit the continuous assessment(s).
- You must respond if you get a C6, or else you will be removed from the course (C7).

Course Introduction

Communications

- Attend lectures and practical sessions
- Read your emails
- Look at myAberdeen for announcements
- Any issues, ask for help during any practical sessions and drop a message to us.

Course Introduction

Ethics and Responsibilities

- Knowledge is power: use it to do right, not wrong.
- You must continue to follow:
  - the law, and
  - university policy.
- University regulations apply to you.
  - All the policies are easy to find on the website.
    `http://www.abdn.ac.uk/dit/student/get-started/policies.php`
- Scots and UK law applies to you.
  - E.g. The Computer Misuse Act and the various amendments.
    `https://en.wikipedia.org/wiki/Computer_Misuse_Act_1990`

Course Introduction

Books and Reading List

- There are many books and sets of lecture notes on security.
- Our course basically follows:
  - D. Gollmann, *Computer Security (3rd Edition)*, John Wiley, 2011.
  - A lot more technical material is explained in here.
- Security technology changes fast, so do cutting-edge aspects, but basic principles tend to be more stable.
- The following book is useful:
  - R. Anderson, *Security Engineering*, 2nd Edition, Wiley.
  - website: `http://www.cl.cam.ac.uk/~rja14/book.html`
- Others
  - *Cryptography, A Very Short Introduction*, Piper and Murphy, O.U.P.
  - *Computer Security: Art and Science*, Matt Bishop, Addison-Wesley.

Course Introduction

Course outline

- Week 1: Introduction to the course, security and cryptography
- Week 2: Symmetric crypto and hashing
- Week 3: Asymmetric crypto
- Week 4: Signatures; zero knowledge proof
- Week 5: Certificates; Authentication
- Week 6: Access control; Security models
- Week 7: Information flow
- Week 8: Security Management; Protocols;
- Week 9: Network Security
- Week 10: Advanced Topics
- Week 11: Revision
- Week 12: EXAM/ASSESSMENT WEEK
- Week 13: EXAM/ASSESSMENT WEEK

After your graduate

If you want more time on some topics, do this:

Cybersecurity, MSc, University of Aberdeen

Any Questions?

Any questions?

- Lectures?
- Practicals?
- Exam?
- Coursework?
- Resources?