Lecture 1: Course introduction

COSC362 Data and Network Security

Book 1: Chapter 1 – Book 2: Chapter 1

Spring Semester, 2021

Motivation

What is this course about?

- How does this course run?
- Why is cyber security important?
- What is in this course?

Outline

Introduction to the course

Why do we need cyber security?

Course outline

Outline

Administration

- Course coordinator and lecturer: Clémentine Gritti
  - clementine.gritti@canterbury.ac.nz
- Teaching assistant: Ryan Beaumont
  - rbe72@uclive.ac.nz
- Materials for lectures, labs, assessment items (quizzes and assignment) are on LEARN

Pre-requisites and textbook

- *Pre-requisites:* COSC264 or INFO333
- It is recommended that COSC362 and COSC364 are taken together.
- *Recommended textbooks:*
  - Book 1: *Cryptography and Network Security: Principles and Practice*, W. Stallings, (5th) 7th Edition
  - Book 2: *Computer Security: Principles and Practice*, W. Stallings and L. Brown, (3rd) 4th Edition
  - Useful to back up lectures and practice with exercises (useful for exam preparation!)
  - Syllabus for the examination mainly defined by the lecture slides, not by the textbooks
- Many useful resources online (some will be mentioned on LEARN)

Assessment

- Ongoing work during the semester:
  - 8 quizzes (20% in total)
  - 1 assignment (20%)
- Labs attendance and participation (10%)
- Final exam (50%)

Check the semester plan and timetable on LEARN:

- Submission dates
- Other useful details
- The timetable may sometimes be updated

Timetable

- Lecture times
  - 19 July – 27 August and 13 September – 22 October
  - Monday 10:00 – 11:00 in E5 Lecture Theatre
  - Thursday 11:00 – 12:00 in E5 Lecture Theatre
- Lab times
  - 26 July – 27 August and 13 September – 22 October
  - Friday 16:00 – 18:00 (01) & Tuesday 16:00 – 18:00 (03) in Jack Erskine 136 Lab 4
  - Wednesday 14:00 – 16:00 (02) in Jack Erskine 131 Lab 1

Check timetable on LEARN (the timetable may sometimes be updated).

Other information

- Online quizzes will give you direct feedback:
  - This kind of multiple-choice questions will be included in the final exam.
- The mid-term assignment will have similar questions to the ones encountered in the final exam.
- Labs:
  - Lab tasks/questions are first released on LEARN.
  - Solutions/answers are released later, say around two weeks after corresponding labs happened.
  - In case you missed one lab, you have one week to submit a report.

Outline

New Zealand – December 2017

Privacy "Agency obligations are defined in the 12 Information Privacy Principles that underpin the Privacy Act 1993." – setting out how agencies may collect, store, use and disclose personal information

Security "Government agencies must consider the nature and value of the information they are managing and the measures needed to protect it."

Risk management "Understanding, assessing and documenting the scope of [the] risk service delivery, reputation, legal exposure, security and integrity, customer confidentiality and investment."

`https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/`

European Union (EU) – May 2018

The EU General Data Protection Regulation (GDPR) aims to "protect and empower all EU citizens data privacy":

Google "We're making these [privacy] updates as the GDPR takes effect across the EU."

LinkedIn "Your privacy comes first in all of these updates. We now meet the high standard for data privacy introduced by the new European data protection law known as the GDPR."

IBM cloud "Measures [are] in place to protect your data, including any personal information that may be subject to data protection regulations, including GDPR."

`https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en`

Dark Hotel attack – 2012

- Targeted phishing attacks using spyware
- Infiltrating guests' computers through Wi-Fi networks in hotels
- Loss of confidentiality

https://www.kaspersky.com/blog/darkhotel-apt/6613/

Ashley Madison data breach – 2015

- Exposing over 30 GB of user data (real names, banking data, credit card transactions)
- Hacktivism: the hacking group decided to “punish” the company
- Loss of confidentiality

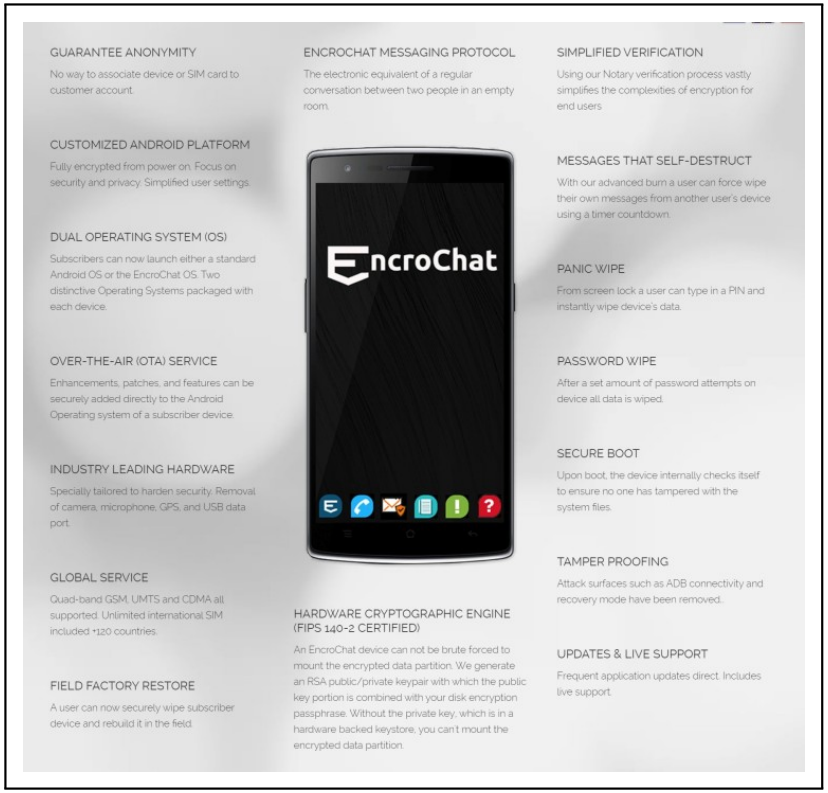
https://digitalguardian.com/blog/timeline-ashley-madison-hack

Hello Barbie attacked – 2016

- POODLE attack (man-in-the-middle exploit)
- Communications intercepted and decrypted between Barbie and servers
- Loss of confidentiality

https://www.iflscience.com/technology/barbie-doll-records-your-voice-has-hackable-security-flaw/

EncroChat used by criminals – 2020



- A communications network and service provider allegedly used by gang members to plan a number of criminal activities
- Infiltrated by police in June and July 2020 during a Europe-wide investigation
- Operations were ceased due to the police operation
- Loss of confidentiality

https://news.sky.com/story/encrochat-what-it-is-who-was-running-it-and-how-did-criminals-get-their-encrypted-phones-12019678

Sony's PlayStation network attacked – 2011

- Attackers inject characters or lines of code into attacked website
- Structure Query Language (SQL) injection attack
- Loss of integrity

`https://news.softpedia.com/news/Sony-Pictures-Hacked-Millions-of-Accounts-Exposed-204036.shtml`

WannaCry ransomware – 2017

- Unpatched Windows systems
- Stolen government hacking tools
- Worm encrypting files on computers' hard drive, then demanding a payment in bitcoin to decrypt them
- Loss of availability

https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

Mirai botnet – 2016

- Botnet attacking IoT devices with default admin credentials
- Distributed Denial of Service (DDoS) attack
- Loss of availability

https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

You, me – July 2021

- Have you been “pwned”?
  - Check whether your private information has been leaked or compromised.
  - Check your email address:
    `https://haveibeenpwned.com/`
- Is your password strong enough?
  - Take a strength test.
  - Check your password’s strength:
    `https://www.my1login.com/resources/password-strength-test/`
- UC tips for better cyber security awareness:
  - `https://www.canterbury.ac.nz/its/cyber-security/`
  - `https://www.comparitech.com/blog/information-security/security-remote-working/`

Outline

Course focus

- Cryptography as a foundation for information security
- Applications of cryptography in network security
- Prominent internet security protocols

Some mathematics for cryptography are needed, but their usage is emphasized rather than proofs.

Course contents

- Historical cryptography
- Modern cryptography:
  - Block ciphers, stream ciphers
  - Public key cryptography
  - Hashing and MAC
- Some mathematics:
  - Modular arithmetic
  - Number theory
  - Elliptic curves
- Using all of the cryptography:
  - Public key infrastructure
  - Secure email
  - TLS (HTTPS)

Any questions?

Fell free to:

- ask during the lectures
- come to see me in my office (no specific office hours)
- send me an email
- post your questions onto the **anonymous** LEARN forum