
Data and Network Security

Jordan Pyott

2021-05-06 17:02

Contents

Course Information	3
Assessment	4
Lectures	5
Lecture One - Course Introduction	5
Lecture Two - Course Overview	6

Course Information

Lecturers Details

- Lecturer: Dr. Clementine Gritti
 - Office: Erskine 304
 - Email: clementine.gritti@canterbury.ac.nz
- Tutor: Ryan Beaumont
 - Email: rbe72@uclive.ac.nz

Other Information

- Labs and Quiz's will be available on learn
- Textbooks
 - Cryptography and network security : principles and practice, William Stallings, 5th edition
 - * This course is inspired from this book as the bulk of the course is founded in cryptography.
 - * The exam will only be on content in the slides not from the book
 - Computer security : principles and practice, William Stallings and Lawrie Brown, 3rd edition

2.1 Term 1 Plan

Week starting date	Course week	Monday lecture	Thursday lecture	Lab
19/07/2021	1	L1: Course introduction	L2: Course overview	no lab
26/07/2021	2	L3: Discrete mathematics	L4: CrypTool (at home)	Lab 1: Introduction
02/08/2021	3	L5: Classical encryption part 1	L6: Classical encryption part 2	Lab 2: Discrete maths exercises
09/08/2021	4	L7: Block ciphers	L8: Block cipher modes	Lab 3: CrypTool part 1
16/08/2021	5	L9: Stream ciphers	L10: Number theory	Lab 4: CrypTool part 2
23/08/2021	6	L11: Hash functions and MACs	no lecture	Lab 5: Number theory exercises

2.2 Term 2 Plan

Week starting date	Course week	Monday lecture	Thursday lecture	Lab
13/09/2021	7	L12: Public key crypto part 1	L13: Public key crypto part 2	Lab 6: Hash functions and MACs exercises
20/09/2021	8	L14: Digital signatures	L15: PKI and certificates	Lab 7: CrypTool part 3
27/09/2021	9	L16: Key establishment	L17: TLS part 1	Lab 8: PKI and certificates
04/10/2021	10	L18: TLS part 2	L19: IPSec and VPN	Lab 9: Digital signatures and key establishment exercises
11/10/2021	11	L20: Email security	L21: Malware and attacks	Lab 10: TLS
18/10/2021	12	L22: Recap lecture	no lecture	Lab 11: IPSec and email security exercises

Figure 1: Timetable

Assessment

1. Labs (10%) - attendance and participation:

- Labs are done individually but you are encouraged to discuss and share with your peers (you are allowed to see each other during labs).
- Attending one lab each week over the semester automatically gives you full mark: – The tutor will assess your attendance.
- If you cannot attend one lab session, then a report (along with a justification of student absence) will be required and assessed:
 - The report needs to be submitted by one week after the missed session.
 - Example: if you miss Tuesday lab on Week X then you are asked to submit a report by Tuesday of Week X+1.
 - The report needs to be sent to *both* the lecturer and the tutor.

2. Weekly quizzes (20%):

- They can be found and done on LEARN.
- 9 quizzes in total.
- Each quiz contains 10 questions. Each question contains 4 choices such that only one choice is correct.
- 2 attempts per quiz, such that the highest grade is taken into account.
- A quiz is given on Friday of Week X, and should be done before Friday of Week X+1 (except for the one released just before the break):

3. Assignment (20%):

- *Deadline*: 17 September 2021.
- Small exercises on what has been covered so far.
- The assignment will be released on LEARN on 20 August 2021.
- Your report should be uploaded to LEARN.

4. Final exam (50%)

- 3-hours duration
- 25 multiple-choice questions
- 5 open questions, such that if additional information is needed to solve the problem then it will be provided.
- Covers all content from all lectures study *definitions, mechanisms, processes*
 - Not expected to remember the code of each standard (e.g. RFC1234)

Lectures

Lecture One - Course Introduction

- All materials will be found on learn, including lectures, labs, quizzes and assignments.
- Course outline available
- Labs must be done in person or a report *will not get full marks if do not attend*
- Labs start next week
- Weekly quizzes go over two lectures each *multi-choice*
- Midterm and final will all be entirely open questions

Why do we need cyber security

- Privacy
- Security
- Risk management

Famous recent attacks

- Dark hotel attack
 - Targeted phishing attacks using spy-ware
 - Infiltrating guests computers through WIFI networks at hotels
 - Loss of confidentiality
- POODLE attack
 - man in the middle exploit
 - Communications can be decryped and exploited
- EncroChat
 - A communications network and service provider
 - Infiltrated by police in 2020
- WannaCry
 - Loss of availability
 - stolen government hacking tools
 - Worm encrypting files on computers hard drive
 - * Was a form of ransom-ware
- Botnet
 - Botnet attacking IoT devices with default admin credentials

- DDos
- Loss of availability

Because of these attacks, some users have lost confidence in the service provided not storing/selling data.

Course Focus

- Cryptography as a foundation for information security
- Applications of cryptography
- History of cryptography
- Modern cryptography
 - Block ciphers, stream ciphers
 - public key crypto
 - Hashing and MAC
- Some mathematics
 - Modular arithmetic
 - Number theory
 - Elliptic curves
- Using all of the cryptography
 - Public key infrastructure
 - Secure email
 - TLS (HTTPS)

Lecture Two - Course Overview

What is cyber security?

Definition from the NIST computer security handbook:

- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources.
 - Some literature might differentiate between *computer security* and *cyber security*

Definitions

- A threat

- Represents a potential security harm to an asset
- An attack
 - is a threat that is carried out
- The threat agent
 - carrying out the attack is referred to as an attacker
- A countermeasure
 - Any means taken to deal with an attack
- A residual level of risk to the assets
 - represented by vulnerabilities possibly exploited by threat agents
- **Assets**
 - Computer systems and other data processing, storage and data communication devices
 - OS, system utilities and applications
 - Files and databases and further data
 - Local and wide area network links
- **Vulnerabilities**
 - A computer system can be:
 - * Leaky
 - meaning gives access to information through the network, violates confidentiality
 - * Corrupted
 - meaning that it does the wrong thing, violates integrity principle
 - * Unavailable
 - meaning that it becomes impossible or impractical to use, violates availability
- Passive attacks
 - Interception
 - Traffic analysis
 - * Spoofing, finding information and observing traffic
- Active attacks
 - Altering information and system resources
 - May be hard to prevent but easy to detect
 - Masquerade

- * the attacker claims to be someone else *authorized*
- Falsification (Man in middle)
 - * the attacker changes messages during transmission
- Misappropriation (DDOS)
 - * the attacker prevents legitimate users from accessing resources
- Inside attacks
 - initiated by an entity INSIDE the security perimeter
 - authorization to access system resources but use of them in a malicious way
 - Exposure
 - * the attacker intentionally releases sensitive information to an outsider.
 - Falsification
 - * the attacker alters or replaces valid data or introduces false data into a file or database.
- Outside attacks
 - initiated from OUTSIDE the perimeter, by an unauthorised or illegitimate user of the system
 - Obstruction
 - * the attacker disables communication links or alters communication control information.
 - Intrusion
 - * the attacker gains unauthorised access to sensitive data by overcoming the access control protections.

Security functional requirements

- Information security management requires to:
 1. Identify threats
 2. Classify all threats according to likelihood and severity
 3. Apply security controls based on cost benefit analysis
- Countermeasures to vulnerabilities and threats comprise:
 1. Computer security technical measures
 - access control, authentication and system protection
 2. Management measures
 - awareness and training

3. Both

- configuration management

Defining Information Security

Definition from the NIST computer security handbook:

- The term security is used in the sense of minimizing the vulnerabilities of assets and resources. An asset is anything of value. A vulnerability is any weakness that could be exploited to violate a system or the information it contains. A threat is a potential violation of security.

The CIA Triad

- Confidentiality
 - Preventing unauthorised disclosure of information
- Integrity
 - Preventing modification or destruction of information
- Availability
 - ensuring resources are accessible when required

Information Security Definitions

- Security Service
 - a processing or communication service to give a specific kind of protection to system resources.
 - Types of security services [Lecture Two - Slide 20/27]:
 - * Peer entity authentication
 - * Data origin authentication
 - * Access control
 - * Data confidentiality
 - * Traffic flow confidentiality
 - * Data integrity
 - * Non-repudiation
 - * Availability
- Security Mechanism
 - a method of implementing one or more security services.
 - Types of security mechanisms

- * Encipherment
- * Digital signature
- * Authentication exchange
- * Traffic padding
- * Routing control
- * Notarization