NTNU | Norwegian University of Science and Technology

COURSE INTRODUCTION

TTM4135 - Applied Cryptography and Network Security

Tjerand Silde

05.01.2026

Contents

Lecturer: Tjerand Silde

- Associate Professor in Cryptology at IIK
- Research Group Leader of the NTNU Applied Cryptology Lab (NaCl)
- PhD in privacy and crypto from IMF
- Work as Security and Cryptography Expert at startup Pone Biometrics
- Have earlier taught Linear Algebra, Discrete Mathematics, and Secure Cryptographic Implementations

Head TA: Emil August Hovd Olaisen

- Head Teaching Assistant in TTM4135
- Former Head TA in TTM4158 – Dependable Performance Design
- PhD Candidate in Cryptology at IIK
- Researching post-quantum crypto

Teaching Assistants

- Jonatan Kifle Assefa Aalen
- Prateek Sharma
- Haakon Kirksæter
- Imre Angelo

Curriculum

- The slides will be based on lecture notes from Colin Boyd and Anamaria Costache who taught this course earlier years.
- The old slides are based on Cryptography and Network Security, William Stallings, 8th Edition, but the textbook is a little out of date.
- The syllabus for the examination is defined by the lecture slides (not by the textbook), the exercises, quizzes, practical, and lab assignments.
- We have recommended a few additional books at the course website.

Assessment

The assessment in TTM4135 consists of two parts:

- Portfolio Assignment (40%)
  - five online quizzes based on the slides (10%)
  - practical cryptanalysis exercise (10%)
  - lab milestones and a written report (20%)
- Written Examination (60%)

Make sure to check the course website ttm4135.iik.ntnu.no for information about the assignments and when they are due.

Timetable

- Lecture slots
  - Weeks 2 to 9
  - Mondays 10:15 – 12:00
  - Thursdays 12:15 – 14:00
- Exercise lectures
  - Weeks 3 to 10
  - Mondays 09:15 – 10:00
- Lab assignment
  - Weeks 11, 12, and 13

Check the course website for more details.

Contents

Defining information security

ISO security architecture definition

"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."

- *Information security* can be defined as security where the assets and resources are information systems. This can include data, software and hardware, people and even buildings.

The CIA triad

Traditional definitions of information security are based on the following three information security goals:

Confidentiality: preventing unauthorized disclosure of information

Integrity: preventing unauthorized (accidental or deliberate) modification or destruction of information

Availability: ensuring resources are accessible when required by an authorized user

Passive Threats

Passive threats do not alter information in the system. Such threats may be impossible to detect for users of the system.

Eavesdropping The attacker monitors the communication, for example by sniffing packets or tapping a telephone wire.

Traffic analysis The attacker monitors the amount, source, and destination of communication.

Active threats

Active threats alter information in the system. Such threats may be hard to detect, and detection mechanisms usually comes with a cost.

Masquerade: the attacker claims to be a different entity.

Replay: the attacker sends a message which has already been sent.

Modification: the attacker changes messages during transmission.

Denial of service: the attacker prevents users from accessing resources

Security services and mechanisms

Security service: a processing or communication service to give a specific kind of protection to system resources

Security mechanism: a method of implementing one or more security services

In this course we look closely at *cryptographic* security mechanisms

Main security services

- *Peer entity authentication* provides confirmation of the identity of an entity.
- *Data origin authentication* provides confirmation of the claimed source (origin) of a data unit (message).
- *Access control* provides protection against unauthorized use of resources. Access control service is usually provided in combination with authentication and authorization services.
- *Data confidentiality* protects data against unauthorized disclosure.

Main security services (continued)

- *Traffic flow confidentiality* protects disclosure of data which can be derived from knowledge of traffic flows.
- *Data integrity* detects any modification, insertion, deletion or replay of data in a message or a stream of messages.
- *Non-repudiation* protects against any attempt by the creator of a message to falsely deny creating the data or its contents.
- *Availability service* protects a systems against denial of service.

Main security mechanisms

- *Encipherment* is the transformation of data in order to hide its information content. We will look at both public-key and symmetric-key encryption.
- *Digital signature mechanisms* are cryptographic algorithms which transform data using a signing key. The essential property is that signed data can only be created with the signing key.
- *Access control mechanisms* including access control lists, passwords, or tokens, which may be used to indicate access rights.
- *Data integrity mechanisms* as “corruption detection techniques” which can be used with “sequence information”.

Main security mechanisms (continued)

- *Authentication exchange* mechanisms are protocols which exchange information to ensure identity of protocol participants.
- *Traffic padding* is spurious traffic generated to protect against traffic analysis. Traffic padding is typically used in combination with encryption.
- *Routing control mechanism* is the use of specific secure routes.
- The *notarization mechanism* uses a trusted third party to assure the source or receipt of data. The trusted third party is sometimes called a notary.

Relating security services to mechanisms

Service \ Mechanism	Encipherment	Digital signature	Access control	Data Integrity	Auth. exchange	Padding	Routing control	Notarization
Peer entity authentication	✓	✓		✓				
Data origin authentication	✓	✓						
Access control			✓					
Data Confidentiality	✓					✓		
Traffic Flow Confidentiality	✓				✓	✓		
Data Integrity	✓	✓		✓				
Non-repudiation		✓		✓				✓
Availability				✓	✓			

From Stallings based on X.800. ✓ indicates the mechanism is relevant to provide the service.

Risk management

Risk assessment is a key tool in information security management:

1. Identify threats
2. Classify all threats according to likelihood and severity
3. Apply security controls based on cost benefit analysis

For more details see NIST Special Publication 800-30, Guide for Conducting Risk Assessments, or ISO 27000 standards.

Contents

Course focus

- Cryptography as a foundation for information security
- Applications of cryptography in network security
- We will cover prominent internet security protocols

You need some mathematics for cryptography, and we will cover some in the lectures, but we emphasize usage rather than proofs in this course.

Course content

- Historical encryption
- Symmetric cryptography: block ciphers, stream ciphers, hash functions, and message authentication codes.
- Some mathematics, particularly to support public key cryptography, such as modular arithmetic, basic number theory, and elliptic curves.
- Public key cryptography and infrastructure.
- Introduction to quantum-safe cryptography.
- Transport Layer Security, secure email, and messaging.

How to complete this course successfully?

- Show up and participate to the lectures; ask questions during the lectures and breaks, and try to answer questions in class.
- Show up and participate to the exercise classes: propose exercises we should cover in more detail and ask if you are stuck on something.
- Hand in all of the assignments in a timely manner
  - If anything prevents you from doing so, let us know *as soon as possible*.
- It is very important that you practice new content covered in this course. You will likely not be familiar with a lot of the mathematical tools. They are not overly complicated, but you do need to spend some time practicing.

Questions?