Lecture 1: Introduction and Overview

TTM4135

Relates to Stallings Chapter 1

Spring Semester, 2025

Many thanks to Colin Boyd for the slides

Motivation

What is this course about?

- How does this course run?
- Why is cryptography and network security important?
- What is the connection between cryptography and general information security?
- What is in this course?

Outline

Introduction to the course

Who Needs Cryptography and Network Security?

Role of Cryptography in Information Security

Course outline

Outline

Administration

- Responsible professor: Assoc. Prof. Anamaria Costache
- Scientific assistants:
  - PhD student Lea Nürnberger
- Materials for lectures, exercises, assessment items are on Blackboard.

Textbooks and lecture notes

- Recommended textbook: Cryptography and Network Security, William Stallings, 8th Edition.
- Textbook will be useful to back up lectures. It is a little out of date.
- The syllabus for the examination is defined by the lecture slides, not by the textbook.
- Exercises will be useful for exam preparation.
- Many useful resources online - some will be mentioned on Blackboard.

Assessment

Three items:

- ongoing work during semester (20%)
  - weekly online quizzes (10%)
  - practical cryptanalysis exercise (10%)
- lab milestones and report (20%)
- written examination (60%)

Check timetable on Blackboard for submission dates and other details. Note that the timetable may sometimes be updated. It is *your responsibility* to be up to date with all the changes and check Blackboard periodically.

Timetable

- Lecture times
  - Mondays 12:15 – 14:00
  - Friday 8:15 – 10:00
- Additional class time
  - Friday 10:15 – 11:00 will be used for different purposes — *not* a lecture
- Lab
  - Three weeks starting from when the lecture phase has finished

Check timetable on Blackboard. Note that the timetable may sometimes be updated.

Comparison with last year

- All physical lectures, no recordings
- Most topics and overall format unchanged
- Small updates to lecture material
- Piazza is used for online Q&A
- Please give feedback and *volunteer for the reference group*

Outline

Outline

What is Privacy?

What is Privacy?

In the EU, human dignity is recognised as an absolute fundamental right.
In this notion of dignity, privacy or the right to a private life, to be autonomous, in control of information about yourself, to be let alone, plays a pivotal role. Privacy is not only an individual right but also a social value.

Historically, in other parts of the world, such as the U.S.A., privacy has often been regarded as an element of liberty, the right to be free from intrusions by the state. This distinction between Europe and other parts of the world is relative since it is also an element of privacy in the EU.

https://edps.europa.eu/data-protection/data-protection_en

Privacy – a fundamental right

Privacy – a fundamental right

Almost every country in the world recognises privacy in some way, be it in their constitution or in other provisions.

Moreover, privacy is recognised as a universal human right while data protection is not – at least not yet.

The right to privacy or private life is enshrined in the Universal Declaration of Human Rights (Article 12), the European Convention of Human Rights (Article 8) and the European Charter of Fundamental Rights (Article 7).

https://edps.europa.eu/data-protection/data-protection_en

A few recent headlines – February 2021

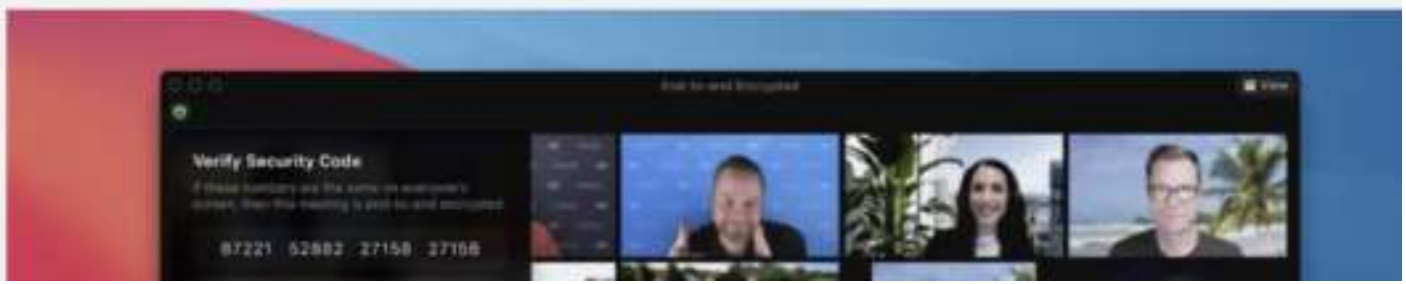
ars TECHNICA

ZOOM CAN'T REDEFINE END-TO-END ENCRYPTION —

Zoom to pay $85M for lying about encryption and sending data to Facebook and Google

Zoom users to get $15 or $25 each in proposed settlement of class-action lawsuit.

JON BRODKIN - 8/2/2021, 9:51 PM

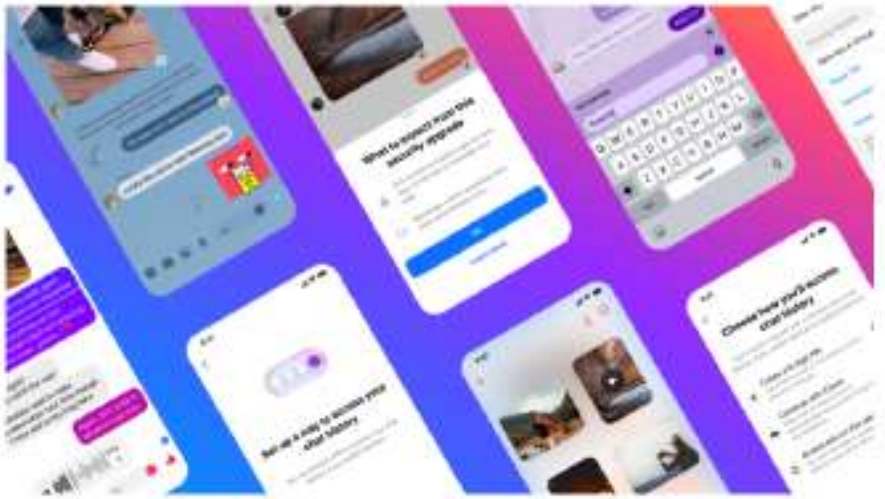


A few recent headlines – December 2023

Messenger

Launching Default End-to-End Encryption on Messenger

December 6, 2023
By Loredana Crisan, Head of Messenger



Takeaways

- We have started to rollout end-to-end encryption for all personal chats and calls on Messenger and Facebook, making them even more private and secure.
- End-to-end encrypted conversations offer additional functionality including the ability to edit messages, higher media quality and disappearing messages.

Outline

Outline

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 three information security goals:

Confidentiality: preventing unauthorised disclosure of information

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

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

OSI Security Architecture X.800

The OSI (Open Systems Interconnection) Security Architecture defines a *systematic approach* to providing security at each layer. It defines security services and security mechanisms that can be used at each of the seven layers of the OSI model to provide security for data transmitted over a network. These services and mechanisms help achieve the CIA goals. Freely downloadable:
http://www.itu.int/rec/T-REC-X.800-199103-I/e

- A bit dated now but still worth looking at. Most definitions and terminology still apply.
- Defines *security threats* (or attacks), *security services* and *security mechanisms* and how they are related.

Useful supplement is Internet Security Glossary, RFC 4949.

Passive Threats

Passive threats do not alter information in the system. Such threats may be hard to detect.

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.

Masquerade: the attacker claims to be a different entity.

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

Modification of messages: the attacker changes messages during transmission.

Denial of service: the attacker prevents legitimate 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 claimed 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 authorisation services.
- *Data confidentiality* protects data against unauthorised disclosure.
- *Traffic flow confidentiality* protects disclosure of data which can be derived from knowledge of traffic flows.

Main security services (continued)

- *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.
  X.800 talks about *nonrepudiation of origin* to protect against denial by the sender of a message, and *nonrepudiation of receipt* to protect against denial by the recipient of a message.
- *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. Later in the course we 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. We will look at standard signature schemes.
- X.800 describes a variety of *access control mechanisms* including access control lists, passwords, or tokens, which may be used to indicate access rights.
- X.800 describes *data integrity mechanisms* as “corruption detection techniques” which can be used with “sequence information”. We will look at the example of message authentication codes.

Main security mechanisms (continued)

- *Authentication exchange* mechanisms are protocols which exchange information to ensure identity of protocol participants. We will study examples such as TLS later.
- *Traffic padding* is spurious traffic generated to protect against traffic analysis. Traffic padding is typically used in combination with encipherment.
- *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	✓	✓		✓				
Nonrepudiation		✓		✓				✓
Availability				✓	✓			

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

Risk management

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.

Outline

Outline

Course focus

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

Need some mathematics for cryptography, but emphasise usage rather than proofs.
Note that you need to be able to use the mathematical tools!

Course content

- Historical cryptography
- Modern cryptography: block ciphers, stream ciphers, public key, hash and MAC.
- Some maths, particularly to support public key. Modular arithmetic, number theory, elliptic curves.
- Public key infrastructure
- Secure email and messaging
- Transport Layer Security (TLS) protocol (HTTPS) and how it uses all of the cryptography

How to complete this course successfully?

- Show up and participate to the lectures – active participation is encouraged!
- Show up and participate to the exercise classes – active particiation is encouraged!
- Hand in all assignments in a timely manner
  - If anything prevents you from doing so, let us know *as soon as possible*
- *Practice!!* It is very important that you practice in your own time! You will likely not be familiar with a lot of mathematical tools. They are not overly complicated, but you do need to spend some time practising.