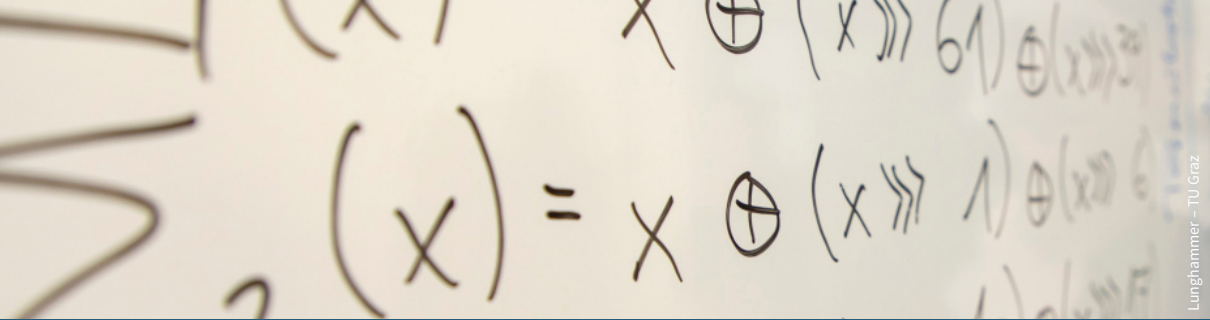
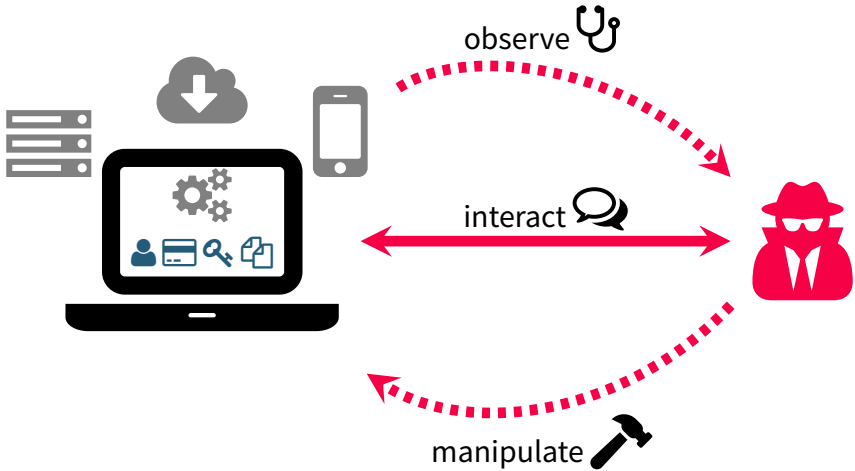


Welcome to "Information Security"

Maria Eichlseder Johannes Feichtner
Daniel Kales Peter Pessl Michael Schwarz

Winter Term 2019/20

Information Security



Information Security – Topics

Cryptography

- How to exchange information securely while everyone's watching?
- The mathematical perspective

System Security

- How to perform computations securely while sharing a processor?
- The system perspective

Network Security

- How to establish secure internet connections?
- The application perspective

Outline

Today: Introducing…

- The Team
- This Course
- Information Security
- Cryptography

TU Graz

SCIENCE
PASSION
TECHNOLOGY

Introduction to “Information Security”

Maria Eichlseder

Information Security – WT 2019/20

The Team

Who are we?

System Security

Cryptology & Privacy

Formal Methods

Secure **Applications**

Team for the Lecture

Maria Eichlseder

Cryptography
Administration

- Assistant Professor
- Cryptology & Privacy

Michael Schwarz

System Security

- PhD Candidate
- System Security

Johannes Feichtner

Network Security

- PhD Candidate
- Secure Applications

Team for the Exercises

Daniel Kales

Administration

- PhD Student
- Cryptology & Privacy

Peter Pessl

- Postdoc
- System Security

Johannes Feichtner

- PhD Candidate
- System Security

Teaching Assistants for the Exercises

Lena Heimberger

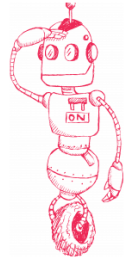
Martin Haubenwallner

Lukas Lamster

Michael Ehrenreich

Alexander Prutsch

BACHELOR'S **THESIS**



You want to do your bachelor's thesis with us? Great!

You'll agree on a topic with your advisor. Below, we list some open topics that we are currently interested in. If you have your own idea for a potential topic, get in touch with any advisor to see whether they want to supervise your thesis.

OPEN **TOPICS**

System Security

Analyzing Address Leakage	Samuel Weiser
Address Leakage Visualization	Samuel Weiser
Infosec needs you!	LosFuzzys
Spying on Hobbits - or how secure constant-time really is	Peter Pessl
Memory Encryption and Authentication	Mario Werner
Fault Attacks against MORUS/AEGIS	Robert Primas

Cryptology & Privacy

Attacks on AES with a Single Secret S-Box	Lorenzo Grassi
A Zoo of Lightweight Ciphers	Maria Eichlseder
Peer-to-Peer Contact Discovery on Smartphones	Daniel Kales
Case Study: Nonces in Practice	Maria Eichlseder
Evaluation of Cryptographic Functions against Fault Attacks	Robert Primas, Maria Eichlseder
Experimental Evaluation of Fault Attacks	Maria Eichlseder, Robert

This Course

Administrative Information

Is this “Introduction to Information Security”?

- Old curricula 15U, 16U: “Introduction to Information Security” aka IIS, EIS
  no longer offered – you can still do the VO exam on 17 Oct, 19 Nov, 14 Jan
- New curricula 19U: “Information Security” aka InfoSec
  this course is **new** and replaces IIS

- IAIK equivalence list: `https://teaching.iaik.tugraz.at/equivalences`

New (CS, ICE, SEM)				Old (SEM)				Old (CS, ICE)			
InfoSec	VO	2.5 SSt	4 ECTS	IIS	VO	2 SSt	3 ECTS	IIS	VO	2 SSt	3 ECTS
InfoSec	KU	2.5 SSt	3 ECTS	IIS	KU	1 SSt	1.5 ECTS	IIS	KU	1 SSt	1.5 ECTS
								RKN	KU	1 SSt	1.5 ECTS

- Questions? Contact your student representation Bits or your Dean of Studies

Schedule

- 9:30–12:00 Lecture
  - actually around 9:40–11:50
  - 60 min lecture + 10 min break + 60 min lecture
- 12:00–13:30
- 13:30–15:00 Practicals
  - not every week
  - presentation of assignments, tutorials, question time

Date	Lecture Fri 9:30–12:00	Practicals Fri 13:30–15:00
04. 10. 2019	Cryptography 1 – Introduction	P1 Kick-off Tutorial
11. 10. 2019	Cryptography 2 – Symmetric Authentication	
18. 10. 2019	Cryptography 3 – Symmetric Encryption	P1 Tutorial
25. 10. 2019	Cryptography 4 – Asymmetric Cryptography	
04. 11. 2019		P1 Deadline (Monday!)
08. 11. 2019	System Security 1	P2 Kick-off Tutorial
15. 11. 2019	System Security 2	
22. 11. 2019	System Security 3	P2 Tutorial
29. 11. 2019	System Security 4	
06. 12. 2019	Nikolaus Special	P2 Deadline
13. 12. 2019	Network Security 1	P3 Kick-off Tutorial
❄ ❄ ❄		
10. 01. 2020	Network Security 2	P3 Tutorial
17. 01. 2020	Network Security 3	
24. 01. 2020	Network Security 4	P3 Deadline
31. 01. 2020	Exam	

Course Goals

Understand the foundations of secure applications:

- Understand which security properties crypto algorithms offer
- Be able to choose & properly apply suitable crypto algorithms
- Know potential risks when processing data
- Detect certain vulnerabilities in implementations
- Know isolation techniques and protection mechanisms
- Understand attacks and defenses for network protocols & web technologies
- **Understand security aspects on all abstraction layers of secure internet communication**

Prerequisites

This course will be a lot easier if you remember stuff from

- Discrete Mathematics
- Computer Organisation / Computernetworks and -Organisation
- System-Level Programming
- Various programming practicals
  Useful for the KU: `C/C++`, `gdb`, Assembler, `Java`, `Python`,...

How do I get a grade?

Lecture (VO):

- Final written exam
  - 90 minutes, closed-book, pen-and-paper
  - Questions in English
  - Answers in English or German
- First exam date: 31 Jan 2020

Practicals (KU):

- Team programming exercises
- 3 Assignments – more details at 13:30!

Links

- Course website:
  - https://www.iaik.tugraz.at/infosec
  - Slides, administrative info, links
- Newsgroup
  - Newsserver news.tugraz.at
  - graz.lv.infosec for questions, news
  - graz.lv.infosec.groupsearch to find partners for the practicals
- STicS:
  - https://stics.iaik.tugraz.at
  - Team registration

Contact & Finding Help

https://www.iaik.tugraz.at/infosec

infosec@iaik.tugraz.at or the responsible lecturer

If you need help for the exercises, try (in this order):

- Newsgroup `graz.lv.infosec`
- Contact the responsible teaching assistant
- Contact infosec@iaik.tugraz.at or the responsible lecturer

This lecture is not based on a particular book, but there are many great books on information security – ask us if you need recommendations

Questions

TU Graz

SCIENCE
PASSION
TECHNOLOGY

Cryptography 1: Introduction

Maria Eichlseder

Information Security – WT 2019/20

Information Security

A Brief Introduction


“Sicherheit”?
(1.) Safety
Adversary / Attacker
(2.) Security

Security

=

se(d) (without) + cura (care, anxiety)

freedom from anxiety

What are we anxious about?

Asset

An **asset** is anything (e.g., an information, a service, a device…)
that has value to an entity (e.g., an organization or a person).

- Identifying assets (precisely) is the first step of any security analysis.
- Security mechanisms often shift the problem of protecting one asset to protecting another (e.g., password)

When do we consider it “protected” or “secure”?

Security Property 

A **security property** defines something that makes the asset valuable.

Main security properties:

- **C**onfidentiality
- **I**ntegrity and Authenticity
- **A**vailability

Some other security properties:

- Anonymity and Privacy
- Non-repudiation of origin & delivery
- Commitment
- Time-stamping
- …

What could possibly go wrong?

Threat

A **threat** describes a potential violation of security.

The sum of all threats describes everything that can lead to a violation of a security property of the asset.

Typically threats can be grouped to hierarchical classes of a threats that form an “attack tree”.

- Add protection mechanisms to minimize the threats and attack surface
- Repeat that until the risks of the remaining threats are acceptable

Something did go wrong…

Vulnerability

A **vulnerability** is a concrete flaw or weakness in a system that can be exploited by one or more threats

Preventing vulnerabilities that can be exploited by a threat:

- is not trivial :)
- Use established standardized security mechanisms and use them correctly
- Test and verify security features

Enter: The Adversary

Attack

An **attack** is a concrete attempt to violate one of the security properties of an asset.

- Prepare for the fact that things can go wrong
- Update mechanisms, logging, tracing mechanisms

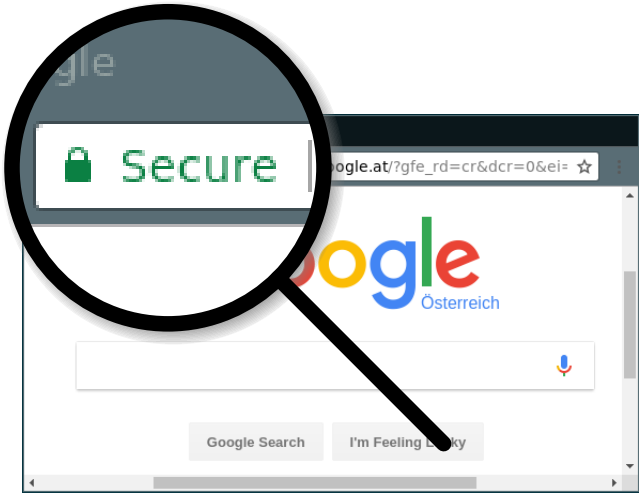
Information Security: Break the Chain

Asset + Security Properties ⛓ Threat ⛓ Vulnerability ⛓ Attack

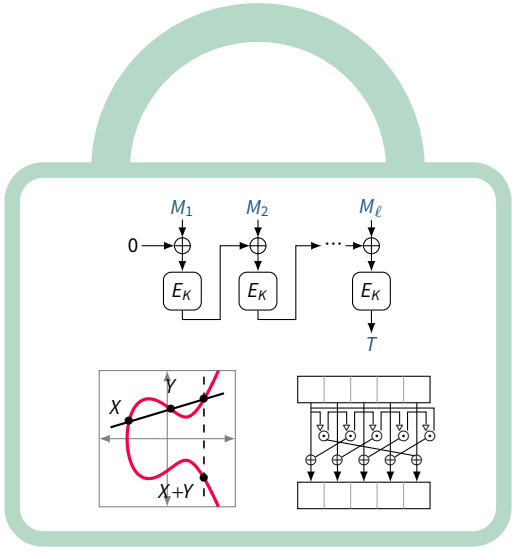
Cryptography

A Brief Introduction

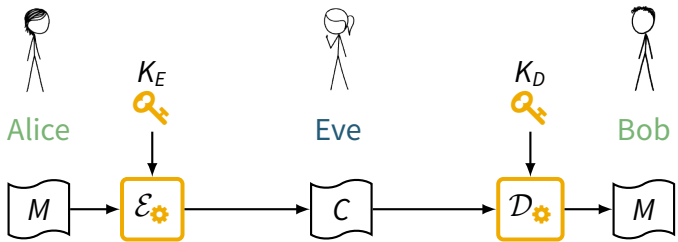
Cryptography – The mathematical backbone of information security



Cryptography – What's inside the padlock?



Secure Communication



Kerckhoffs' principle

Algorithms $\mathcal{E}, \mathcal{D}$ public – Security based on keys K_E, K_D

Basic terminology

- Entities / parties: Alice and Bob
- Adversary: Eve

- Plaintext / message: M
- Ciphertext: C
- Keys: K_E, K_D

- Cryptographic primitive & scheme (cipher): $\mathcal{E}, \mathcal{D}$
- Cryptographic protocol: How to use the primitives

Historical examples

This basic scenario reflects the typical historical (usually military) context:

- Scytale cipher (Sparta) 
- Caesar cipher (Rome) 
- Vigenère cipher (16th century Italy) 
- Enigma machine (1920s–1940s, Nazi Germany) 

The Vernam Scheme (One-Time Pad)

- M, C, K are strings of length N over the alphabet $\{0, 1, \ldots, L-1\}$
- each key character is **randomly** generated and used only **once**
- Encryption:

$$C_i = M_i + K_i \bmod L \qquad i = 1, \ldots, N$$

- Symmetric encryption with perfect secrecy!

Perfect secrecy

- Given an intercepted ciphertext `QUIZZ`:
  - The key `16-5-19-14-21` decrypts it to the message `APPLE`
  - The key `5-16-22-11-12` decrypts it to the message `LEMON`
  - …
- For all 5-character words, there is a key that decrypts `QUIZZ` to that word.
- The ciphertext gives no information about the message

Why other encryption primitives ?

- Long keys are impractical
  How to generate, exchange, store, access, authenticate, … ?

- Protecting the new asset (= long key) isn't much easier than the original one (= message)

→ Purpose of encryption primitives:

- Provide real-world (non-perfect) secrecy
- Using a key as small as possible
- With an algorithm as fast as possible

In the 1970s: The dawn of modern cryptography

- Before 1970s, cryptography is the domain of military & intelligence agencies
- In the 1970s, commercial applications for everyone emerge
- Triggers many innovations in open cryptographic research
  - “Open-source” symmetric crypto to protect everyone’s communication
  - Asymmetric crypto to establish new communication channels
- Cryptography research is moving on, but 1970s crypto is still everywhere!
  - `DES/3DES` block cipher, `MD` hashing, `DH` key exchange, `RSA` signatures, …

Modern crypto algorithm: two families

Symmetric (secret-key) cryptography

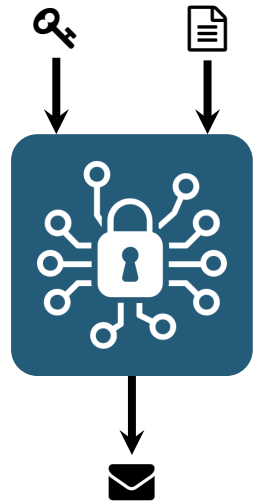
- the secret key is shared and known by Bob and Alice alone
- sender and receiver can be interchanged (insider/outsider view)

Asymmetric (public-key) cryptography

- Bob and Alice use different keys
- public keys and private keys (known only by owner – user-centric view)
- enables advanced protocols, but primitives more difficult to design (?)

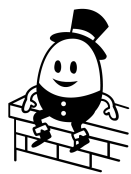
Cryptographic primitives

- Somehow, we need to turn a bunch of simple CPU instructions into a magic box with “unpredictable” behaviour that provides a defined **security level**
- The cryptographic primitive is where this magic happens
- Processes fixed-size inputs, specification is public
- Not meaningful to use by itself, needs a scheme
- Examples:
  `AES` block cipher, `RSA` trapdoor one-way function



Cryptographic security

> *"When I use a word,"* Humpty Dumpty said, in rather a scornful tone,
> *"it means just what I choose it to mean – neither more nor less."*



Security proof: A proof of some property, not a guarantee of security

3 Shades of “security” in cryptography

1. **Information-theoretic**: unconditional, perfect security
2. **Complexity-theoretic**: reduce security to “hard” problems
3. **Cryptanalytical**: secure against state-of-the-art cryptanalysis

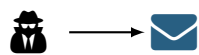
Attacks – What does the Adversary want?

- Confidentiality break:

  Read secret messages?

- Authenticity break:

  Forge a ciphertext or signature?

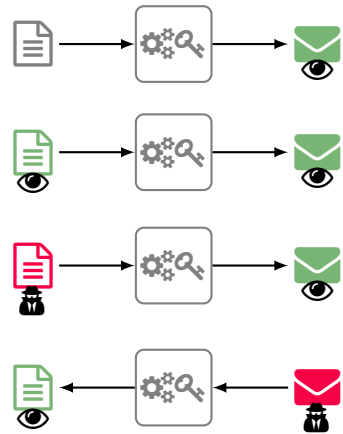


- Full break: Recover the key?

- …?

Attacks – What are the Adversary's abilities?

- Ciphertext-only attack?
- Known-plaintext attack?
- Chosen-plaintext attack?
- Chosen-ciphertext attack?



Terminology: The Adversary asks "Queries" to the "Oracle"

Attacks – What can the Adversary exploit?

- Black-box attack:

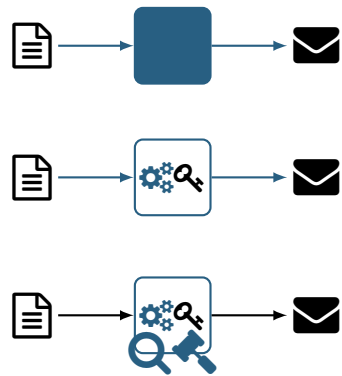
  Exploit only the interface?

- Dedicated black-box attack:

  Exploit the specification of the algorithm?

- Gray-box attack:

  Cheat with side-channels, faults, …?



Conclusion

- Information security protects assets against adversaries
  - Break the chain:
    Security Property ⚯ Threat ⚯ Vulnerability ⚯ Attack
- Cryptography is the mathematical foundation of secure communication
  - Algorithms to transform data so it can be sent over untrusted channels
  - Creates a new asset: the key

Lecture Outlook – October

C2 – Symmetric Authentication

- Goal: Integrity
- Hash functions
- Message Authentication Codes (MACs)
- Useful primitives

C3 – Symmetric Encryption

- Goal: Confidentiality
- (Authenticated) Encryption (AEAD)
- Construction of a primitive

C4 – Asymmetric Cryptography

- Goal: Establishing authentic communication
- Key exchange
- Signatures
- Asymmetric primitives

Questions

Questions for You

- Assets?
- Threats?
- (Potential) vulnerabilities?
- (Potential) attacks?

Questions for You

- What are the advantages of “open-source” crypto specifications (Kerckhoffs’ principle)? Disadvantages?
- What is a cryptographic key?
  What’s the key size and how is it relevant?
- What are some notions of cryptographic security?