

# Mobile Security

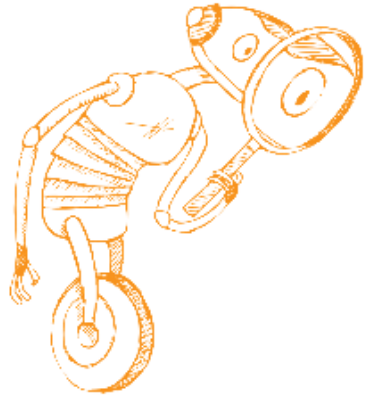
SS 2021



Johannes Feichtner

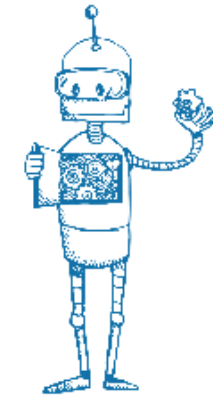
[johannes.feichtner@iaik.tugraz.at](mailto:johannes.feichtner@iaik.tugraz.at)

WE **UNITE RESEARCH** ON ALL ASPECTS OF INFORMATION SECURITY  
TO **FIND ANSWERS** TO THE PRESSING SECURITY CHALLENGES.



**FORMAL  
METHODS**

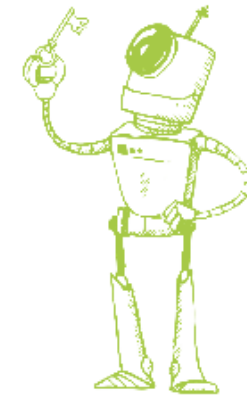
**SECURE  
SYSTEMS**



**SECURE  
APPLICATIONS**

Tools and Innovations  
for Security

**CRYPTOLOGY &  
PRIVACY**



## Team Tauber

**EGIZ** is a research group at IAIK that consists of a young and dynamic team. A high level of expert knowledge in many areas of information technology is necessary for further developing eGovernment. EGIZ supports the Federal Ministry for Digital and Economic Affairs in further developing the ICT strategy of the federal government, and it conducts research in the area of technical innovations in the eGovernment environment. We are driven by advancing technologies in the field of identity management, digital signatures and other security technologies in eGovernment, like electronic delivery. We aim to facilitate the adoption and shift towards new technologies in public services like mGovernment, cloud computing or distribute ledgers. For the latest research projects see the [EGIZ Demo Portal](#).

### Team Members

<b>Arne Tauber</b>	Stephan Keller
Andreas Abraham	Thomas Lenz
Emina Ahmetovic	Christof Rabensteiner
Felix Hörandner	Kevin Theuermann

## Team Lipp

With our long reputation as a pioneer in security software development, we provide a comprehensive set of crypto products for the Java™ platform that helps you make your environment and applications more secure. While we focus on the areas of eID, eSignatures and PKI where we are also involved in standardisation activities, our implementations cover underlying crypto, from AES via elliptic curves to post-quantum methods up to protocols like TLS, tools like policy-driven automated trust verifiers or applications like certification authority software. Whenever ready, our partner, [Stiftung SIC](#), is responsible for all sales of these products.

### Team Members

<b>Peter Lipp</b>	Simon Guggi
Lukas Alber	Reinhard Lüftenegger
Dieter Bratko	Stefan More
Harald Bratko	Franco Nieddu
Otto Gerald Touzil	Olamide Omolola

## Team Leitold

The **A-SIT** team's research at IAIK is driven by information security needs of the public sector, like in eGovernment. We are thrilled by exploring technologies that help advance the public sector secure electronic service offerings. We have expertise in basic building blocks like electronic signatures and electronic identity. With mGovernment initiatives and mobile-first strategies, a current research focus is on mobile security, like on app security analysis. We also research on the role of emerging concepts like distributed ledger or peer-to-peer infrastructures in public services. For some recent results see the [A-SIT Technology Server](#).

### Team Members

<b>Herbert Leitold</b>	Gerald Palfinger
Edona Fasllija	Reinhard Posch
Johannes Feichtner	Bernd Prünster
Christian Kollmann	Peter Teufl
Alexander Marsalek	Thomas Zefferer
Dominik Mocher	Dominik Ziegler

SECURE  
APPLICATIONS



# A-SIT

<https://www.a-sit.at>

- Members
  - Federal Ministry of Digital and Economic Affairs
  - Central bank of the Republic of Austria
  - Federal Computing Centre
  - Graz University of Technology
  - Danube University Krems
- IAIK: IT Security Research
- A-SIT: Practical aspects + Counseling of public institutions



# Myself

- A-SIT @ IAIK
- Current focus
  - Smartphones
  - Browser & Network Security
- Lectures
  - Mobile Security (MobileSec)
  - Computer Organisation and Networks (CON)
  - Information Security (InfoSec)
  - (Computer and Communication Networks (RKN))
- Seminar projects, theses



Johannes Feichtner  
[johannes.feichtner@iaik.tugraz.at](mailto:johannes.feichtner@iaik.tugraz.at)

# Course Facts

## Lecture (705.012)

- Registration Deadline: 14.03.2021, 23:59
- 3 ECTS credits
- Elective master course (+ part of InfoSec catalog)

## Assignments (705.013)

- Deadline as above
- 2 ECTS credits

# Course Organisation

## Lecture

- English
- Thursdays, 10:00 to 12:00

## Assignments

- Thursdays, 12:00 to 13:00 **but** discussions only, no general „topic“ or lecture
- Your task: *Do research and fast prototyping*
- Outcome depends on your initiative
- Could be a seed for theses, projects, and further research

## MOBILE SECURITY


Course Number 705012 and 705013 | Sommersemester 2021

### Content

This course is a seminar-style class which focuses on security aspects of mobile devices. We study the security mechanisms of smartphones and show how to employ them to protect sensitive information. Based on that, we analyze mobile applications regarding security-critical deficiencies, examine platform and application vulnerabilities and discuss how they can be exploited by attackers.

- Security features of mobile platforms, e.g. Android, iOS, ...
  - *Access protection (PIN, Patterns, ...), Secure Element, OS updates, permissions, sandboxing, ...*
  - *Which mechanisms are provided in order to protect sensitive data?*
  - *How do they work?*
- Key and data storage on mobile devices
  - *Device encryption, key derivation functions, key management, risks*
  - *Which kind of keys do you manage on your device?*
  - *In practice, what are the risks you have to cope with?*
- Using mobile devices for identity management
  - *Mobile e-signatures, threats*

### Lecturers

 Johannes Feichtner

### Table of Content

- > [Content](#)
- > [Material](#)
- > [Administrative Information](#)
- > [Lecture Dates and Exams](#)
- > [Lecturers and Teaching Assistants](#)

<https://iaik.tugraz.at/mobilesec/>



# Assignments

- Two subsequent tasks
  - The first to do individually
  - The second to do in a group of max. 3 people
  - For a positive grade, **>= 50% per assignment needed!**
- **Your** creativity, skills, and ideas form an **integral** part
- Focus on research, fast-prototype oriented work
  - Can serve as basis for future projects, theses, etc

# Assignment - Task 1

To solve individually!  
(no group work)

Soft introduction to application analysis

- Requirements:
  - Acquired in „Computer and Communication Networks“ / „Information Security“
  - Man-in-the-middle (MITM)
  - Certificate Pinning

**Analyze** a set of Android or iOS applications

- Find out if they are susceptible to MITM, make use of Pinning
- Reverse Engineering

**Submit** your results until 10.04.2020 and explain your findings

# Assignment – Task 2

Max. group size: 3

- Topics will be suggested **but**
  - You are very welcome to bring in your own ideas, related to the lecture!
- **Decide** on a topic until 21.03.
- Final presentation: 10.06.
  - Hand-in: 08.06.
- Grading depends on contribution / results

# Next Steps

- Register to the lecture and assignments courses [until 14.03., 23:59.](#)
- Assignments – Task 1: Think about apps you would like to analyse
  - Early start is possible 😊
- Assignments – Task 2: Think about a topic you would like to work on
  - Choose from the list of topics **or** propose your own subject
  - Decide on one [until 21.03.](#)

**Questions?**