IAIK TU Graz

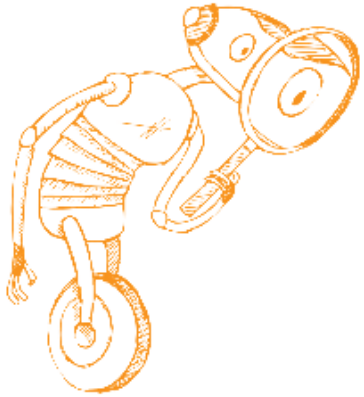
Mobile Security

SS 2023

Florian Draschbacher
florian.draschbacher@iaik.tugraz.at

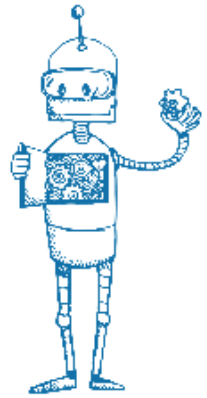
Some slides based on material by **Johannes Feichtner**

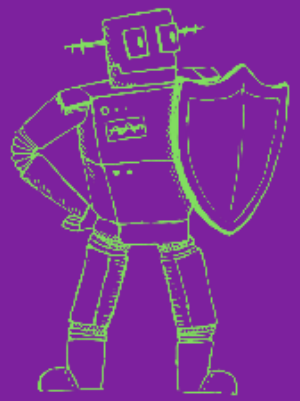
WE **UNITE RESEARCH** ON ALL ASPECTS OF INFORMATION SECURITY
TO **FIND ANSWERS** TO THE PRESSING SECURITY CHALLENGES.



FORMAL
METHODS

SECURE
SYSTEMS

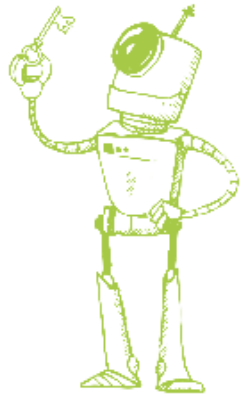




SECURE
APPLICATIONS

Tools and Innovations
for Security

CRYPTOLOGY &
PRIVACY



IAIK TU Graz

Team A-SIT

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 artificial intelligence in public services. For some recent results see the A-SIT Technology Server.

Team Members

Emina Ahmetovic
Florian Draschbacher
Edona Fasllija
Jakob Heher
Stephan Keller
Karl Koch
Stefan Kreiner
Herbert Leitold
Thomas Lenz
Stefan More
Gerald Palfinger
Blaž Podgorelec
Lukas Posch
Arne Tauber
Hannes Weissteiner

Team SIC

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, CMS or S/MIME, or applications like certification authority and cloud based mobile signature solutions. Whenever ready, our partner, Stiftung SIC, is responsible for all sales of these products.

Team leaders are Harald Bratko and Thomas Zefferer.

Team Members

Dieter Bratko
Harald Bratko
Fabian Gruber
Simon Guggi
Adrian Lukas Jury
Verena Schröppel

Team A-SIT+

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 leader is Peter Teufl.

Team Members

Peter Teufl
Felix Hörandner
Christian Kollmann
Bernd Prünster
Thomas Zefferer

SECURE APPLICATIONS

IAIK TU Graz

SECURE APPLICATIONS

Team A-SIT

Research & Teaching

eGovernment

Mobile Security

Self-Sovereign Identity

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

Emina Ahmetovic
Florian Draschbacher
Edona Fasllija
Jakob Heher
Stephan Keller
Karl Koch
Stefan Kreiner
Herbert Leitold
Thomas Lenz
Stefan More
Gerald Palfinger
Blaž Podgorelec
Lukas Posch
Arne Tauber
Hannes Weissteiner

Team SIC

Java Crypto

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 implementation covers underlying crypto, from AES via elliptic curves to post-quantum methods up to protocols like TLS, CMS or S/MIME, or applications like certification authority and cloud based mobile signature solutions. Whenever ready, our partner, Stiftung SIC, is responsible for all sales of these products.

Team leaders are Harald Bratko and Thomas Zefferer.

Team Members

Dieter Bratko
Harald Bratko
Fabian Gruber
Simon Guggi
Adrian Lukas Jury
Verena Schröppel

Team A-SIT+

Operational Projects
(mostly for public sector)

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 leader is Peter Teufl.

Team Members

Peter Teufl
Felix Hörandner
Christian Kollmann
Bernd Prünster
Thomas Zefferer

IAIK TU Graz

A-SIT

https://www.a-sit.at

- Members
  - Federal Ministry of Digital and Economic Affairs
  - Federal Computing Centre (BRZ)
  - Graz University of Technology
  - Danube University Krems
  - Johannes Kepler University Linz

- IAIK: IT Security Research
- A-SIT: Practical aspects + Counseling of public institutions

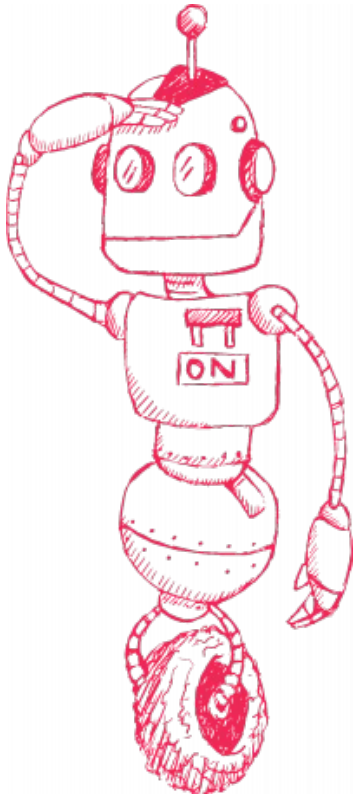
Myself

- A-SIT @ IAIK
- Current focus
  - Vulnerability Detection and Mitigation in Apps
  - Mobile Security
  - Android and iOS
  - Application Patching
- Lectures
  - Mobile Security (MobileSec) VO & KU
- Seminar projects, theses

Course Facts

Lecture (705.012)

- Registration Deadline: 20.03.2023, 23:59
- 3 ECTS credits
- Elective master course (+ part of InfoSec catalog)



Assignments (705.013)

- Deadline as above
- 2 ECTS credits

Course Organisation

Lecture

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

Assignments

- Fridays, 12:00 to 13:00 **but** discussions only, no general „topic“ or lecture
- Your task: ***Do research and fast prototyping***
- You are welcome to suggest your own project ideas!
- Could be a seed for theses, projects, and further research

MOBILE SECURITY (SS 2023)

Course Number 705012 and 705012 | Sommersemester 2023

Lecturers

Florian Draschbacher

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 Architectures of Android and 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?*
- Common security mistakes in mobile applications
  - *Responsibilities of app developers*
  - *Proper use of access protection for files and data*
  - *Securing communication channels*
- Key and data storage on mobile devices
  - *Device encryption, key derivation functions, key management, risks*

Table of Content

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

We have a Discord channel!

- For asking questions regarding assignments, exams, …
  - Ask on Discord if your question is relevant for others as well!
- Receiving updates on organisational matters

1. Join IAIK server
   https://discord.gg/66ZnGV8jJa

2. React with 📱 emoji in getting-started channel

3. You are automatically granted access to mobilesec channel

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 Organization and 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
- Task details on course website and in next week‘s lecture

Submit your results until 17.04.2023 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 31.03.

- Final presentation: 16.06.
  - **Hand-in:** 12.06.

- Grading depends on contribution / results

Next Steps

- Register to the lecture and assignments courses until 20.03., 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 31.03.

Getting to know you

fbr.io/mobsec

What is your experience with Mobile Security?

Getting to know you

fbr.io/mobsec

What are your expectations for the lecture?

Questions?