

# Advanced Security for Systems Engineering WS18

## Lecture 00: Preliminary Discussion

Florian Fankhauser  
Christian Schanes



# ESSE



- Institute of Information Systems Engineering
- Research Group for Industrial Software (INSO)
- Working Group Establishing Security (ESSE)
- Lectures
  - Introduction to Security (*WS, Bachelor*)
  - Security for Systems Engineering (CTF-Contest) (*SS, Bachelor*)
  - Advanced Security for Systems Engineering (*WS, Master*)
  - IT Security in Large IT Infrastructures (CTF-Contest) (*SS, Master*)
  - Seminar on Security
  - Projects
  - Bachelor Thesis, Master Thesis, PhD Thesis

## Research Topics (Excerpt)

- Electronic Payments
- Large IT Infrastructures
- Connected Cars
- Secure and Anonymous Communication
- Embedded Security and Internet of Things
- Governance, Risk and Compliance
- eHealth
- Penetration Testing, Security Audits, Security Certification
- Identification, Authentication and Authorization, eID solutions
- IT Security Teaching Methods

## Excerpt of Applying Subject Areas

- Malware and Internet Crime
- Physical Security of IT Systems
- Applied Cryptography
- Exploit Development, Offensive Computing, and Exploit Mitigation
- Rootkits and OS Security
- Honeypots, Honeynets, and Honeytokens
- Mobile Security
- Privacy-Protection in Cloud/Mobile Applications
- Security Usability for End-2-End Security
- Security Engineering in the Software Life-Cycle

- Questions regarding Advanced Security for Systems Engineering
  - <https://security.inso.tuwien.ac.at/>
  - Tuwel forum
  - lva.security@inso.tuwien.ac.at – please state the lecture name as this e-mail address is used for multiple lectures
  - *Please don't use other ways, e.g., Tuwel submission comments*
  
- Office Hour on agreement, Exercise Interviews, . . . :  
Wiedner Hauptstraße 76/2/2
  
- esse@inso.tuwien.ac.at

# Advanced Security for Systems Engineering VU WS18



## Aim of the Lecture

The class covers *advanced aspects* of multiple topics of *IT security* based on a *broad overall view of IT security* using *theoretical lectures*, *guest lectures giving insights in “real life“ of IT security* and *exciting exercises*.

When having finished this course the students shall have the *skills* to timely *recognize advanced aspects of IT security* and introduce *appropriate security measures* in order to achieve a *sufficient level of IT security* during the operation of the respective systems.

We expect of you *interest in IT security*, *commitment*, also in regard to the exercises, and the *endeavor for good results*.



- 8 lectures and guest lectures
- 1 test, registration via TISS needed
- Grading: 60% exercises, 40% test, starting with the first submission of a lab a certificate will be issued
- The test as well as the exercises have to be positive (i.e., more than 40 resp. 60 points)
- Course material: slides, notes, literature references (library)
- Registration via TISS until October 12, 2018

# Overview Exercises

- 3 exercises (1 individual, 2 in teams)
- Exercises are mandatory, lab0 is final registration
- Team registration, submission of exercises etc. in tuwel
- Operating system used for exercises: Mainly Linux

## Course Discontinuation

- Sometimes, you recognize your goals were set too high. . .
- Be fair to your team colleagues: inform your colleagues and us ([lva.security@inso.tuwien.ac.at](mailto:lva.security@inso.tuwien.ac.at)) directly after your decision
- Consequence: negative certificate after first submission

## Registration for Teams

- Registration for teams in tuwel
- You have to registrate yourself for a team
- Tewel forum may be helpful for finding a team
- Before joining a team with members you don't know, please ask :)
- If you don't know anyone and can't find a team please join the tuwel team *Random Assignment After Deadline* and we will assign you to a team after the deadline for the team registration.
- Arrangement of teams is mandatory (otherwise, 0 points for lab1/lab2)
- If there are problems in teams, please write ASAP an e-mail to [lva.security@inso.tuwien.ac.at](mailto:lva.security@inso.tuwien.ac.at)

- Communication should be encrypted nowadays
- X.509 standard is currently state of the art
  
- ESSE has its own Certification Authority (CA) for
  - Lab resources
  - Partly e-mail communication
  
- Download of the ESSE Root CA certificate via the ESSE website and also as a second path via tuwel
- Add it to your trusted CAs, otherwise you will probably get errors

# Note on Attacks on the IT Security of Systems

- You will learn precise attacks on IT systems in the course
- This is only
  - to better understand IT security
  - secure your own IT systems
  - test your own IT systems in regard to the security level
  - and/or use in other legal ways
- Attacking TU Wien or conducting attacks based on systems of TU Wien may lead to the withdrawal of your eligibility to study
- Exception: Attacks within our lab in order to achieve the assignments are OK :-)

## Planned Lectures – 1/2

- 05.10.2018** Preliminary Discussion
- 12.10.2018** Web Application Security
- 19.10.2018** Secure Architectures
  
- 09.11.2018** Advanced Attacks on Applications 1
- 16.11.2018** Advanced Attacks on Applications 2
- 23.11.2018** Applied Cryptography
- 30.11.2018** Forensics

**07.12.2018** TBA

**14.12.2018** IT Security in the Field: Passport Security

**21.12.2018** TBA

**11.01.2019** Mobile Applications

**18.01.2019** Test

**25.01.2019** Inspection of the Test in Wiedner Hauptstraße 76/2/2

**SS2019** 3 Additional Tests



## Planned Exercise Dates

**lab0** 20 points, exercise has to be finished alone,  
17.10.2018–31.10.2018

**Building of teams for lab1 and lab2** 05.11.2018–12.11.2018

**lab1** 50 points, team exercise, 14.11.2018–05.12.2018

**lab2** 50 points, team exercise, 05.12.2018–16.01.2019

**examination for lab1/lab2** 21.01.2019–23.01.2019

*Please note:*

ESSE exercises traditionally begin at 11:55pm

# Support for Questions Regarding the Lecture

- Questions that are interesting/should be visible for other students as well
  - Tuwel forum
  - *Please note: We do not monitor other forums*
  - *Please do not use other ways, e.g. Tuwel submission comments*
  
- Specific questions
  - `Iva.security@inso.tuwien.ac.at` – please state the lecture name as this e-mail address is used for multiple lectures
  - Office hour

- Ross Anderson. *Security Engineering. A Guide to Building Dependable Distributed Systems*. Wiley Publishing, Inc., 2 edition, 2008. ISBN 978-0-470-06852-6. <http://www.cl.cam.ac.uk/~rja14/book.html>
- Ed Skoudis and Tom Liston. *Counter Hack Reloaded. A Step-by-Step Guide to Computer Attacks and Effective Defenses*. Pearson Education, Inc., 2 edition, 2006. ISBN 0-13-148104-5
- Matt Bishop. *Computer Security: Art and Science*. Pearson Education, Inc, 2003. ISBN 0-201-44099-7
- Bruce Schneier. *Secrets & Lies: Digital Security in a Networked World*. Wiley Publishing, Inc., Indianapolis, Indiana, 2004. ISBN 0-471-45380-3

- Florian Fankhauser, Christian Schanes, and Christian Brem. Sicherheit in der softwareentwicklung. In *Softwaretechnik - Mit Fallbeispielen aus realen Entwicklungsprojekten*, chapter 13, pages 589–646. Pearson Studium, München, 1 edition, 2009

**Thank you!**

<https://security.inso.tuwien.ac.at/advsecsyseng-ws2018/>

