

# IT Security in Large IT Infrastructures SS18

## Lecture 00: Preliminary Discussion

Florian Fankhauser

Christian Schanes

Christian Brem

Franz Mairhofer



# 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 IT Security in Large IT Infrastructures
  - <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

# IT Security in Large IT Infrastructures SS18



At the end of the term the students of the lecture should have the *abilities* to *recognize* and *establish security aspects* in software projects in *large IT infrastructures* timely in order to achieve a *sufficient level of IT security* during the operation of the specific software project.

A *focus* is put on the *understanding how IT security is managed in large IT infrastructures* and *why* specific *security measures work* or *don't work*.



- 8 lectures and guest lectures
- 1 written exam, registration mandatory
- Grading: 50% exercises, 50% test, after the first submission a certificate is issued
- Test + exercises have to be passed, i.e., you need to earn more than 50 points respectively
- Documents: slides, written notes, literature references
- Please consider: Slides only may not be enough for the test
- Registration for the course in TISS until 09.03.2018

- 3 labs (1 individual, 2 in teams (incl. CTF contest))
- Exercises mandatory, lab0 is final registration
- Team registration, exercise submission etc. in tuwel
- Exercise interview for lab1 in Wiedner Hauptstraße 76/2/2
- CTF contest takes place on Sat June 09, 2018, full-day
- ESSE CA Certificate for secure access to ESSE resources can be downloaded in tuwel

## 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, do ask your prospective team mates :)
- 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)

## 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

## Note on Attacks on IT security of IT systems

- In the lecture you learn specific attacks on IT security of IT systems
- This is only for
  - getting a better understanding of IT security
  - securing your own systems
  - testing the IT security of your own systems
  - usage in the legally approved scope
- Attacking the TU Wien or attacking other systems based on systems of TU Wien can lead to the withdrawal of the permit to study
- Exception: Attacks on our infrastructure as defined in the lecture ;)

## Currently Planned Lectures

- 2 Workshops (16.03.2018, 23.03.2018, 11:15AM-02:45PM)
- Requirements for an ISMS based on the new ISO 27001:2013 Standard Exemplified by the BRZ Infrastructure
- Cloud Security
- Security of the German Health Telematics Infrastructure
- Lifecycle and IT Security of a Banking Chipcard from the Issuing to the Expiration
- Security of Connected Cars

## Planned Exercise Dates

**Lab0** Individual lab, 10 points, 13.03.2018–23.03.2018

### Registration for teams

**Lab1** Team lab, 50 points, 24.04.2018–01.06.2018, exam interview

**Lab2** CTF Contest, 40 points, 09.06.2018

### *Note:*

ESSE exercises (lab0, lab1) usually start and end traditionally 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
  - lva.security@inso.tuwien.ac.at – please state the lecture name as this e-mail address is used for multiple lectures
  - Office hour



## Feedback From Last Terms

- Thanks for the great security LVA!
- The guest lectures were very interesting
- CTF was fun
- The new lab (securing a server infrastructure) is a good idea
- The descriptions of what should be done are quite vague and unclear [...] In my opinion it would be better and easier if there is a detailed list of what should be done.
- A good preparation for the test is not possible using the slides only
- Please give us feedback early if something is unclear
- This way many issues can be solved quickly

## Literature Recommendations 1/2

- 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. *Introduction to Computer Security*. Pearson Education, Inc, 2003. ISBN 0-321-24744-2
- 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. <http://www.inso.tuwien.ac.at/publications/softwaretechnik/>

## Thank You!

More information, Changes, RSS feed etc. can be found at  
<https://security.inso.tuwien.ac.at/itsec-large-infrastructures-ss2018/>

