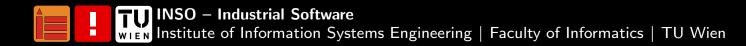
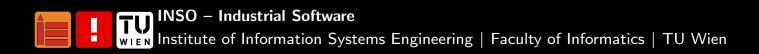


### **ESSE IT Security in Large IT Infrastructures 23S** Lecture 00: Preliminary Discussion

Florian Fankhauser, Christian Schanes, Franz Mairhofer



#### ESSE



### **ESSE** – Establishing Security

- Institute of Information Systems Engineering
- Research Group for Industrial Software (INSO)
- Working Group Establishing Security (ESSE)
- Lectures

6226

- Introduction to Security (W, Bachelor)
- Security for Systems Engineering (CTF-Contest) (S, Bachelor)
- Mobile Security (W & S, Bachelor)
- Advanced Security for Systems Engineering (W, Master)
- Selected Topics of Digital Forensics I (S, Master)
- IT Security in Large IT Infrastructures (CTF-Contest) (S, Master)
- Seminar on Security
- CTF Contests: Hands-On Experience of the IT Security Culture (S, Bachelor/Master)
- Projects, Bachelor Thesis, Master Thesis, PhD Thesis

## **Research Topics (Excerpt)**

- Electronic Payments
- Large IT Infrastructures
- 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
- XML Security
- DevSecOps

# esse Excerpt of Applying Subject Areas

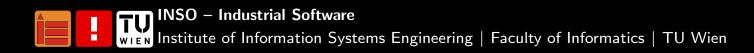
- Malware and Internet Crime
- Physical Security of IT Systems
- Applied Cryptography
- Exploit Development, Offensive Computing, and Exploit Mitigation
- Rootkits and OS Security
- Honeypots, Honeynets, and Honeytokens
- Mobile Security
- Privacy-Protection in Cloud/Mobile Applications
- Security Usability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



- Questions regarding IT Security in Large IT Infrastructures
  - See slide 18

- Other matters, e.g., bachelor/master thesises, projects,...:
  - esse@inso.tuwien.ac.at
  - Office Hour on agreement: Wiedner Hauptstraße 76/2/2

### **IT Security in Large IT Infrastructures 23S**





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. (Spoiler: This is also a crucial aspect of the test.)

IT Security in Large IT Infrastructures 23S | Preliminary Discussion 8 / 22

## **Face-2-Face and Distance Learning**

- Until further notice Face-2-Face Lectures
- If situation changes:
  - Announcement via tuwel
  - Workshops and discussions held via INSO Jitsi
  - Detailed room information/password in tuwel
  - Web browser is needed in order to join
  - Slides will be available
  - Test in tuwel
  - email: esse-itseclarge@inso.tuwien.ac.at
  - tuwel forum



- 7 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 10.03.2023



- 3 labs (1 individual, 2 in teams (incl. CTF contest))
- Exercises mandatory, lab0 is final registration
- Team registration, exercise submission etc. in tuwel
- Exercise interviews for lab1 in Wiedner Hauptstraße 76/2/2
- CTF contest takes place on Sat June 17, 2023, full-day (09:00AM-06:00PM)



#### **Registration for Teams**

6226

- Registration for teams in tuwel
- You have to registrate yourself for a team
- Tuwel 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 you must 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 esse-itseclarge@inso.tuwien.ac.at



- Sometimes, you recognize your goals were set too high...
- Be fair to your team colleagues: inform your colleagues and us (esse-itseclarge@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 ;)

## Planned Lectures – 1/2

- 03.03.2023 Preliminary Discussion
- **10.03.2023** IT Security Challenges in Project Management Exemplified by POS and Telemetry Systems
- **17.03.2023** Workshop 1 Interactive Lecture with Discussions
- **24.03.2023** Workshop 2 Interactive Lecture with Discussions
- 21.04.2023 Aspects of (Common Criteria) Certifications
- **28.04.2023** Offensive Security and IT Risk in a Financial Institution



- 05.05.2023 TBA
- 12.05.2023 TBA
- 16.06.2023 Wrap-Up
- 23.06.2023 Test

Beginning 2023W First additional test



IT Security in Large IT Infrastructures 23S | Preliminary Discussion 16 / 22



Lab0 Individual lab, 10 points, 13.03.2023–27.03.2023
Registration for teams
Lab1 Team lab, 50 points, 25.04.2023–23.05.2023, exam interview
Test CTF optional, no points, 02.06.2023, 06:00PM-09:00PM
Lab2 ESSE CTF Contest, 40 points, 17.06.2023, whole day (09:00AM-06:00PM)

Note:

ESSE exercises (lab0, lab1) usually start and end traditionally at 11:55PM

## **Support for Questions Regarding the Lecture**

- Questions that are interesting and should be visible for other students as well
  - Tuwel forum
  - No solutions, commands etc.  $\rightarrow$  otherwise deduction of points
  - Please note: We do not monitor other forums
- Specific questions
  - esse-itseclarge@inso.tuwien.ac.at please state your team and the exercise, if available, as well
  - Office hour



#### Feedback From Last Terms

6226

- 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 preperation 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

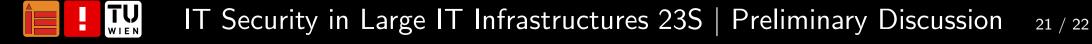
#### IT Security in Large IT Infrastructures 23S | Preliminary Discussion 19 / 22

## **EXAMPLE 7** 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. https://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

# **EXAMPLE 7** Literature Recommendations 2/2

 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!

More information, Changes, RSS feed etc. can be found at https://security.inso.tuwien.ac.at/itsec-large-infrastructures-2023s/

INSO – Industrial Software Institute of Information Systems Engineering | Faculty of Informatics | TU Wien