esse

ESSE Advanced Security for Systems Engineering 22W
Lecture 00: Preliminary Discussion

Florian Fankhauser, Christian Schanes, Christian Brem, Franz Mairhofer

ESSE

ESSE – Establishing Security

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

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

Contact

- Questions regarding ESSE Advanced Security for Systems Engineering
  - See slide 19

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

ESSE Advanced Security for Systems Engineering VU 22W

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*.

Possible Change to Distance Learning

- Announcement in tuwel
- Slides as well as transcriptions of lectures
- Literature research to deepen further theoretical aspects
- Slides online evening before lecture
- During begin of lecture time available in INSO Jitsi for possible discussions
- Detailed room information/password in tuwel
- Web browser is needed in order to join

- email: lva.security@inso.tuwien.ac.at
- tuwel forum

Overview Lecture

- 12 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 14, 2022

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) 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
- Tuwel 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 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 lva.security@inso.tuwien.ac.at

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

07.10.2022 Preliminary Discussion, Advanced Attacks on Applications 1

14.10.2022 Secure Architectures

21.10.2022 XML Security

28.10.2022 Advanced Attacks on Applications 2

04.11.2022 Advanced Attacks on Applications 3

11.11.2022 Advanced Attacks on Applications 4

18.11.2022 Forensics

25.11.2022 Implementation of Zero Trust in Complex IT Infrastructures (Current Status of Implementation within the German Health Telematics Infrastructure)

Planned Lectures – 2/2

02.12.2022 TBA

09.12.2022 Advanced Aspects of Pentesting & Red Teaming

16.12.2022 Applied Cryptography

13.01.2023 Mobile Applications

TBA Oral Exams

2023S 3 more optional dates for test

Planned Excercise Dates

lab0 20 points, exercise has to be finished alone, 21.10.2022–04.11.2022

Building of teams for lab1 and lab2 04.11.2022–10.11.2022

lab1 50 points, team exercise, 11.11.2022–09.12.2022

lab2 50 points, team exercise, 09.12.2022–13.01.2023

Please note:

ESSE exercises traditionally begin at 11:55pm

Tips for sucessfully mastering this course

- Start early with the exercises
- Interactively engage in the lectures/discussions
- For seemingly complex problems, simple solutions might exists.
- Use the lectures to discuss solutions approaches, learning priorities, and your understanding of the material
- If you prefer to self-study the material without the guidance giving in our lectures, be sure to get familiar with the given literature references

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
  - lva.security@inso.tuwien.ac.at – please state the lecture name as this e-mail address is used for multiple lectures; please state your team number, if available, as well
  - Office hour
- *Please* do not *use other ways, e.g., Tuwel submission comments*

Literature 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. *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

Literature 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!

https://security.inso.tuwien.ac.at/advsecsyseng-2022w/