esse

Selected Topics of Digital Forensics I 23S
Lecture 00: Preliminary Discussion

Thomas Grechenig, Florian Fankhauser, Martin Moutran, Monika Schrenk

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

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 Selected Topics of Digital Forensics I
  - See slide 16

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

esse

Selected Topics of Digital Forensics I 23S

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

Aim of the Lecture

At the end of the term, the students of the lecture should know *critical aspects of forensic investigations*.

Moreover, students should know *different fields of application of forensics* as well as the different *important facets* of these.

Forensics supports a *high level of IT security*. At the end of the term, students should know *how this can be achieved*.

In short, students should know *when and how forensic methods can and should be applied*.

A *focus* is put on how *forensic methods* are applied *in real world projects*.

Lecture

- Grading: 50% written exam, 50% lab exercises
- After the first exercise submission a certificate is issued
- Exam + exercises have to be passed, i.e., you need to earn more than 50% respectively
- Documents: slides, mindmaps, literature references
- Registration for the course in TISS until 30.03.2023

Exercises

- 2 labs (1 individual lab, 1 team lab)
- Exercises mandatory
- Lab0 / Optional entry question: final course registration
- Lab1 is a rolling lab, i.e., more exercises get published in time
  - After 09.05.2023 no exercise releases
- Team registration, submissions etc. in tuwel

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, 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)
- If there are problems in teams, please write ASAP an e-mail to esse-akdfi@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 (esse-akdfi@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

02.03.2023	Preliminary Discussion + Introduction to Digital Forensics
16.03.2023	Fingerprinting of Soft- and Hardware
23.03.2023	Incident Reconstruction of Systems
30.03.2023	Forensic Analysis (Images, Videos, Documents and More)
20.04.2023	Introduction to Mobile Forensics
27.04.2023	Honeypots and Event Monitoring
04.05.2023	Forensic Methods for Memory and Storage Dumps
11.05.2023	Guest Lecture: IOT Forensics
25.05.2023	Anti-Forensics
15.06.2023	Written Exam (FH Hörsaal 7 - GEO)

Planned Exercise Dates

Lab0 Individual lab, 20 points, 13.03.2023–27.03.2023

Registration for teams 31.03.2023–07.04.2023

Lab1 Team lab, 80 points, 25.04.2023–06.06.2023

Note:

ESSE exercises usually traditionally start and end 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-akdfi@inso.tuwien.ac.at – please state your team and the exercise, if available, as well
  - Office hour
- *Please* do not *use other ways, e.g., Tuwel submission comments*

Thank You!

More information, Changes, RSS feed etc. can be found at
https://security.inso.tuwien.ac.at/selected-topics-digital-forensics-i-2023s/