esse

Selected Topics of Digital Forensics I 22S
Lecture 00: Preliminary Discussion

Thomas Grechenig, Florian Fankhauser, Franz Mairhofer, Andreas Ehringfeld

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 *(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
  - `https://security.inso.tuwien.ac.at/`
  - Tuwel forum
    - Questions that are interesting/should be visible for other students as well
    - *Please note:* We *do not* monitor other forums
    - *Please* do not *use other ways, e.g. Tuwel submission comments*
  - 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 on agreement: Wiedner Hauptstraße 76/2/2
- esse@inso.tuwien.ac.at

esse

Selected Topics of Digital Forensics I 22S

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

- Workshops (6 lectures)
- Team presentations (2 lectures)
- Grading: 50% exercises, 50% team presentations
- After the first exercise submission a certificate is issued
- Presentation + 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 31.03.2022

Exercises

- 2 labs (1 individual lab, 1 team lab)
- Exercises mandatory, lab0 is final course registration
- Lab1 is a rolling lab, i.e., more exercises get published in time
  - After 12.05.2022 no exercise releases
- Team registration, exercise submission etc. in tuwel

Team Presentations 1/2

- Topic must be ...
  - Chosen from the field of Digital Forensics
  - Submitted via tuwel
  - Approved by ESSE
- Duration depends on the number of participants (final decision after team registration is completed)
- High quality sources (listed in slides)
- Slides must be written in English and submitted via tuwel before first team presentation date – details will be published in tuwel
- Only submitted version of slides must be presented

Team Presentations 2/2

- Due to time constraints, the presentation must not be held as a workshop but can contain short interactive elements or demonstration parts
- Audience: all participants of this course
- Presentation will be held via Jitsi
- Test your setup! – e.g., with public Jitsi server meet.jit.si
- Q&A Session: 5 minutes after presentation slot
- Team work, presentation style freely selectable within specifications
- Time Contingent Management: no under- or overflow, hard timecut
- Grading mainly based on live presentation
- Team issues? → Mail: lva.security@inso.tuwien.ac.at

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 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) 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

03.03.2022	Preliminary Discussion, Introduction to Digital Forensics
17.03.2022	Forensic Analysis (Images, Videos, Documents and More)
24.03.2022	Incident Reconstruction of Systems
31.03.2022	Fingerprinting of Soft- and Hardware
28.04.2022	Forensic Methods for Memory and Storage Dumps
05.05.2022	Anti-Forensics
12.05.2022	Team Presentations
19.05.2022	Team Presentations

Planned Exercise Dates

Lab0 Individual lab, 20 points, 17.03.2022–31.03.2022

Registration for teams 01.04.2022–06.04.2022

Lab1 Team lab, 80 points, 07.04.2022–02.06.2022

Note:

ESSE exercises usually traditionally start and end 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; please state your team number, if available, as well
  - Office hour

Thank You!

More information, Changes, RSS feed etc. can be found at
https://security.inso.tuwien.ac.at/selected-topics-digital-forensics-i-2022s/