

ESSE Einführung in Security – VO 00: Vorbesprechung

Christian Schanes, Florian Fankhauser, Rafael Vrecar

24W



ESSE (Establishing Security) – IT Security Research Team
Research Group for Industrial Software (INSO)

<https://establishing-security.at/>

ESSE

ESSE – Establishing Security

- Institut für Information Systems Engineering
- Forschungsgruppe Industrial Software (INSO)
- Arbeitsgruppe Establishing Security (ESSE)
- Auszug aus (bisherigen) Lehrveranstaltungen
 - Einführung in Security (*W, Bakk.*)
 - Security for Systems Engineering (CTF-Contest) (*S, Bakk.*)
 - Mobile Security (*W & S, Bakk.*)
 - 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 aus Security
 - CTF Contests: Einführung und Vertiefung in die „Olympiade“ der IT Security Kultur (durch OlympionikInnen) (*S, Bakk./Master*)
 - Projekte, Bakkalaureatsarbeiten, Diplomarbeiten, Dissertationen

Forschungsthemen (Auszug)

- Large IT Infrastructures
- DevSecOps
- eHealth
- Embedded Security and Internet of Things
- Penetration Testing, Security Audits, Security Certification
- IT Security Teaching Methods
- Electronic Payments
- Secure and Anonymous Communication
- Governance, Risk and Compliance
- Identification, Authentication and Authorization, eID solutions

Erforderliche Detailgebiete (Auszug)

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

- Fragen betreffend ESSE Einführung in Security
 - siehe Slide 20

- Andere Angelegenheiten, z.B. Bachelor-/Masterarbeiten, Projekte,...
 - esse@inso.tuwien.ac.at
 - Sprechstunde nach Vereinbarung:
Wiedner Hauptstraße 76, Stiege 2, 2. Stock

ESSE Einführung in Security VU 24W

<https://establishing-security.at/>

Ziel der Lehrveranstaltung

Die Absolvent:innen sollen die *Fähigkeit* besitzen, *sicherheitsrelevante Aspekte* in Projekten frühzeitig bereits im Engineering-Prozess von Systemen zu *erkennen* und *geeignete Maßnahmen* einzuleiten, damit man während des Betriebs von Systemen einen *ausreichenden Grad an Sicherheit* erreicht.

Dabei wird Ihre generelle *Security-Awareness* gefördert und Sie wechseln immer wieder in die *Rolle von Angreifer:innen*, damit Sie *nachdenken wie Sicherheitsmaßnahmen fehlschlagen* können und Sie die *Hintergründe verstehen*, weshalb Systeme einer Absicherung bedürfen.

Ablauf VO-Teil

- 15 Vorlesungen incl. Gastvorträge, Security-Themen aus der ESSE-Praxis
- 1 Test, Anmeldung über TISS erforderlich
- Benotungsschema: 50% Übung, 50% Test, ab 1. Abgabe wird ein Zeugnis ausgestellt
- Test + Übung jeweils positiv (d.h. jeweils mehr als 50 Punkte)
- Insgesamt 2 mögliche Testtermine (Haupttermin + Nachtest), letzter Antritt zählt
- Unterlagen: Slides, Transkriptionen, Mitschriften, Literaturreferenzen
- Anmeldung über TISS bis 11.10.2024
- *Achtung:* Anmeldung zu Präsenzterminen für Vorlesungen in tuwel erforderlich!
- Maximal erreichbare Punktezahl: 100

Ablauf UE-Teil

- 2 Übungsbeispiele (1 einzeln, 1 in Teams)
- Übung verpflichtend, Lab0/Einstiegsfrage als fixe Anmeldung
- Teameinteilung, Übungsabgaben etc. über tuwel
- Abgabegespräch für Lab1 (im Team) in Wiedner Hauptstraße 76/2/2
- UE-Umgebung: Linux
- Linux-Workshop (Selbststudium)
 - Linux-Einführung für Linux-Einsteiger:innen
 - Voraussetzung zur Teilnahme: Lösung einer kleinen Aufgabe (1 Zusatzpunkt, dennoch: cut-off bei 100)
- Maximal erreichbare Punkteanzahl: 100

3 ECTS-Variante dieser LVA

- VU Introduction to Security
- Im Rahmen dieser LVA absolvierbar
- Weniger Teststoff (siehe Folgeslides)
- Weniger Übungsbeispiele (werden auf 100 Punkte hochskaliert, i.e., x Punkte erreicht, y Punkte erreichbar
⇒ $(x/y) * 100$ Übungspunkte)
- Keine Teams aus zwei verschiedenen LVAs
- Anmeldung in tuwel, heute ab 16:00 CET
bis **spätestens 11.10.2024, 23:59 CET**

Anmeldung zu Teams

- Anmeldung zu Teams in tuwel (Voraussetzung: Lab0/Einstiegsfrage abgegeben)
- Selbständige Anmeldung erforderlich
- Teamfindung über eigenes Teamfindungs-Forum in tuwel möglich
- Vor Eintragung in „fremde“ Teams bitte unbedingt bei bestehenden Teammitgliedern nachfragen
- Anmeldung im Team *Zuteilung durch LVA-Leitung* für automatische Zuteilung zu einem Team
- Teameinteilung verpflichtend (andernfalls 0 Punkte)
- Bei Unklarheiten im Team bitte *frühzeitig* e-mail an lva.security@inso-world.com schreiben

LVA-Abbruch

- Hin und wieder kommt man drauf, dass man sich zu viel vorgenommen hat...
- Fairness gegenüber Ihren Teammitgliedern: Informieren Sie bitte Ihr Team und uns (lva.security@inso-world.com) sobald Ihre Entscheidung feststeht
- Konsequenz: negatives Zeugnis nach der 1. Abgabe

Hinweis zu Angriffen auf die IT-Sicherheit von Systemen

- Sie lernen in der Lehrveranstaltung konkrete Angriffe auf IT-Systeme
- Dies dient ausschließlich
 - zum besseren Verständnis der IT-Sicherheit
 - zur Absicherung eigener IT-Systeme
 - zur Überprüfung eigener IT-Systeme
 - bzw. zur Verwendung im rechtlich erlaubten Rahmen
- Angriffe auf die TU Wien oder Angriffe über Systeme der TU Wien können bis zum Entzug der Studienberechtigung führen
- Ausnahme: Angriffe in der Übungsumgebung im Rahmen der Übungen sind erlaubt :-)

Geplante Termine Vorlesung – 1/3

- 04.10.2024 Vorbesprechung + Einführung in die IT-Sicherheit
- 11.10.2024 Kryptographie + Netzwerksicherheit
- 18.10.2024 Sicherheit in der Software-Entwicklung
+ Identität, Authentifizierung, Autorisierung
- 08.11.2024 Organisatorische Sicherheit und Sicherheitsmanagement
+ (6) Sicherheitsimplikationen von Typisierung in
Programmiersprachen
- 22.11.2024 Testing
+ Betriebssystemsicherheit am Beispiel von Linux und Windows
- 29.11.2024 Sicherheitskonzepte von macOS + (6) Mobile Security

Geplante Termine Vorlesung – 2/3

06.12.2024 (6) Web Application Security + *Erste Lab1 Sprechstunde*

13.12.2024 Sicherheitsfaktor Mensch/Social Hacking
+ (6) Usable Security und Trust

10.01.2025 Unterschiedliche IT-Security Themen aus der ESSE-Praxis
+ *Zweite Lab1 Sprechstunde*

17.01.2025, 18:00-20:00 Test (1. Termin, Haupttermin)

24.01.2025, 14:00-15:00, **Wiedner Hauptstraße 76/2/2** Testeinsicht

20.02.2025 Test (2. Termin, Nachtest)

Hinweis: Die Termine am 25.10.2024 und 20.12.2024 werden wir nur bei Bedarf nutzen.

Geplante Termine Vorlesung – 3/3

Wichtige Anmerkungen

- Aufgrund der großen Nachfrage: verschiedene Hörsäle, um möglichst viele Präsenzplätze anbieten zu können. Details auf der Website, ICS-Datei für Kalender-Abo in tuwel.
- Die mit vorangestellter (6) gekennzeichneten Vorlesungseinheiten sind für die Personen, welche die 6 ECTS-Variante der Lehrveranstaltung absolvieren, zusätzlicher Teststoff.

Übung – derzeitig geplante Termine

- **Lab0** 20 Punkte, Einzelübung, 18.10.2024–08.11.2024
- **Teamanmeldung (Lab1)** 08.11.2024–15.11.2024
- **Lab1** 80 Punkte, Teamübung, 22.11.2024–17.01.2025
(nicht alle Beispiele am 22.11. online, weitere folgen schrittweise bis spätestens 20.12.)
- **Abgabegespräch (Lab1)** 20.01.–24.01.2025 (vorauss.)

Hinweis:

ESSE-Übungen beginnen und enden traditioneller Weise um 23:55 Uhr CET

Übung – Linux-Workshop

- Optional
- Grundlagen von Linux für Anwendung in den ESSE Labs
- Bei Erfahrung mit Linux auf Shell wahrscheinlich nicht viel Neues
- Slides werden zur Verfügung stehen
- Verbindliche Anmeldung via tuwel
- Voraussetzung Beantwortung einfacher Einstiegsfrage in tuwel (Achtung: Zeugnis!)
- Einstiegsfrage auch durchführbar, wenn Sie nicht am Linux-Workshop teilnehmen möchten
- 21.10.2024 Linux Workshop Unterlagen online

Unterstützung bei Fragen zur LVA

- Fragen, die auch für andere Studierende interessant sind und sichtbar sein sollen
 - tuwel-Forum
 - Achtung: Keine Lösungswege, Befehlszeilen etc. → sonst Punkteabzug!
 - *Hinweis:* Andere Foren werden von uns *nicht* betreut
- Spezielle Fragen
 - lva.security@inso-world.com – bitte schreiben Sie ggf. Teamnummer & Aufgabe mit in das e-mail
 - Sprechstunde
- *Bitte verwenden Sie nur diese Wege für direkten Kontakt mit uns, nicht z.B. Tuwel-Kommentare zu Aufgaben*

Positives Feedback

- Inhalte spannend
- Gute Gastvorträge
- Viel Neues gelernt
- Die Übungen sind unglaublich lustig. Sehr einfallsreich und spannend. Würde am liebsten alles nochmal machen :).
- Ich möchte Ihnen ein Kompliment machen, dass eine LVA so viel Spaß machen kann! Ich müsste seeehr lange nachdenken (wahrscheinlich noch länger als um auf das Flag dieser Challenge zu kommen :joy:) um eine LVA zu finden, die in meinem Studium bisher mehr Spaß gemacht hat!

Anregungen

- Unterlagen (Slides) unzureichend
 - → Transkriptionen, Literaturreferenzen, Mitschrift, Selbstorganisation :-)
- Probleme bei Teams
 - → Bitte frühzeitig an LVA-Leitung wenden!
- Bei Unklarheiten/Problemen bitte gleich melden!
- Oftmals können wir dann kurzfristig helfen
- Auf anonyme Anfragen ist es jedoch schwierig konkret zu reagieren

Literaturempfehlungen 1/3

- Ross Anderson. *Security Engineering. A Guide to Building Dependable Distributed Systems.*
Wiley Publishing, Inc., 2. Auflage, 2008.
ISBN 978-0-470-06852-6.
<https://www.cl.cam.ac.uk/~rja14/book.html>
- Ed Skoudis und Tom Liston. *Counter Hack Reloaded. A Step-by-Step Guide to Computer Attacks and Effective Defenses.*
Pearson Education, Inc., 2. Auflage, 2006.
ISBN 0-13-148104-5
- Matt Bishop. *Introduction to Computer Security.*
Pearson Education, Inc, 2003.
ISBN 0-321-24744-2

Literaturempfehlungen 2/3

- Bruce Schneier. *Secrets & Lies: Digital Security in a Networked World*. Wiley Publishing, Inc., Indianapolis, Indiana, 2004.
ISBN 0-471-45380-3
- Claudia Eckert. *IT-Sicherheit: Konzepte - Verfahren - Protokolle*. Oldenbourg, 2007.
ISBN 3486578510

Literaturempfehlungen 3/3

- Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, und Carl Landwehr. **Basic concepts and taxonomy of dependable and secure computing.** *Dependable and Secure Computing, IEEE Transactions on*, 1(1):11 – 33, Januar/März 2004.
ISSN 1545-5971.
doi: [10.1109/TDSC.2004.2](https://doi.org/10.1109/TDSC.2004.2)
- Florian Fankhauser, Christian Schanes, und Christian Brem. **Sicherheit in der Softwareentwicklung.** *In Softwaretechnik - Mit Fallbeispielen aus realen Entwicklungsprojekten*, Kapitel 13, Seiten 589–646. Pearson Studium, München, 1. Auflage, 2009

Vielen Dank!

Weitere Informationen, Änderungen, RSS-Feed etc. finden Sie auf

`https://establishing-security.at/`