esse

ESSE Security for Systems Engineering 2022S – VO 00: Vorbesprechung

Florian Fankhauser, Christian Schanes

Christian Brem, Franz Mairhofer

ESSE

ESSE - Establishing Security

- Institut für Information Systems Engineering
- Forschungsgruppe Industrial Software (INSO)
- Arbeitsgruppe Establishing Security (ESSE)
- Lehrveranstaltungen
  - Introduction to Security *(W, Bakk.)*
  - Security for Systems Engineering (CTF-Contest) *(S, Bakk.)*
  - Mobile Security *(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)

- 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

Erforderliche Detailgebiete (Auszug)

- 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

Kontakt

- Fragen betreffend ESSE Security for Systems Engineering
  - 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 Security for Systems Engineering VU 2022S

IT-Sicherheit – Ganzheitliche Sicht auf IT-Systeme erforderlich – 1/2

- Solar Winds: Praktikant soll an schlechtem Passwort des gehackten Servers schuld sein
- Sensible Daten von 500.000 Patienten in Frankreich landeten im Netz
- Schwere Windows-Sicherheitslücke blieb zwölf Jahre lang unentdeckt
- Hacker stellen Sammlung von 3,2 Milliarden Passwörtern ins Netz
- Hacker versuchten Wasserversorgung in Florida zu vergiften
- Schwere Sicherheitslücke in Sudo bleibt bei MacOS vorerst offen
- Passwörter auf dem Tisch: Das Datenschutzdesaster auf Wiens Teststraßen
- Let's Encrypt hat vorerst doch „nur" 1,7 Millionen Zertifikate zurückgezogen

IT-Sicherheit – Ganzheitliche Sicht auf IT-Systeme erforderlich – 2/2

- Passwortherausgabe: SPD-Politiker wirft „hirnrissigen“ Gegnern Täterschutz vor
- WLAN-Lücke Kr00k: Sicherheitsforschern zufolge 1 Milliarde Geräte gefährdet
- Cybersicherheit: Forscher warnt vor Hackerangriffen auf Satelliten
- Ghidra: NSA stellt quelloffenes Software-Analyse-Tool vor
- DevSecOps-Studie: Automatisierung führt zu mehr Sicherheit
- Sicherheitspanne an New Yorker Flughafen besteht fast ein Jahr
- 1&1: Kundenportal akzeptierte jedes Passwort
- BMW ConnectedDrive gehackt
- Phishing: Manager überweist 17 Millionen Dollar an Internetbetrüger
- KCI Attacks against TLS

Ziel der Lehrveranstaltung

Die AbsolventInnen 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.

Dazu hilft ein Verständnis *wie Systeme fehlschlagen*
und *wie man sie gezielt dazu bringen kann*.

Insbesondere soll der Blick dafür geschärft werden,
dass die *Gesamtsicherheit von Systemen* relevant ist
und Einzelaspekte nicht ausreichen, um ein *ausreichendes*
Sicherheitsniveau zu erreichen.

Präsenzlehre/Distance Learning

- Bis auf Widerruf: Präsenzlehre
- Falls sich die Situation ändert:
  - Slides + Transkriptionen
  - tuwel-Forum
  - e-mail

Ablauf VO-Teil

- 11 Vorlesungseinheiten + Gastvorträge
- 1 Test, Anmeldung erforderlich
- Benotungsschema: 50% Übung, 50% Test, ab 1. Abgabe wird ein Zeugnis ausgestellt
- Test + Übung jeweils positiv (d.h. jeweils mehr als 50 Punkte)
- Unterlagen: Slides, Mitschriften, Literaturreferenzen (Bibliothek)

- Anmeldung über TISS bis 11.03.2022

Ablauf UE-Teil

- 3 Übungsbeispiele (1 einzeln, 2 in Teams (incl. CTF-Contest))
- Übung verpflichtend, lab0 als fixe Anmeldung
- Teameinteilung, Übungsabgaben etc. über tuwel
- Abgabegespräch für lab1 in Wiedner Hauptstraße 76/2/2
- CTF-Contest an 1 Tag

- UE-Umgebung: Linux

- ESSE-CA-Zertifikat für sicheren Zugriff auf ESSE-Ressourcen in tuwel

Anmeldung zu Teams

- Anmeldung zu Teams in tuwel
- Selbständige Anmeldung erforderlich
- Teamfindung eventuell über Forum in tuwel
- 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.tuwien.ac.at schreiben

LVA-Abbruch

- Hin und wieder kommt man drauf, dass man sich zu viel vorgenommen hat...
- Fairness gegenüber Ihren Teammitgliedern: Informieren Sie Ihr Team und uns (lva.security@inso.tuwien.ac.at) 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 Inhalte Vorlesung – 1/2

04.03.2022	Vorbesprechung, CTF-Einführung
11.03.2022	Netzwerksicherheit
18.03.2022	Sichere Programmierung
25.03.2022	Web Application Security
01.04.2022	Risikomanagement und IT-Grundschutz
08.04.2022	Mobile Security
29.04.2022	Pentesting & Red Teaming

Geplante Inhalte Vorlesung – 2/2

06.05.2022	Windows Security
13.05.2022	macOS Security
20.05.2022	Security in der Praxis: Datenspuren im Internet
03.06.2022	Intrusion Detection und Intrusion Prevention Systeme
24.06.2022	Test

Übung – derzeitig geplante Termine

Lab0 Einzelarbeit, 10 Punkte, 14.03.2022–28.03.2022

Anmeldung zu Teams

Lab1 Teamarbeit, 50 Punkte, 26.04.2021–24.05.2021, Abgabegespräch

Probe-CTF-Contest optional, ohne Punkte, 21.05.2022, 15:00-18:00

Lab2 CTF-Contest, 40 Punkte, 04.06.2022 ganztägig (09:00-18:00)

Hinweis:

ESSE-Übungen (lab0/lab1) beginnen und enden traditioneller Weise um 23:55

Unterstützung bei Fragen zur LVA (VO und UE)

- Fragen, die auch für andere Studierende interessant sind und sichtbar sein sollen
  - tuwel-Forum
  - *Hinweis:* Andere Foren werden von uns *nicht* betreut
- Spezielle Fragen
  - lva.security@inso.tuwien.ac.at – bitte schreiben Sie den LVA-Namen mit in das e-mail, die e-mail-Adresse wird für mehrere Lehrveranstaltungen verwendet; ergänzen Sie bitte auch, falls vorhanden, Ihre Teamnummer.
  - Sprechstunde
- *Bitte verwenden Sie nur diese Wege für direkten Kontakt mit uns,* nicht *z.B. Tuwel-Kommentare zu Aufgaben*

Feedback aus vergangenen Semestern

- Die Vorlesungen waren sehr spannend gestaltet
- Der Gastvortrag des Berufsdetektiven war top!
- Faire Klausur
- CTF ist eine coole Idee, Respekt für die gelungene, kreative Umsetzung!
- Die Übungen waren spannend aufgebaut und im Team sehr lustig zu erarbeiten

- Es wurde beim Test nach Erklärungen für Angriffe gefragt, von welchem auf den Folien gerade mal der Name steht.
- Beim CTF war leider nicht klar, was man für die jeweiligen Punkte, die man für das Protokoll bekommt, am Ende vorweisen muss.

- Bei Unklarheiten/Problemen bitte gleich melden!
- Oftmals können wir dann kurzfristig helfen

Literaturempfehlungen 1/2

- 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
- Bruce Schneier. *Secrets & Lies: Digital Security in a Networked World.* Wiley Publishing, Inc., Indianapolis, Indiana, 2004. ISBN 0-471-45380-3

Literaturempfehlungen 2/2

- 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
- Full Disclosure. Full Disclosure Mailing List. `https://nmap.org/mailman/listinfo/fulldisclosure`

Vielen Dank!

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

`https://security.inso.tuwien.ac.at/secsyseng-2022s/`