esse

ESSE Introduction to Security – VO 00: Vorbesprechung

Christian Schanes, Florian Fankhauser, 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 *(WS, Bakk.)*
  - Security for Systems Engineering (CTF-Contest) *(SS, Bakk.)*
  - Advanced Security for Systems Engineering *(WS, Master)*
  - Selected Topics of Digital Forensics I *(SS, Master)*
  - IT Security in Large IT Infrastructures (CTF-Contest) *(SS, Master)*
  - Seminar aus Security
  - 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

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 Introduction to Security
  - `https://security.inso.tuwien.ac.at/`
  - tuwel-Forum
  - 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
  - *Bitte verwenden Sie nur diese Wege,* nicht *z.B. Tuwel-Kommentare zu Aufgaben*
- Sprechstunde nach Vereinbarung: Wiedner Hauptstraße 76, Stiege 2, 2. Stock
- esse@inso.tuwien.ac.at

esse

ESSE Introduction to Security VU 21W

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.

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

Distance Learning

- Slides + Transkriptionen

- tuwel-Forum
- e-mail

Ablauf VO-Teil

- 10 Vorlesungseinheiten incl. Gastvorträge
- 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 4 mögliche Testtermine (Haupttermin + 3 Nachtests)
- Unterlagen: Slides, Transkriptionen, Literaturreferenzen (Bibliothek)

- Anmeldung über TISS bis 08.10.2021

- Maximal erreichbare Punktezahl: 100

Ablauf UE-Teil

- 3 Übungsbeispiele (1 einzeln, 2 in Teams)
- Übung verpflichtend, lab0/Einstiegsfrage als fixe Anmeldung
- Teameinteilung, Übungsabgaben etc. über tuwel

- UE-Umgebung: Linux
- Linux-Workshop
  - Linux-Einführung für Linux-EinsteigerInnen
  - Voraussetzung zur Teilnahme: Lösung einer kleinen Aufgabe
- Maximal erreichbare Punkteanzahl: 100

Anmeldung zu Teams

- Anmeldung zu Teams in tuwel
- Selbständige Anmeldung erforderlich
- Teamfindung über eigenes Teamfindungs-Forum in tuwel möglich
- Vor Eintragung in „fremde“ Teams bitte bei bestehenden Teammitgliedern nachfragen
- Gegebenenfalls 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

ESSE-CA

- Kommunikation sollte heute verschlüsselt erfolgen
- X.509-Standard ist derzeit State-of-the-Art

- ESSE betreibt eine eigene Certification Authority (CA) für
  - Übungs-Ressourcen
  - teilweise e-mail-Kommunikation

- Download ESSE-Root-CA-Zertifikat über ESSE-Website, als 2. Kanal auch in tuwel verfügbar
- Hinzufügen zu CAs, denen man vertraut – sonst kann es zu Fehlermeldungen kommen

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

01.10.2021	Vorbesprechung
08.10.2021	Einführung in die IT-Sicherheit
15.10.2021	Kryptographie
22.10.2021	Netzwerksicherheit
29.10.2021	Sicherheit in der Software-Entwicklung
05.11.2021	Testing
12.11.2021	Identität, Authentifizierung, Autorisierung
19.11.2021	Organisatorische Sicherheit und Sicherheitsmanagement
26.11.2021	Sicherheitsfaktor Mensch/Social Hacking

Geplante Inhalte Vorlesung – 2/2

03.12.2021 Betriebssystemsicherheit am Beispiel von Linux und Windows

10.12.2021 Sicherheitskonzepte von macOS

14.01.2022, 16-18 Test

SS2022 3 weitere optionale Testtermine

Übung – derzeitig geplante Termine

Lab0 20 Punkte, Einzelübung, 15.10.2021–03.11.2021

Anmeldung zu Teams für lab1 und lab2 05.11.2021–10.11.2021

Anmeldung zu Netzwerk-Dump-Slots lab1

Lab1 40 Punkte, Teamübung, 12.11.2021–10.12.2021

Lab2 40 Punkte, Teamübung, 12.11.2021–12.01.2022

Hinweis:

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

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 Einstiegs-Frage in tuwel
- Zusatz-Übung auch durchführbar, wenn Sie nicht am Linux-Workshop teilnehmen möchten

- 09.10.2021 Linux Workshop Unterlagen online

Unterstützung bei Fragen zur LVA (VO und UE)

- Fragen, die auch für andere Studierende interessant sind/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
  - Sprechstunde
  - *Bitte verwenden Sie nur diese Wege für direkten Kontakt mit uns*, nicht *z.B. Tuwel-Kommentare zu Aufgaben*

Positives Feedback aus vergangenen Semestern

- 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 Challange zu kommen :joy:) um eine LVA zu finden, die in meinem Studium bisher mehr Spaß gemacht hat!

Anregungen aus vergangenen Semestern

- Unterlagen (Slides) unzureichend
  - → 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 1/2

- Ross Anderson. *Security Engineering. A Guide to Building Dependable Distributed Systems*. Wiley Publishing, Inc., 2. Auflage, 2008. ISBN 978-0-470-06852-6. `http://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

- Claudia Eckert. *IT-Sicherheit: Konzepte - Verfahren - Protokolle*. Oldenbourg, 2007. ISBN 3486578510
- 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
- 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://security.inso.tuwien.ac.at/introsec-2021w/`