esse

Introduction to Security – VO 00: Vorbesprechung

Florian Fankhauser
Christian Schanes

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)*
  - IT Security in Large IT Infrastructures (CTF-Contest) *(SS, Master)*
  - Seminar aus Security
  - Projekte
  - Bakkalaureatsarbeiten, Diplomarbeiten, Dissertationen

Forschungsthemen (Auszug)

- Electronic Payments
- Large IT Infrastructures
- Connected Cars
- 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

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 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, Abgabegespräche,. . . :
  Wiedner Hauptstraße 76, Stiege 2, 2. Stock
- esse@inso.tuwien.ac.at

esse

Introduction to Security VU WS18

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.

Ablauf VO-Teil

- 10 Vorlesungseinheiten 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 4 mögliche Testtermine (Haupttermin + 3 Nachtests)
- Unterlagen: Slides, Mitschriften, Literaturreferenzen (Bibliothek)

- Anmeldung über TISS bis 12.10.2018

Ablauf UE-Teil

- 3 Übungsbeispiele (1 einzeln, 2 in Teams)
- Übung verpflichtend, lab0/Einstiegsfrage als fixe Anmeldung
- Teameinteilung, Übungsabgaben etc. über tuwel
- Abgabegespräch für lab1/lab2 in Wiedner Hauptstraße 76/2/2

- 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

05.10.2018	Vorbesprechung, Einführung in die IT-Sicherheit
12.10.2018	Kryptographie, Verschlüsselung, Key-Management
19.10.2018	Netzwerksicherheit
09.11.2018	Sicherheit in der Software-Entwicklung
16.11.2018	TBA
23.11.2018	Testing
30.11.2018	Identität, Authentifizierung, Autorisierung

Geplante Inhalte Vorlesung – 2/2

07.12.2018 Organisatorische Sicherheit und Sicherheitsmanagement

14.12.2018 Sicherheitsfaktor Mensch/Social Hacking

21.12.2018 Betriebssystemsicherheit

11.01.2019 Unterschiedliche IT-Security Themen aus der ESSE-Praxis

18.01.2019 Test

25.01.2019 Testeinsicht

SS2019 3 Testtermine

Übung – derzeitig geplante Termine

Lab0 20 Punkte, Einzelübung, 17.10.2018–31.10.2018

Anmeldung zu Teams für lab1 und lab2 05.11.2018–12.11.2018

Anmeldung zu Netzwerk-Dump-Slots lab1

Lab1 40 Punkte, Teamübung, 21.11.2018–16.01.2019

Abgabegespräch Lab1 21.–23.01.2019

Lab2 40 Punkte, Teamübung, 21.11.2018–16.01.2019

Abgabegespräch Lab2 21.–23.01.2019

Hinweis:

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

Übung – Linux-Workshop

- Optional
- Grundlagen von Linux für Anwendung in den ESSE Labs
- Slides werden zur Verfügung stehen
- Bei Erfahrung mit Linux auf Shell wahrscheinlich nicht viel Neues

- Verbindliche Anmeldung via tuwel
- Voraussetzung Beantwortung einfacher Einstiegs-Frage in tuwel
- Zusatz-Übung auch durchführbar, wenn Sie nicht am Linux-Workshop teilnehmen möchten
- Bei zu später/keiner Abmeldung und keiner Teilnahme 20 Punkte Abzug für Übung

- 13.10.2018, 09:30–13:30, evtl. 20.10.2018, 09:30-13:30

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*

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 :).
- 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-ws2018/`