Techniken und Werkzeuge für die IT-Sicherheit im Cloud-Computing und in verteilten Systemen

Sommersemester 2013

LS14 - Arbeitsgruppe Software Engineering for Critical Systems

15.04.2013

Agenda

Das Proseminar - Wichtige Meta-Fähigkeiten

	Studium	Abschluss	Beruf
Vortrag			
Ausarbeitung			
Einarbeiten			

Werbung

Abschlussarbeiten

- Themen siehe: `http://www-jj.cs.tu-dortmund.de/secse/pages/teaching/thesis/index_de.shtml`
- Proseminarthemen können auf Abschlussarbeitsthemen vorbereiten

Hilfskräfte

- Themen siehe: `http://www-jj.cs.tu-dortmund.de/secse/pages/home/jobs_de.shtml`
- Mitarbeit in verschiedenen Projekten

Ablauf

Leistungsbestandteile

- Kommentierte Gliederung
- Review-Fassung
- Reviews
- Abgabe Ausarbeitung
- Abgabe Folien
- Vortrag
- Diskussion

Betreuung

- Vorgespräch (Verständnisfragen)
- Besprechung der Gliederung
- Besprechung der Reviews/ der Reviewfassung
- Besprechung der Folien

Gliederung

Gliederung

- Kapitelüberschriften
- Kurze Übersicht über die Kapitelinhalte (ca. 100 Worte pro Kapitel)
- Literaturübersicht

Besprechung der Gliederung

- Struktur und geplanter Inhalt
- Literaturauswahl

Ausarbeitung (1/2)

Umfang

- ca. 8 Seiten Hauptinhalt, nicht mit gerechnet:
  - Titelblatt
  - Inhalts- / Tabellen- / Abbildungsverzeichnis
  - Bibliographie
- min. 5 Seiten Reintext
  - Ohne Abbildungen
  - Ohne Kapitelumbrüche

Vorlagen (Bitte einhalten!)

Liegen im Latex und Word Format vor.

`http://www-jj.cs.tu-dortmund.de/secse/pages/teaching/allgemeineInfo/index_de.shtml`

Ausarbeitung (2/2)

Inhalt

- Verständliche Darstellung des Inhalts
  - Zielgruppe: Bachelor-Studierende
  - Selfcontainment: Erklären der benötigten Begriffe
- Fokus auf Problemstellung, Umsetzung, Anwendung
- Eher weniger Metainformationen (Wer, wann, etc.)
- Fazit mit eigener kritischer Stellungnahme

Einstiegsliteratur

Wichtig: Nutzung weitergehender Literatur!

Review

Zwei Reviews

- Jeder bekommt zwei Reviews
- Jeder erstellt zwei Reviews

Inhalt und Form

- ca. 1 Seite
- Kurze Zusammenfassung
- Positive Punkte
- Problematische Punkte
- Verbesserungsvorschläge

Vortrag

Umfang

- Vortragsdauer: 30 Min (25-35 Min. ok)
- anschließend Diskussion

Beamer und Präsentationsrechner (PDF) stehen zur Verfügung.

Zum Inhalt

- Benötigte Grundlagen kurz aber ausreichend
- Wie in der Ausarbeitung auch:
  - Fokus auf Problemstellung, Umsetzung, Anwendung
  - Eher weniger Metainformationen (Wer, wann, etc.)
- Wenn möglich Live-Demonstrationen

Was selbstverständlich sein sollte....

Plagiat

Durchgefallen und Benachrichtigung des Prüfungsausschusses!

Verspätete Abgabe

- Ohne Absprache wird die Teilleistung mit 5 bewertet
- Absprache muss von Betreuer bestätigt werden

Anwesenheit

Bei allen Vorträgen ist die Anwesenheit Pflicht!

Abgabeformat

PDF

Zeitplan

15.04.13 (14:00)	Themenvorstellung
19.04.13 (12:00)	Rückmeldung
13.05.13 (24:00)	Abgabe Gliederung
10.06.13 (24:00)	Abgabe Vorversion Ausarbeitung
24.06.13 (24:00)	Abgabe Reviews
08.07.13 (24:00)	Abgabe Ausarbeitung
22.07.13 (24:00)	Abgabe Folien
16.09. - 20.09.13	Vorträge (unter Vorbehalt)

Noten ...

Ausarbeitung und Gliederung 40%

Struktur, Verständnis, Form, Inhalt, Quellen, ...

Review 10%

Struktur, “Hilfeleistung“, ...

Vortrag 40%

Verständlichkeit, Aufbau, ...

Teilnahme an der Diskussion 10%

Häufigkeit, Qualität, ...

CTF?

Capture the Flag

- Anwenden einiger erlernter Techniken aus dem Proseminar
- Hacken des Servers der gegnerischen Teams
- Verteidigen/Sichern des eigenen Servers

Voraussetzungen

- Falls Interesse von genügend Teilnehmern (min. 10)
- Separater Termin nach den Vorträgen
- Erfordert einige Stunden Zeit

Vergabe der Themen

Vergabe der Themen per Losverfahren

- Ein Los pro Teilnehmer
- Tauschen der Themen möglich
  - Mail mit den aktuellen Themennummern der beiden Tauschpartner
- christian.wessel@cs.tu-dortmund.de

Deadline

Freitag: 19.04.13 (12:00)

Themen (1/3)

- Buffer Overflows (165)
- “Man in the middle”-Attacken (inkl. Spoofing-Technologien) (203)
- SQL Injections (191)
- Cross Site Scripting (179)
- Port-Scanner (nmap, etc.) (154)

Themen (2/3)

- (D)DoS-Angriffe (190)
- Packet-Sniffer (bspw. wireshark) (118)
- Anonymisierungs-Tools (bspw. TOR, JAP, etc.) (106)
- Web Application Attack Framework (w3af) (129)
- Metasploit Penetration Testing-Werkzeug (166)

Themen (3/3)

- Google-Hacking (130)
- Honey Pots / Tar Pits (178)
- GPS-Hacking (155)
- Gesetze zur IT-Sicherheit (inkl. Ethik) (143)
- Biometrische Kryptographie (167)

Vielen Dank für die Aufmerksamkeit

Fragen?