Werkzeugunterstützung für sichere Software

Wintersemester 2013/14

LS14 - Arbeitsgruppe Software Engineering for Critical Systems

15.10.2013

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. 10 Seiten Hauptinhalt, nicht mit gerechnet:
  - Titelblatt
  - Inhalts- / Tabellen- / Abbildungsverzeichnis
  - Bibliographie
- min. 6 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: Notenabzug
- Absprache muss von Betreuer bestätigt werden

Anwesenheit

Bei allen Vorträgen ist die Anwesenheit Pflicht!

Abgabeformat

PDF

Zeitplan

16.10.13 (16:15)	Themenvorstellung (Themenliste)
17.10.13 (12:00)	Rückmeldung
19.11.13 (24:00)	Abgabe Gliederung
16.12.13 (24:00)	Abgabe Review-Fassung Ausarbeitung
12.01.14 (24:00)	Abgabe Reviews
31.01.14 (24:00)	Abgabe Ausarbeitung
06.02.14 (12:00)	Abgabe Folien
10.02.14 - 21.02.14	3 Tage 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, ...

Teil-Noten

Noten

1-6

6er-Regel

Eine 6 ->Durchgefallen

Erster Teil der Prüfungsleistung

Abgabe der Gliederung

Vergabe der Themen

Vergabe

Mail mit

- Name
- Matrikelnummer
- Wunschreihenfolge der Themen
- persönlicher Hintergrund (max. 100 Worte)

an thomas.ruhroth@tu-dortmund.de

Deadline

Donnerstag: 17.10.13 (12:00)

Themen Jürjens I

Analysis Techniques for Information Security Kap. 1, 2: Introduction, Foundations (JJ; 2 Bearbeiter)

Literatur:Anupam Datta, Somesh Jha, Ninghui Li, David Melski, and Thomas Reps: Analysis Techniques for Information Security. 2010, Morgan and Claypool. E-Book (kostenloser Zugang über Uninetz). Kap. 1, 2.

Analysis Techniques for Information Security Kap. 3: Detecting Buffer Overruns Using Static Analysis (JJ)

Literatur:Anupam Datta, Somesh Jha, Ninghui Li, David Melski, and Thomas Reps: Analysis Techniques for Information Security. 2010, Morgan and Claypool. E-Book (kostenloser Zugang über Uninetz). Kap. 3.

Themen Jürjens II

Analysis Techniques for Information Security Kap. 4: Analyzing Security Policies (JJ)

Literatur:Anupam Datta, Somesh Jha, Ninghui Li, David Melski, and Thomas Reps: Analysis Techniques for Information Security. 2010, Morgan and Claypool. E-Book (kostenloser Zugang über Uninetz). Kap. 4.

Analysis Techniques for Information Security Kap. 5: Analyzing Security Protocols (JJ)

Literatur: Anupam Datta, Somesh Jha, Ninghui Li, David Melski, and Thomas Reps: Analysis Techniques for Information Security. 2010, Morgan and Claypool. E-Book (kostenloser Zugang über Uninetz). Kap. 5.

Themen Pape I

CrypTool 2 – Visuelle Programmierung / Visualisierung von Algorithmen (SP)

Literatur:http://www.cryptool.org

CrypTool 2 – Kryptoanalyse (SP)

Literatur:
http://www.cryptool.org

Themen Pape II

Penetration Testing und Vulnerability Scanning – Metasploit(able) (SP)

Literatur:
http://www.metasploit.com/

Reverse Engineering – Java Decompiler (SP)

Literatur:
http://java.decompiler.free.fr/

Themen Pape III

Web Application Security: SQL Injection, Cross Site Scripting – w3af (SP)

Literatur:
http://w3af.org/

Themen Bürger I

Modellbasierte Softwareentwicklung mit Sicherheitseigenschaften und UMLsec (JB)

- Beachtung von Sicherheitseigenschaften in Softwarekomponenten zu Beginn eines Projekts
- UMLsec: formal fundierte Erweiterung von UML
- UML-Modelle mit sicherheitsrelevanten Anforderungen erweitern

Literatur:
http://www-secse.cs.tu-dortmund.de/jj/umlsec/

Themen Bürger II

CARiSMA (JB)

- plugin-basierte Plattform für Compliance-, Risiko- und Sicherheitsanalysen
- Reimplementierung des früheren UMLsec-Tools
- Überprüfung von UMLsec-Sicherheitseigenschaften auf Modellen

Literatur:
http://carisma.umlsec.de

Themen Bürger III

WBMP/Riskfinder (JB)

- Compliance: wichtig für Entwicklung sicherer Software für regulierte Industrie
- Anforderungsdokumente meist allgemein formuliert und natürlichsprachlicher
- WBMP/Riskfinder: Unterstützung bei der Identifikation relevanter Anforderungen
- BPMN/UML-Modell mit Prozess, Gegenüberstellung mit Anforderungen

Literatur:
http://www.ub.tu-dortmund.de/katalog/titel/1319080

Themen Bürger IV

Model-based risk assessment with CORAS (JB)

- Methode zur Durchführung von Sicherheitsrisikoanalysen
- Ansatz als UML-Profile
- Tool für Dokumentation, Wartung und Analysereport

Literatur:
http://coras.sourceforge.net/
http://www.ub.tu-dortmund.de/katalog/titel/1395510

Themen Bürger V

Packetsniffer (wireshark) (JB)

- Packetsniffer: wichtig u.a. für Fehlerdiagnose in Computernetzwerken
- Ethernet-Netzwerke für Web, Zugriff auf Cloud-Diensleistungen, Industristeuerungen Telefonanlagen, Hausautomation, Türzutrittssysteme
- Analysen des Netzwerkverkehrs wichtig für Entwicklung und Test sicherer Software

Literatur:
http://www.wireshark.org/

Vielen Dank für die Aufmerksamkeit

Fragen?