

Willkommen zum Proseminar Kickoff Software Engineering für Sichere Systeme Systeme für den Zahlungsverkehr

Agenda

- Betreuer
- Präsentationsseminar
- Vorgaben Ausarbeitung
- Vorgaben Vortrag
- Milestones
- Notenbildung
- Sonstiges Organisatorisches
- Themenvergabe

Betreuer

- Software Engineering für Sichere Systeme
 - Dr. Ing. Holger Schmidt
 - Holger.Schmidt@cs.tu-dortmund.de
- Systeme für den Zahlungsverkehr
 - Dipl. Winf. Stephan Faßbender
 - Stephan.Fassbender@cs.tu-dortmund.de
- Präsentationsseminar
 - Dipl. Winf. Stephan Faßbender
 - Stephan.Fassbender@cs.tu-dortmund.de

Präsentationsseminar

- 29.10.2010, 14:00-16:00 (OH16 Raum 205) Vortrag über Wissenschaftliches Arbeiten / Schreiben
- 05.11.2010, 10:00-12:00 und 13:00-15:00 (OH16 Raum 205) Praktische Übung zu wissenschaftlichem Arbeiten / Schreiben
- 03.12.2010, 10:00-12:00 (OH16 Raum 205) Vortrag zu Präsentation und Rhetorik
- 10.12.2010, 10:00-12:00 und 13:00-15:00 (OH16 Raum 205) Übungen zu Vortrag und Rhetorik
- 14.01.2011, 10:00-16:00 (OH16 Raum 205) Kurzvorträge (5 Minuten) zum Proseminarthema und aktuellem Stand

Vorgaben Ausarbeitung

- 9-10 Seiten Ausarbeitung
 - Ohne Inhalts- / Tabellen- / Abbildungsverzeichnis, Titelblatt, Bibliographie und Index
 - Min 7 Seiten Reintext (Ohne Abbildungen / Kapitelumbrüche etc.)
 - Formatvorlagen verwenden und einhalten
 - Liegen im Latex und Word Format vor
 - Latex wird dringend empfohlen!!!
 - <http://ls14-www.cs.tu-dortmund.de/main2/jj/teaching/formatVorlagen/index.htm>
 - Fazit mit eigener kritischer Stellungnahme sollte enthalten sein

Vorgaben Ausarbeitung

- Kapitel / Paper sind Grundlage und Kernliteratur
 - Andere Quellen gewünscht
- Wissenschaftliches Arbeiten
 - Quellenrecherche, -prüfung und -angaben
 - Fehlerhafte Quellenangaben oder Plagiatsversuche führen zur Abwertungen oder Ablehnung der Ausarbeitung
 - Formulierungen
- Abgabe elektronisch und 1 Mal gedruckt
 - Gedruckte Version mit Unterschrift der ehren-wörtlichen Erklärung

Vorgabe Vortrag

- Dauer 25 Minuten + 10 Minuten Diskussion
 - Ist einzuhalten. Kleine Abweichungen in Ordnung
- Ziel ist es den anderen Seminarteilnehmern den Themenblock verständlich näher zu bringen
- Fokus auf die wichtigen Aspekte
- Anschließende Diskussion in der Seminarrunde
- Spezieller Medieneinsatz sollte abgesprochen werden
- Standardpräsentationsequipment wird vorhanden sein

Milestones

- 18.10.2010 Kickoff mit Themenvergabe
- 19.11.2010 Vorschlag Gliederung und Quellenverzeichnis
 - Erster Vorschlag für eine Gliederung der Seminararbeit
 - Ergebnis der Quellensuche als Quellenverzeichnis
 - Elektronisch als PDF an den Betreuer
 - Terminvorschläge (mindestens 3) für Woche 22.11-26.11
 - Deadline : 19.11.2010 12:00 Uhr
- 22.11 - 26.11.2010 Feedback
 - Schriftliches (Auf Wunsch oder in angebrachten Fällen persönliches) Feedback zum Exposé

Milestones

- 14.01.2011 Kurzvorträge (5 Minuten) zum Proseminarthema und aktuellem Stand
- 28.1.2011 Erste vollständige Version Ausarbeitung und Vortrag
 - Abgabe der aus Sicht des jeweiligen Seminarteilnehmers finalen Fassungen der Ausarbeitung und des Vortrags
 - Elektronisch als PDF, PPT oder ODP an Betreuer
 - Terminvorschläge (mindestens 3) für Woche 31.01-04.02
 - Deadline : 28.01.2011 12:00 Uhr
- 31.01 - 04.02.2011 Persönlicher Feedbacktermin
 - jeweils auf 30 Minuten begrenzt

Milestones

- 18.02.2011 Finale Version Ausarbeitung und Vortrag
 - Finale Version der Ausarbeitung und der Präsentation für den Vortrag
 - Elektronisch als PDF, PPT oder ODP an
 - Deadline : 18.02.2011 12:00 Uhr
- Woche ab dem 21.02.2011 Blockseminar
 - Genauer Termin nach Absprache
 - Falls ein Termin / Uhrzeit in der Woche nicht geht Mail an Stephan.Fassbender@cs.tu-dortmund.de

Notenbildung

- Ausarbeitung 50%
 - Inhalt
 - Struktur
 - Verständnis
 - Form
 - Quellen
- Vortrag 40%
 - Verständlichkeit
 - Aufbau
- Teilnahme an Diskussionen 10%

Sonstiges Organisatorisches

- Die Bücher werden in der Bereichsbibliothek Informatik zur Verfügung gestellt
 - Sie können jeweils für einen Tag ausgeliehen werden, um das für den eigenen Vortrag benötigte Kapitel zu kopieren
- Bei Fragen oder Problemen:
 - Mail an Betreuer
 - Kurze Beschreibung worum es geht
 - Unter Umständen Terminvorschlag
- Nach Ende des Kickoffs bitte schnellst möglich eine Mail mit Thema und Kontaktdaten an stephan.fassbender@cs.tu-dortmund.de

Themenvergabe

SE für Sichere Systemer

- Introduction to Computer Security
- Introduction to Cryptography
- Symmetric Encryption - DES and AES
- Asymmetric Encryption - RSA
- Cryptographic Hash Functions
- Authentication Mechanisms
- Digital Signatures, Certificates and Key Management
- SSL (Secure Socket Layer) Protocol
- Diffie-Hellman Key Exchange, Needham-Schroeder, and Kerberos Protocols

Themenvergabe

SE für Sichere Systeme

- Access Control Mechanisms
- Vulnerability Analysis
- Intrusion Detection
- Malicious Logic
- Security Evaluation and Certification (2 Personen)
- IT-Grundschutz - Gefährdungskataloge und Vorgehensweise (2 Personen)
- Nonmalicious Program Errors
- Smart Card Security

Themenvergabe

Systeme für den Zahlungsverkehr

- Basics and History of ePayment
- Requirements for ePayment
- Symmetric Encryption - DES and AES
- Asymmetric Encryption - RSA
- Authentication Mechanisms
- Cryptographic Hash Functions
- Digital Signatures, Certificates and Key Management
- The iKP und the uiKP protocol
- The SET protocol

- A Secure Account-Based Mobile Payment Protocol
- Towards Multiple-Payment Schemes for Digital Money
- Off-Line Micro-payment System for Content Sharing in P2P Networks
- P2P-Paid: A Peer-to-Peer Wireless Payment System