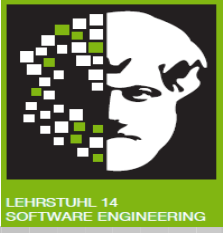


Konzeption und Entwicklung eines sicheren Cloud-basierten Internetbanking-Systems mit anschließender Sicherheitsanalyse auf Basis von Business Process Mining

im SoSe 2011 & WS 2011/12

Prof. Jan Jürjens, Dr. Holger Schmidt, Stephan Fassbender
TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

Agenda

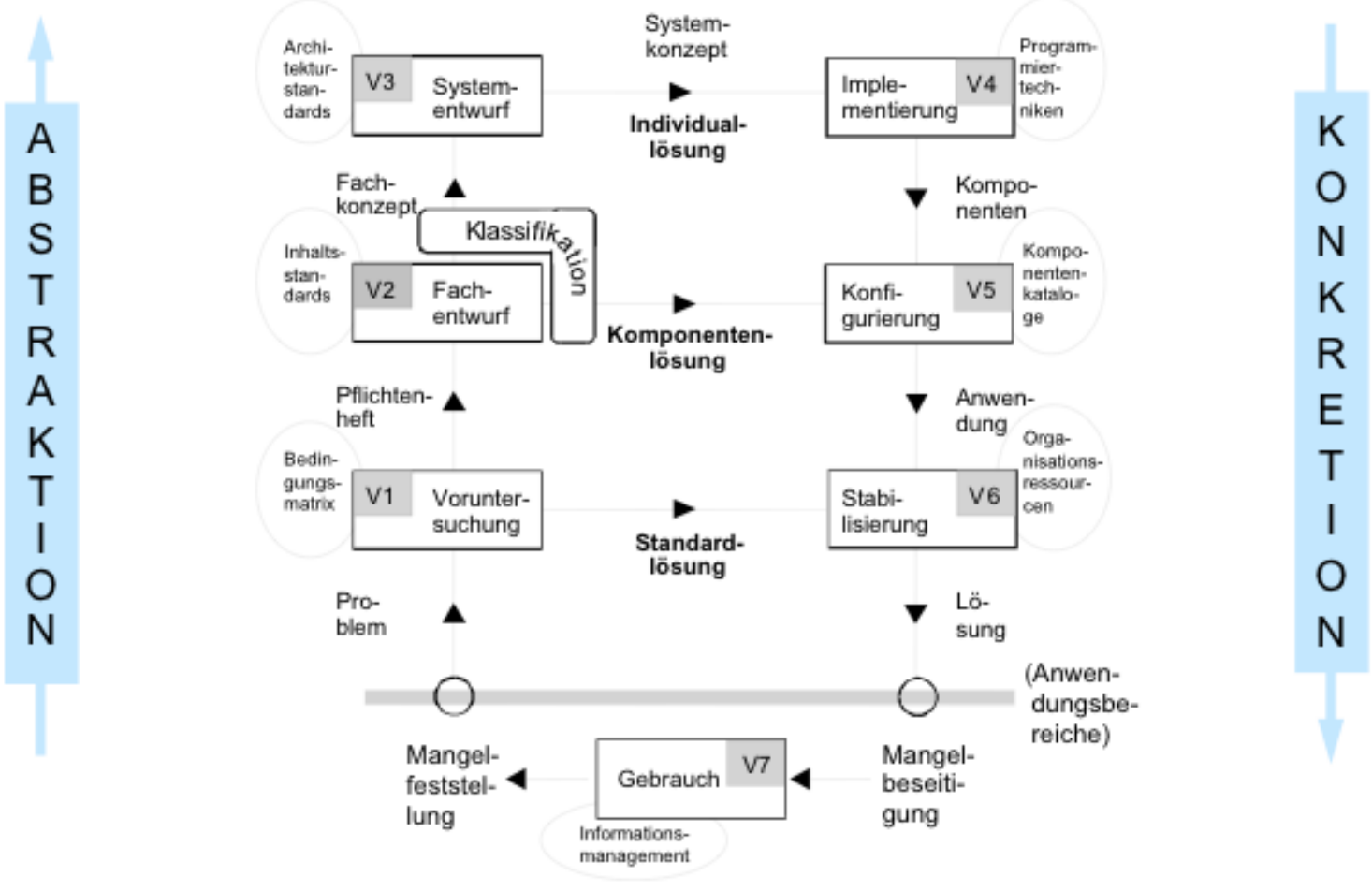
1. Das Vorgehen
2. Rollen
3. Seminarphase
4. Rollen & Themenvergabe
5. Terminklärung

Agenda

1. Das Vorgehen
2. Rollen
3. Seminarphase
4. Rollen & Themenvergabe
5. Terminklärung

Wie soll Vorgegangen werden?
Vorgehensmodell

Multipfad – Vorgehensmodell (MP2M)



Wie soll Vorgegangen werden?
Projektplan SoSe

Aufgabe	Anfang	Ende	Wochen
Einarbeitungsphase			
- Vorbereitung u. Seminar	KW15	KW16	2
- Projektplan erstellen	KW17	KW17	1
Voruntersuchung			
- Anforderungserhebung und -analyse	KW18	KW20	3
- Spezifikation	KW21	KW22	2
Fachentwurf			
- Prozessmodellierung	KW23	KW25	3
- Grafische Benutzeroberfläche	KW26	KW26	1
Systementwurf			
- Auswahl von Technologien	KW27	KW27	1
- Architekturentwurf	KW28	KW29	2
Dokumentation			
- Zwischenbericht	KW15	KW29	15

Wie soll Vorgegangen werden?
Projektplan WS

Aufgabe	Anfang	Ende	Wochen
Implementierung	KW41	KW51	11
Konfigurierung	KW2	KW2	1
Stabilisierung - Unit-Testen - Anwendungsbeispiele - Seminar zu Softwaresicherheit - Penetrationstesten	KW3	KW6	4
Dokumentation - Endbericht	KW41	KW6	16

Agenda

1. Das Vorgehen
2. Rollen
3. Seminarphase
4. Rollen & Themenvergabe
5. Terminklärung

Rollen

- Jeder muss in jeder Phase arbeiten!!
- Aber:
  - Pro Phase gibt es min. einen Fachmann
    - Arbeitet sich in Thema ein
    - Transferiert Wissen
    - Hat den Hut in seinen Themen auf
  - Es gibt Phasenübergreifende Rollen

Rollen

- Cloud Entwickler & Architekt (2 Personen)
- Compliance Analyst (2 Personen)
- Test Ingenieur (2 Personen)
- Security Analyst (1 Person)
- Prozess Analyst (2 Personen)
- Projektmanager (1 Person)
- Infrastruktur- & Qualitätsmanager (1 Person)

Rollen

- Cloud Entwickler & Architekt (2 Personen)
  - Vor allem gefordert bei
    - der Erstellung des Systemkonzept
    - der Implementierung
    - der Durchführung von Customizing
  - Erfordert Wissen über
    - Aufbau von Clouds (Technisch / Konzeptionell)
    - Zugriff auf Clouds (API, Management etc.)
    - Software Architekturen für Clouds

Rollen

- Compliance Analyst (2 Personen)
  - Vor allem gefordert bei
    - der Erstellung des Pflichtenhefts
    - der Erstellung des Fachkonzepts
  - Erfordert Wissen über
    - Gesetzgebung bezüglich IT im allgemeinen
    - spezielle Regelwerke für Cloud
    - domänenspezifische Regularien

Rollen

- Test Ingenieur (2 Personen)
  - Vor allem gefordert bei
    - der Erstellung des Systemkonzepts
    - der Implementierung
    - der Stabilisierung
  - Erfordert Wissen über
    - testen zur Erstellungszeit
    - testen zur Laufzeit

Rollen

- Security Analyst (1 Person)
  - Vor allem gefordert bei
    - der Erstellung des Pflichtenhefts
    - der Erstellung des Systemkonzepts
    - der Stabilisierung des Systems
  - Erfordert Wissen über
    - Penetrationtesting
    - IT Sicherheit im Allgemeinen
    - Standards
    - Angriffe

Rollen

- Prozess Analyst (2 Personen)
  - Vor allem gefordert bei
    - der Erstellung des Pflichtenhefts
    - der Erstellung des Fachkonzepts
    - der Stabilisierung
  - Erfordert Wissen über
    - Business Prozesse
    - Prozess Management
    - Prozess Mining
    - Prozess Modellierung

Rollen

- Projektmanager (1 Person)
  - Vor allem gefordert bei
    - Der Zeit- und Ressourcenplanung
    - Vorgehen und Teammanagement
    - Controlling
    - Koordination
  - Erfordert Wissen über
    - IT Projektmanagement
    - Controlling
    - Teamführung

Rollen

- Infrastruktur- & Qualitätsmanager (1 Person)
  - Vor allem gefordert bei
    - Bereitstellung von Tools
    - Bereitstellung von Infrastruktur
    - Erstellung von Qualitätsrichtlinien
    - Prüfung von Endprodukten
  - Erfordert Wissen über
    - Entwicklungswerkzeuge
    - Qualitätsmanagement

Rollen

- Cloud Entwickler & Architekt (2 Personen)
- Compliance Analyst (2 Personen)
- Test Ingenieur (2 Personen)
- Security Analyst (1 Person)
- Prozess Analyst (2 Personen)
- Projektmanager (1 Person)
- Infrastruktur- & Qualitätsmanager (1 Person)

Agenda

1. Das Vorgehen
2. Rollen
3. Seminarphase
4. Rollen & Themenvergabe
5. Terminklärung

Seminarphase
Ergebnisse

- Wissen gewinnen
  - Fachmann erarbeitet Wissen und sollte sich auf PG relevante Themen fokussieren
- Vortrag
  - Als Mini-Vorlesung (min. 45 Minuten) zum Thema gedacht
  - Evtl. Wiederholung im Verlauf der PG
    - wenn Thema relevant wird und sollte dann genauer auf den aktuellen Stand angepasst sein
- Projekthandbuch
  - Min 5 Seiten Summary
  - Weiterführende Quellen, HowTo's, Resourcenlinks usw.

Seminarphase
Themen & Rollen

- Cloud Entwickler & Architekt
  - Cloud Grundlagen und Architekturen
  - Cloud Infrastrukturen, Programming und Management
- Compliance Analyst
  - Compliance spezifisch für Clouds
  - Compliance spezifisch für Banken
- Test Ingenieur
  - Testen während der Erstellung
  - Testen zur Laufzeit

Seminarphase
Themen & Rollen

- Security Analyst
  - Security
- Prozess Analyst
  - Business Process Mining
  - Prozess- und IT-Management für Banken
- Projektmanager
  - IT-Projektmanagement
- Infrastruktur- & Qualitätsmanager
  - Developing-Tools & Qualitätsmanagement

Seminarphase
Themen

- Cloud Grundlagen und Architekturen
  - Aufbau
  - Virtualisierungstechniken
  - dezentrales Datenmanagement
  - Kommunikationsprotokolle
  - Architekturen für Clouds (SOA etc.)
- Literatur

  - M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “Above the clouds: A berkeley view of cloud computing,” EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28, 2009
  - L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, “A break in the clouds: towards a cloud definition,”SIGCOMM Comput. Commun. Rev., vol. 39, no. 1, pp. 50–55, 2009.

Seminarphase
Themen

- Cloud Infrastrukturen, Programming und Management
  - OS Cloud Systeme
  - Cloud Anbieter vergleichen
    - Datenmanagements
    - API
    - externer Zugriff auf die Cloud (GUI, Daten-In/Out)
    - Adminstrationsinterface (Performance beobachten, etc)

Seminarphase
Themen

- Compliance allgemein und spezifisch für Clouds
  - Service Level Agreements (SLA's)
  - Statements on Auditing Standards (SAS) Number 70 Type II
  - Vergleich verschiedener Zertifikate
  - Bundesdatenschutzgesetz
  - Telekommunikationsgesetz

- Literatur:
  - Fraunhofer SIT, Cloud Computing Sicherheit - Schutzziele.Taxonomie.Marktübersicht, 2009

Seminarphase
Themen

- Compliance spezifisch für Banken
  - MARisk BA
  - 25a Kreditwesengesetz (KWG), Riskomanagement für den Finanzsektor
  - 33 Abs.2 Wertpapierhandelsgesetz (WpHG), Richtlinien für Outsourcing im Finanzsektor

- Literatur:

- Rath and Sponholz, IT-Compliance, Erich Schmidt Verlag, 2009
- http://www.bafin.de/cln_170/nn_722758/SharedDocs/Veroeffentlichungen/DE/Service/Rundschreiben/2009/rs__0915__ba__marisk.html

Seminarphase
Themen

- Testen während der Erstellung
  - White-Box Testen z.B. mit Junit
  - Adäquate Auswahl von Testdaten (unter Beachtung von Äquivalenzklassen)
  - Organisation, z.B. Checklisten mit erwarteten Testresultaten

- Literatur:
  - Sommerville, I. (2007). Software Engineering 8 [Chapter 23]. Addison-Wesley.
  - Franz, K. (2007). Handbuch zum Testen von Web-Applikationen. Springer

Seminarphase
Themen

- Testen zur Laufzeit
  - Black-Box Testen z.B. mit JWebUnit (http://jwebunit.sourceforge.net/index.html) für Browser-basierte Anwendungen
  - Spezifisches Testen für Clouds
  - Adäquate Auswahl von Testdaten (unter Beachtung von Äquivalenzklassen)
  - Organisation, z.B. Checklisten mit erwarteten Testresultaten
- Literatur:
  - Sommerville, I. (2007). Software Engineering 8 [Chapter 23]. Addison-Wesley.
  - Franz, K. (2007). Handbuch zum Testen von Web-Applikationen. Springer

Seminarphase
Themen

- Security
  - Penetration-Testen und Fuzzing
  - Protokollanalyse
  - Angriffe, z.B. Sniffing, Man-In-the-Middle

- Literatur:
  - Bishop, M. (2003). Computer Security - Art and Science [Chapter 19.3.3]. Addison-Wesley.
  - Sommerville, I. (2007). Software Engineering 8 [Chapter 23]. Addison-Wesley.

Seminarphase
Themen

- Business Process Mining
  - Kontrollfluß-Mining
  - Aufdecken von Anomalien in Kontrolfluß (Soll-Ist-Vergleich, d.h. Definiertes Prozessmodell mit aus Ausführung gewonnenem Modell vergleichen)

- Literatur:
  - Van der Aalst, Workflow Mining: Discovering Process Models from Event Logs, 2004
  - Van der Aalst, Process Mining and Security: Detecting Anomalous Process Executions and Checking Process Conformance, 2005
  - Wespi, Dacier and Debar, Intrusion Detection Using Variable-Length Audit Trail Patterns, 2000

Seminarphase
Themen

- Prozess- und IT-Management für Banken
  - Business und IT Prozesse
  - Business Process Engineering
  - IT Riscmanagement / Landscapeplanning
  - Charakteristika heutiger Banken IT System
  - IT Abläufe in Banken
- Literatur
  - Moormann, Jürgen, Schmidt, Günter : „IT- in der Finanzbranche“, Springer, Heidelberg, 2006
  - Alt, Rainer, Bernet, Beat, Zernet, Thomas: „Transformation von Banken“, Springer, Berlin, 2009
  - Strahringer, Susanne: „Business engineering“, Dpunkt-Verl, Heidelberg, 2005
  - Riese, Cornelius: „Industrialisierung von Banken“, GWV Fachverlag GmbH, Wiesbaden
  - Sax, Anke: „Methoden der strategischen Planung und Steuerung der IT“, Gabler Verlag, 2010

Seminarphase
Themen

- IT-Projektmanagement
  - Agile Methoden (Scrum, Extrem Programming, usw)
  - Lean Softwaredevelopment
  - Vorgehensmodelle
  - Zeit- und Ressourcenplanung
  - Projektcontrolling (Projektkennzahlensystem usw.)
  - Teammanagement (Konfliktlösung, Steuerung, fähigkeitsbasierte Allocation, Wissenmanagement)
- Literatur
  - Eckstein, Jutta: „Agile Softwareentwicklung mit verteilten Teams“, D-Punkt, Heidelberg, 2009
  - Tiemeyer, Ernst: „Handbuch IT-Projektmanagement“, Hanser, München, 2010

Seminarphase
Themen

- Developing-Tools & Qualitätsmanagement
  - IDE's (Eclipse, Netbeans, usw.)
  - Versionsmanagement (SVN, Git, usw.)
  - Build Tools (Ant, Maven, Cbuild, usw.)
  - Coding & Documentation Policies
  - Bug Tracking, Groupware
  - Qualitätsmanagement, -metriken und -durchsetzung
  - QA Tools (FindBungs, Check Style, Squale, usw.)
- Literatur
  - Bartsch-Beuerlein, Sandra: „Qualitätsmanagement in IT-Projekten“, Hanser, München, 2000

Agenda

1. Das Vorgehen
2. Rollen
3. Seminarphase
4. Rollen & Themenvergabe
5. Terminklärung

Rollen & Themenvergabe

1 Cloud Grundlagen und Architekturen
2 Cloud Infrastrukturen, Programming und Management
3 Compliance spezifisch für Clouds
4 Compliance spezifisch für Banken
5 Testen während der Erstellung
6 Testen zur Laufzeit
7 Security
8 Business Process Mining
9 Prozess- und IT-Management für Banken
10 IT-Projektmanagement
11 Developing-Tools & Qualitätsmanagement

Agenda

1. Das Vorgehen
2. Rollen
3. Seminarphase
4. Rollen & Themenvergabe
5. Terminklärung