Lehrgebietsvorstellung “Software Engineering für kritische Systeme”

Jan Jürjens
LS 14 (Software Engineering), Fakultät Informatik & Fraunhofer Institut für Software- und Systemtechnik, Dortmund

technische universität dortmund

Fraunhofer ISST

http://jan.jurjens.de

Wer bin ich ?

- Professor für Software Engineering an der TU Dortmund
- Wissenschaftskoordinator „Enterprise Engineering“ am ISST
- Leiter der Fraunhofer-Attract-Projektgruppe „Architectures for Auditable Business Process Execution (Apex)“ (2009-2014)
- Wissenschaftlicher Direktor des EU-Projektes „Security Engineering for Lifelong Evolvable Systems (Secure Change)“
- Ehrenhalber: Senior Member am Robinson College (Univ. Cambridge)

Vorher u.a.:

- Royal Society Industrial Fellow bei Microsoft Research Cambridge
- Research Fellow am Robinson College (Univ. Cambridge)
- Postdoc an der TU München
- Promotion zu „Principles for Secure Systems Design“ (Univ. Oxford)
- Forschungsaufenthalte am LFCS (Univ. Edinburgh) und Bell Labs (Palo Alto)
- Studium Mathematik (Nebenfach Informatik) an Univ. Bremen und Univ. Cambridge

Wer ist meine Forschungsgruppe ?

- Misha Aizatulin (Microsoft Research Cambridge, Projekt Csec)
- H. Selcuk Beyhan (Logica (Germany))
- Stephan Braun (TUD, Projekt SecureClouds)
- Francois Dupressoir (Microsoft Research Cambridge, Projekt Csec)
- Stephan Faßbender (TUD)
- Stephan Gaschler (ISST, Projekt Apex)
- Michael Giddings (Open University)
- Jan-Christoph Küster (ISST, Projekt Apex)
- Christopher McLaughlin (IBM)
- Martin Ochoa (TUD, Projekt Secure Change)
- Sebastian Pape (TUD)
- Stefan Taubenberger (Münchener Rückversicherung)
- Dr. Sven Wenzel (TUD)

Vertrauenswürdige IT-Systeme

IT Systeme durchziehen heute fast alle Funktionen in Wirtschaft und Gesellschaft. IT hat direkten (oft invasiven) Einfluss auf fast alle Aspekte menschlichen Lebens.

Die Erwartungen an die Vertrauenswürdigkeit dieser Systeme sind daher in den letzten 10 Jahren stark gestiegen. Diese Erwartungen werden oft nicht erfüllt. Teil des Problems ist, dass die bislang verwendeten System- und Software-Entwicklungsmethoden mit den gestiegenden Erwartungen bei gleichzeitig steigender Systemkomplexität nicht mithalten konnten.

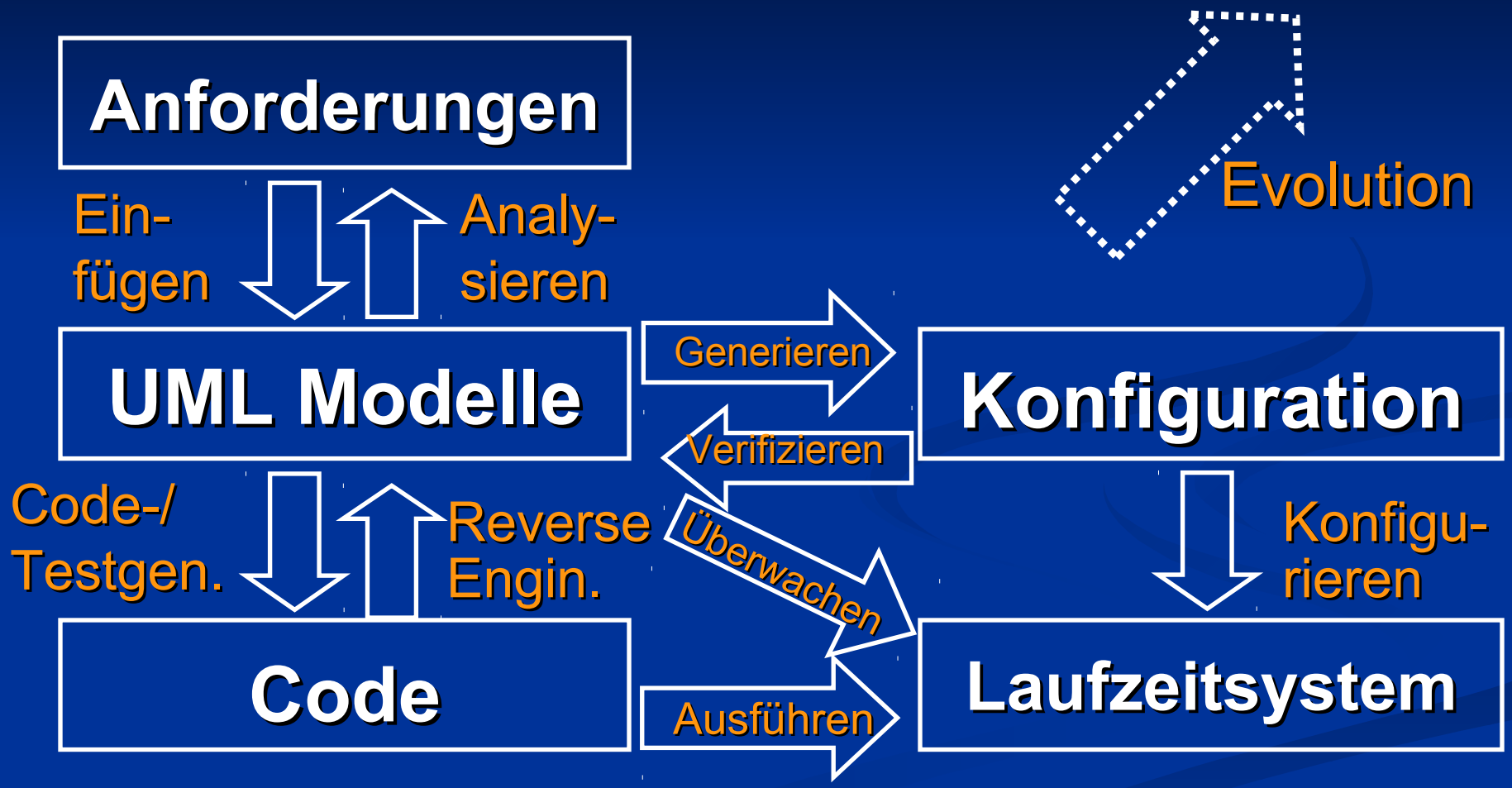
Offene Systeme

Aus Flexibiliäts- und Kostengründen sind moderne IT Systeme meist über offene Infrastrukturen realisiert, zum Beispiel:

- Internet
- Mobile Netze

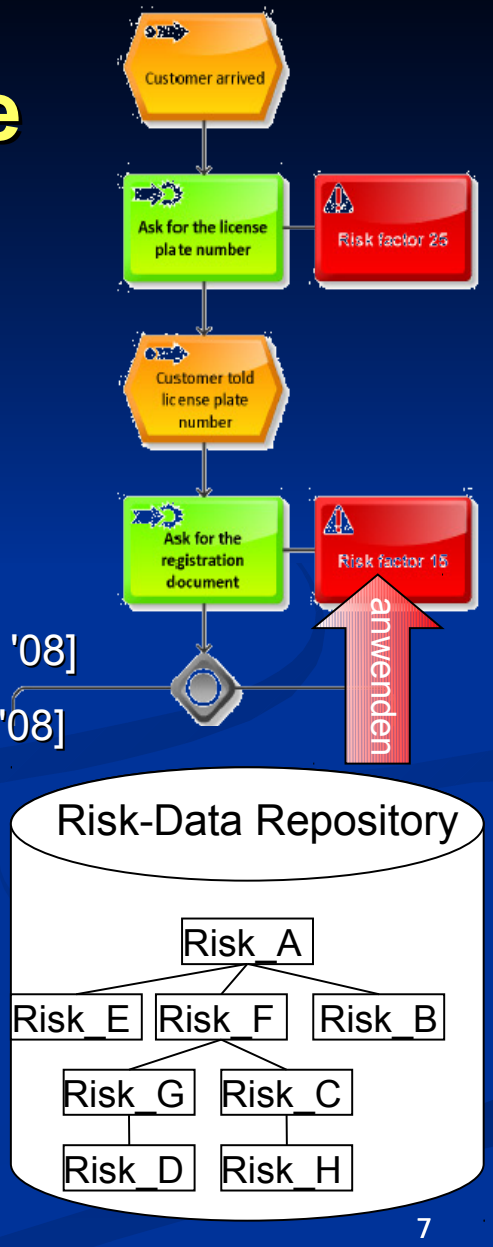
Aufgrund ihrer Offenheit sind sie dem Zugriff von Personen ausgesetzt, die in verschiedenem Maße vertrauenswürdig sind. Dieser Zugriff muss daher systemseitig reguliert werden. Aus Flexibiliäts- und Kostengründen wird dies oft auf der Softwareebene gelöst. Eine vertrauenswürdige IT braucht also sichere Software.

Modellbasierte Entwicklung

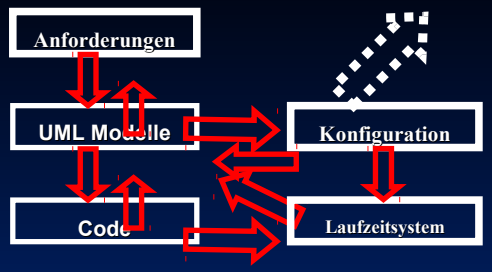


Governance, Risk & Compliance auf Geschäftsprozessen

- Idee: Automatische Analyse von Geschäftsprozessmodellen auf operationale Risiken, z.B.:
  - gegenüber Benutzerberechtigungen zur Laufzeit, sowie der Benutzer-berechtigungen gegenüber der Sicherheitspolitik, [FASE '08] [ICSE '08]
  - automatische Risiko-Identifikation und -Bewertung
- Laufendes Projekt (Fraunhofer Attract): Architekturen für auditierbare Geschäftsprozessausführung (Apex).



Werkzeugunterstützung



Java editor
data flow
UML editor
"uses"
Java code
UMLsec model
Code with Assert's; Tests
Text Report
Attack Trace
Assertion/Test Generator
Analyzer
Control Flow Graph
Local Code Checker
Automated Theorem Prover
Attack generator
Security Analyzer
FOL fmla
Prolog prog.

[UML 04, FASE 05, Jour. Softw. Tools & Techn. Transf. (STTT) 07]

Internes Informationssystem bei BMW

MetaSearch Engine: Personalisierte Suche im Firmen-Intranet (passwort-geschützt).

[ICSE 07]

Einige Dokumente sehr sicherheitskritisch.

Über 1.000 potentielle Benutzer, 280.000 Dokumente, 20.000 Anfragen pro Tag.

Nahtlos in unternehmensweite Sicherheitsarchitektur integriert. Bietet Sicherheitsdienste für Anwendungen (Benutzerauthentisierung, rollenbasierte Zugangskontrolle, globales Single-Sign-On), Ansatzpunkte für weitere Sicherheitsdienste.

Erfolgreich mit UMLsec analysiert.

BMW Group

Weitere Anwendungen

- Gesundheitskarte: Architektur untersucht, Schwachstellen aufgedeckt [Jour. Meth. Inform. Medicine '08]
- Mobile Architekturen bei O_2 (Germany) [ICSE '08]
- Digitaler Formularschrank bei HypoVereinsbank [SAFECOMP '03]
- Common Electronic Purse Specifications [ASE '01]
  (Globaler Standard für elektronische Geldbörsen):
  mehrere Schwachstellen aufgedeckt
- Biometrische Authentisierungssysteme: mehrere Schwachstellen aufgedeckt [ACSAC '05, Models '09]
- Gesundheitsinformationssysteme [Caise '09]

Hiwi-Tätigkeiten

Es gibt verschiedene Möglichkeiten für eine Beschäftigung als Hiwi am Fraunhofer ISST oder am LS 14 / TUD:

- Unterstützung des "Secure Change" Projektes (Java-Programmierung eines UML-Analyse Werkzeuges)
- Unterstützung des "Architectures for Auditable Business Process Execution (APEX) - Monitoring, Control, and Compliance" Projektes
- Unterstützung in der Lehre (Tutorien in SWK-Vorlesung, WS 2011/12, Folienerstellung etc)

Informationen unter: http://jan.jurjens.de/jobs/hiwis.html

Abschlussarbeiten

Abschlussarbeiten können in inhaltlicher Beziehung zu einer Hiwi-Tätigkeit am Fraunhofer ISST oder LS 14 / TUD durchgeführt werden.

Sie können insbesondere in Zusammenhang mit Anwendungsprojekten am ISST durchgeführt werden, wodurch sich vielfältige Möglichkeiten zu Kooperation mit Unternehmen ergeben, zB:

- Apex: Versicherungen / Banken (Münchener Rückversicherung, Signal Iduna, Wüstenrot), Softwarehersteller (SAP, IDS Scheer)
- Secure Change: Telekom / Smartcards (Telefonica, Gemalto)
- Csec: Microsoft Research Cambridge
- Secure Clouds: Cloud-Anbieter (Nionex, LinogistiX), IT-Berater (ITESYS, TÜV-IT)

Informationen unter: http://jan.jurjens.de/jobs/hiwis.html

Einige Themen für Abschlussarbeiten

- Formale Abbildung von regulatorischer Compliance auf Security Policies
- Modellierung und Automatische Sicherheits-Analyse für Cloud Computing Systems
- Business Process Mining
- Spezifikation von IT-Sicherheitszielen für die Geschäftsprozessmodellierung und deren Integration in die Ausführung im Workflow
- Design und Entwicklung einer Schnittstelle zwischen der Business Prozess Management Suite ARIS und dem Sicherheitsanalysetool UMLsec zur Compliance Analyse in der Versicherungsdomäne
- Generierung von Geschäftprozessen mit OpenArchitectureWare unter Berücksichtigung von Sicherheitseigenschaften
- Werkzeuggestützte Modell-basierte Sicherheitsanalyse
- Werkzeugunterstützte Analyse von sicherheitskritischen SAP-Berechtigungen im Finanzbereich
- Modell-basiertes Return on Security Investment (ROSI) im IT-Sicherheitsmanagement

Informationen unter: http://jan.jurjens.de/jobs/hiwis.html

Auslandsaufenthalte

Wir haben vielfältige internationale Kontakte, mit denen Auslandsaufenthalte arrangiert werden können, zB:

- Projekt Secure Change: Unis Trento (I), Oslo, Innsbruck, Lille, Besancon, Leuven, Open University (bei London); Firmen Deep Blue (I), Gemalto (F), Telefonica (S), Thales (F)
- Kontakte über externe Doktoranden: Microsoft Research Cambridge, IBM (UK)
- Alma Maters: Unis Cambridge, Edinburgh, Oxford

Viele weitere Kontakte für Auslandsaufenthalte.

Und danach ?

“Erfolgreich auch in der Krise“
[http://fraunhofer.de/presse/presseinformationen/2009/06/Presseinformation18062009Ergebnis.jsp]

“Mit 1,4 Mrd. Euro erreichte das Finanzvolumen der Fraunhofer-Gesellschaft im vergangenen Jahr ein neues Rekordniveau. ... Im Geschäftsjahr 2008 konnten 1400 neue Stellen besetzt werden. Damit sind 15 000 Mitarbeiterinnen und Mitarbeiter in der Forschungsorganisation tätig. ...

Trotz der weltweiten Finanz- und Wirtschaftskrise geht die Fraunhofer-Gesellschaft für die Jahre 2009 und 2010 von weiterem Wachstum und einer positiven Entwicklung ihrer Ertragslage aus. Der Grund: Zahlreiche Firmen investieren auch in der Krise in Forschung und Entwicklung. ...

Besonders erfreulich: Fraunhofer gehört zu den beliebtesten Arbeitgebern deutscher Studentinnen und Studenten. Das ist das Ergebnis eines Rankings, das die Wirtschaftwoche im Mai diesen Jahres veröffentlicht hat. Laut der Universum Studentenbefragung belegt Fraunhofer den 2. Platz nach dem Autobauer Porsche.“

Und: Promotion projekt-begleitend möglich.

Kontakt: http://jan.jurjens.de

Backup-Folien

Lehrveranstaltungen WS 2011/12

- Software-Konstruktion (INF-BSc-211, Wahlpflicht-Vorlesung Bachelor + Übung (2+1 SWS))
- Oberseminar (Seminar (2 SWS)): Informationen auf Anfrage

Informationen unter: http://jan.jurjens.de/teaching
Zuordnung der Wahlveranstaltungen zu Schwerpunktgebieten (Diplom):

- Sicherheit und Verifikation
- Software-Konstruktion

Forschungsbereich Master: Software, Sicherheit und Verifikation

(weitere Zuordnungen sind möglich)

Lehrveranstaltungen in folgenden Semestern (geplant)

SoSe 2011:

- Master-Basismodul Software-Engineering (4 SWS; angefragt)
- FP „Werkzeugunterstützung zur Entwicklung sicherer Softwaresysteme (4 SWS; angefragt)
- FP „Business Process Mining“ (4 SWS; angefragt)
- … Weitere in Planung ...

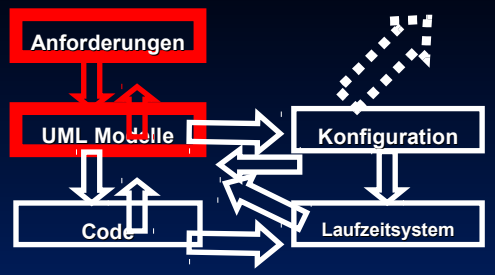
Langfristig:

- Softwarearchitekturen im Finanz- und Versicherungsbereich (Vertiefungs-Vorlesung, 2+1 SWS)
- Modellbasierte Softwaretechniken für sichere Systeme (Vertiefungs-Vorl., 2+1 SWS)
- Werkzeugunterstützung für UML- und Geschäftsprozessmodelle (Fachprojekt oder Projektgruppe)
- e-Finance (Seminar), e-Business (Seminar)
- Ausgewählte Themen des Modellbasierten Sicherheits-Engineerings (Seminar)
- Architektur- und Geschäftsprozess-Modellierung (Seminar)
- E-Commerce Systeme: Architekturen und Anwendungen (Seminar)
- Geschäftsprozesse und Compliance (Proseminar)
- Weitere mögliche Themen: “Konstruktion von Internetbank-Architekturen”, “Software-Testen”, “Systeme für den Zahlungsverkehr”, “Compliance-Regulierungen“, „Smartcard-Programmierung“, „e-Government-Systeme“, „Enterprise-Architekturen“, „Software-Archäologie“, „Software-Evolution und -Wartung“

Vorschläge für Projektgruppen können ebenfalls berücksichtigt werden.

Informationen unter: http://jan.jurjens.de/teaching

Modellierung mit UMLsec

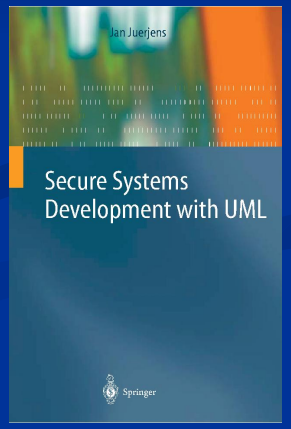


Ziel:

- Dokumentation und automatische Analyse von sicherheits-relevanten Informationen (z.B. Sicherheits-Eigenschaften und -Anforderungen) als Teil der Systemspezifikation.

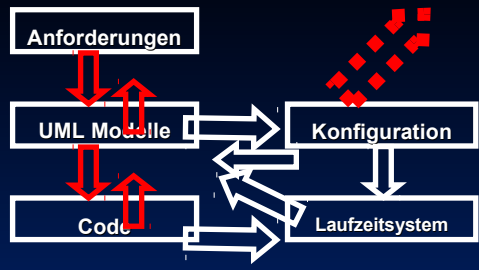
Idee:

- UML für System-Modellierung. [FASE 01, UML 02]
- Sicherheitsinform. als Markierungen (Stereotypen) einfügen. Definiere dazu UML-Erweiterung UMLsec.
- Formale Semantik mit stromverarbeitenden Funktionen als Grundlage für Verifikation.



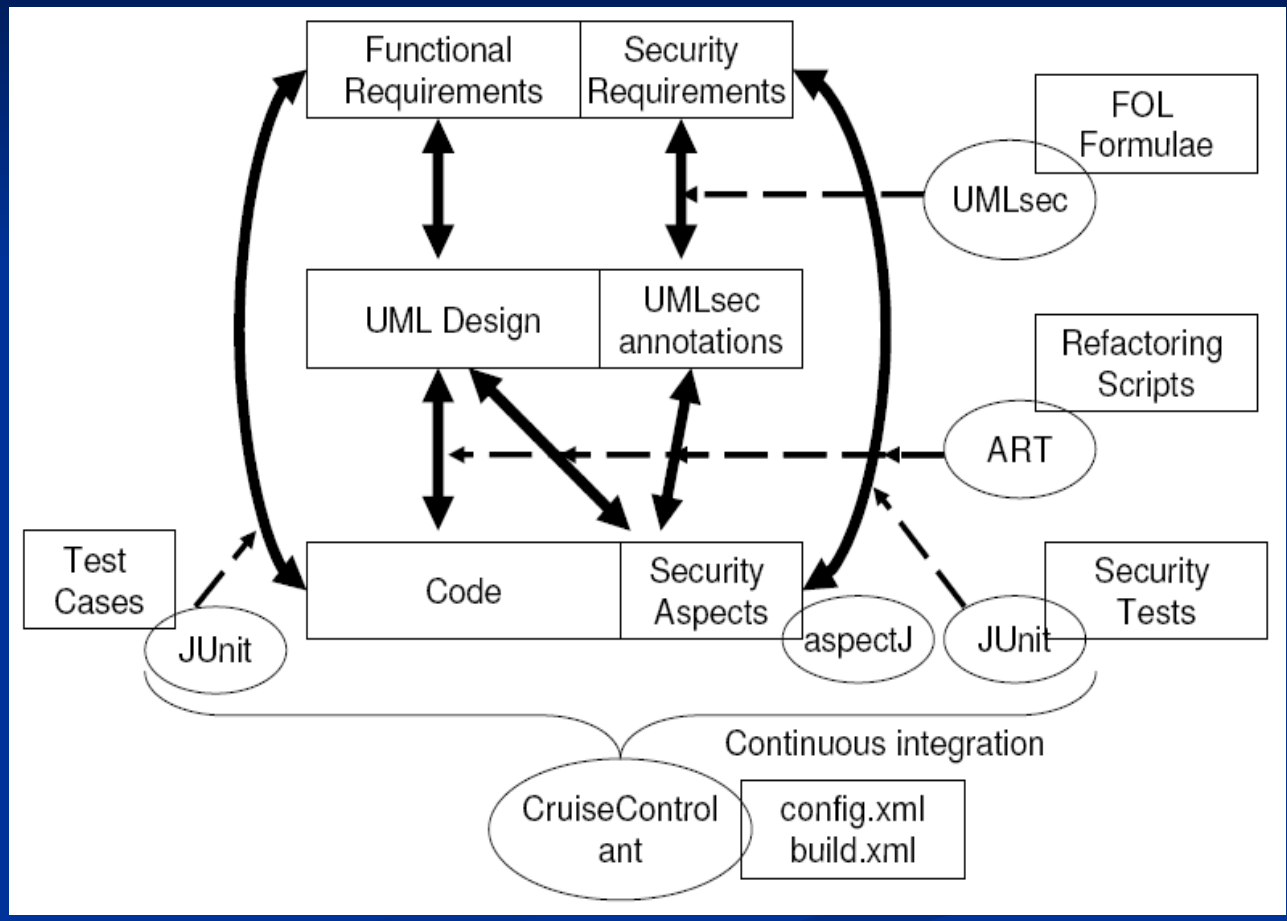
[Jour. Logic & Algebr. Program. '08]

Sichere Evolution: Werkzeugunterstützung



Nachverfolgbarkeit von Anforderungen vs. Implementierung bei Evolution durch Refactoring bewahren.

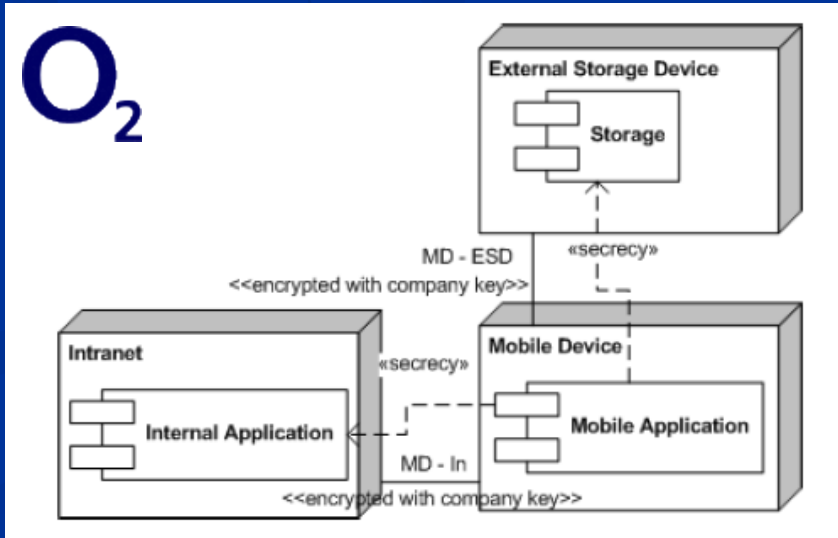
[ASE'07, ICSM'08, ASE'08, Computer Journal '10]



Mobile Informationssysteme bei O_2

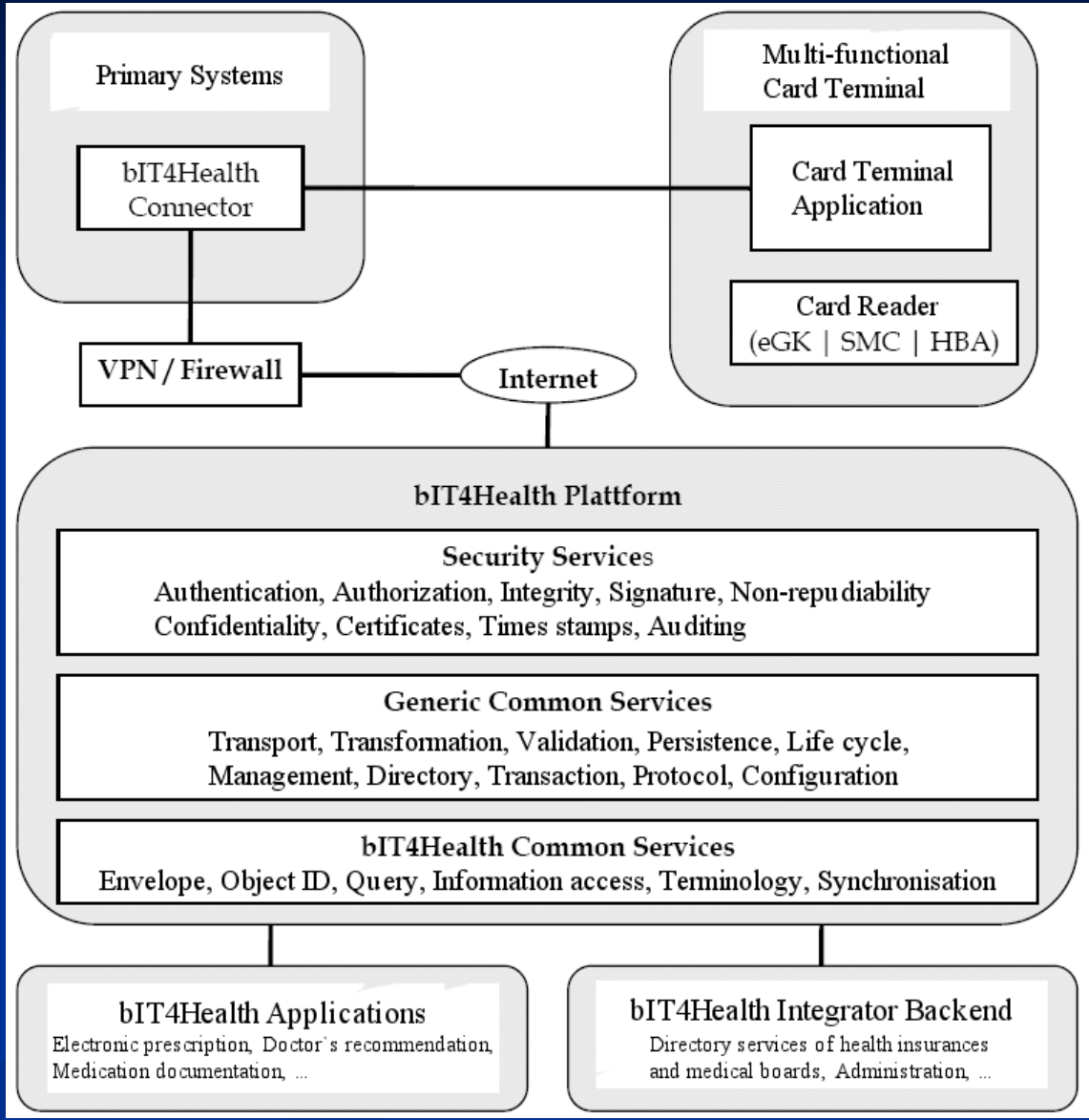
[ICSE 08]

- Anwendung von UMLsec auf mobile Kommunikations-Architekturen bei O_2 (Germany)
- Alle 62 Sicherheitsanforderungen aus der Security Policy erfolgreich verifiziert.
- Modellbasierte Techniken bringen Zusatzaufwand.
- Macht sich bezahlt bei wichtigen Sicherheitsanforder-ungen und Konzentration auf kritische Architekturanteile (auch im Vergleich mit anderen QS Ansätzen mit vergleichbarer Verlässlichkeit)
- UMLsec adäquat für mobile Architekturen.



Informationssysteme im Gesundheitsbereich: Die Gesundheitskarte

- Architektur mit UMLsec analysiert
- Einige Schwachstellen aufgedeckt (fehlender Vertraulichkeits-schutz für digitale Rezepte)



[Meth. Inform. Medicine 08]

Bank-Informationssystem bei der HVB

Modellbasierte Sicherheitsanalyse von webbasierter Bankanwendung (“digitaler Formularschrank”).

Geschichtete Architektur (SSL Protokoll, darauf Client Authentisierungs-Protokoll)

Anforderungen:

- Vertraulichkeit
- Authentisierung

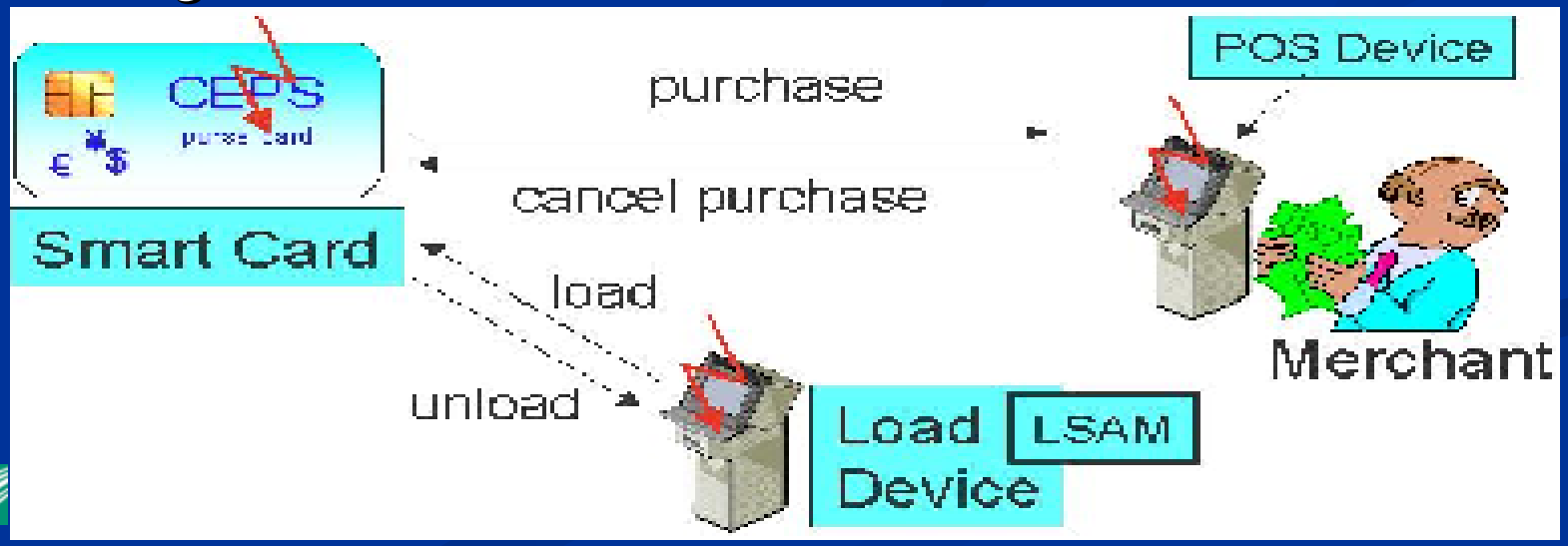
[IFIPSEC 01, ASE 01]

Mobiles Bezahlsystem

Common Electronic Purse Specifications:
Globaler Standard für eGeldbörsen (Visa et al.).

Smartcard enthält Kontostand, sichert Transaktionen mithilfe Krypto.

Formale Analyse von Load und Purchase Protokollen: signifikante Schwachstellen: Kauf-Umleitung, Betrug Ladegerätbetreiber vs. Bank.



[ACSAC 05]

Biometrische Authentisierung

Smartcard basiertes System.

Analysiert mit UMLsec parallel zur Entwicklung durch Firma in gemeinsamem Projekt.

Entdeckten drei signifikante Schwachstellen in verschiedenen Versionen (Fehlbedienungszähler umgangen durch Löschen / Wiederholen von Nachrichten; Smartcard unzureichend authentisiert durch Mischen von Sitzungen).

Endgültig entwickelte Version sicher.