Willkommen zur Vorlesung

Modellbasierte Softwaretechniken für sichere Systeme

im Sommersemester 2012

Prof. Dr. Jan Jürjens

TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

Vorlesungswebseite (bitte notieren):

http://www-jj.cs.tu-dortmund.de/secse/pages/teaching/ss12/mbse/index_de.shtml

0. Organisatorisches und Einleitung

Agenda

- Organisatorisches
- Vorstellung des Fachgebietes
- Vorlesungsinhalte

Organisatorisches – Agenda

- Studienordnung
  - Einordnung / Kompetenzen / Struktur / Prüfung
- Vorlesung
  - Bildungsvertrag, Termine, Feedback
- Übung
  - Konzept / Termine
- Prüfung

- Diplom
  - Schwerpunkte 1
  - Schwerpunkt 5
- Master Informatik / Angewandte Informatik
  - Basismodul
  - Forschungsbereich Software, Sicherheit und Verifikation

Modulkatalog Master-Studiengänge Informatik
Modul INF-MSc-420: Modellbasierte Softwaretechniken für sichere Systeme
MA-Studiengänge: Informatik, Angewandte Informatik
Turnus: Jedes WS. Dauer: 1 Sem.. Studienabs.: 2.-3. Sem., Credits: 6, Aufwand: 180 h (60/120)
Modulstruktur:

Nr.	Element / Lehrveranstaltung	Typ	Credits	SWS
1	Modellbasierte Softwaretechniken für sichere Systeme	V	3	2
1	Übungen zu Modellbasierte Softwaretechniken für sichere Systeme	Ü	3	2

Lehrveranstaltungssprache: Deutsch und/oder Englisch
Prüfungen

- Modulprüfung: Klausur oder mündliche Prüfung
- Studienleistungen: 50% der Aufgabenpunktzahl, aktive Teilnahme an Uebungen (beides Voraussetzung fuer die Zulassung zur Pruefung), Pruefung.
- Prüfungsformen und -leistungen: Modulprüfung

7 Teilnahmevoraussetzungen

- Basismodul aus dem Forschungsbereich A (Software, Sicherheit und Verifikation)

Modultyp und Verwendbarkeit des Moduls

- Vertiefungsmodul in den Masterstudiengängen Informatik und Angewandte Informatik
- Forschungsbereich: Software, Sicherheit und Verifikation

Erlangbare Kompetenzen innerhalb der Vorlesung:

Die Studierenden sollen über die grundlegenden Fähigkeiten zur Einschätzung von Methoden und theoretischen Ansätzen für die modell-basierte Entwicklung sicherer Softwaresysteme (im Sinne von IT Security) verfügen. Sie können geeignete methodische Zugriffe und theoretische Ansätze zur Spezifikation und zum modell-basierten Entwurf von sicherheitskritischer Software auswählen und bei der Bearbeitung des Untersuchungsgegenstands empirisch und konzeptionell erproben.

- 4 SWS:
  - 2 SWS Verlesung
  - 2 SWS Übung
- 6 Credits
  - 3 Credits Vorlesung
  - 3 Credits Übung
- Aufwand 180 Stunden
  - 60 Stunden Vorlesung
  - 120 Stunden Übung
- Veranstaltungssprache Deutsch, Folien z.T. Englisch

Bildungsvertrag
Wir bieten ...

- Fachliche Einführung in Modellbasierte Softwaretechniken für sichere Systeme
- Engagierte Betreuung
  - Interessante Vorlesung
  - Regelmäßige Sprechstunden (Termin s. Homepage)
  - Betreute Übungen
  - Korrigierte Hausübungen
  - Transparente Anforderungen
  - Möglichkeiten zum direkten Feedback
- Möglichkeit zum Erwerb des Scheins

Bildungsvertrag
Wir erwarten ...

- Aktives Auseinandersetzen mit den Vorlesungsinhalten
  - Aktive Teilnahme an der Vorlesung
  - Vor- und Nachbereitung der Vorlesung
  - Aktive Teilnahme an den Übungen
  - Bearbeitung der Hausübungen

- Termin:
  - Di. 16:15 bis 18:00 Otto-Hahn-Str. 14 – E02

- Aktuelle Informationen zur Vorlesung:

(Bitte regelmäßig beachten wegen möglicher Vorlesungs-ausfälle o.ä..)

http://www-jj.cs.tu-dortmund.de/secse/pages/teaching/ss12/mbse/index_de.shtml

Wir haben besonderes Interesse an vorlesungsbegleitendem Feedback, um etwaige Verbesserungsvorschläge ggf. schon während des Semesters zu berücksichtigen.

Übliche Kontaktmöglichkeiten:

- Nach der Vorlesung
- E-mail jan.jurjens@cs.tu-dortmund.de
- Tel.: 0231 755-7208
- Sprechstunde: Montags 10.00-11.00 Uhr (am Fraunhofer ISST; bitte vorher per email anmelden)
- Anonymes Kontaktformular: Link von Vorlesungswebseite

Darüberhinaus (unregelmäßig):

- „1 Minute – 2 Questions“

- Termine:
  - Mi. 16:00 bis 18:00, OH-14, Raum 304
  - 1. Übung am 11.04.2012
- Abgabe im Briefkasten 5 in der OH20 jeweils bis folgenden Montag. Übungsblätter auf der Homepage.
- Scheinkriterium: 50% Aufgabenpunktzahl, aktive Teilnahme an Übungen
- Kontakt
  - Bei Fragen zu den Übungen und ihrer Durchführung: Christian Wessel: http://www-jj.cs.tu-dortmund.de/secse/pages/people/wessel

Inpud-Forum

- Ziel: Diskussion der Studierenden untereinander
- Keine Kommunikation mit den Veranstaltern dort
  - Keine garantierten Antwortzeiten
  - Für dringendes: Mail oder Sprechstunde nutzen
- Organisatorische + inhaltliche FAQ
  - Für Fragen von Studierenden, die auch für andere interessant sein könnten
- Moderation durch die Veranstalter

- Prüfung
  - mündlich
  - Einzelheiten, Termine etc. später

Diplom

- Für Studierende nach den Prüfungsordnungen 2000/2001:
  - Studierende können zu dieser Lehrveranstaltung einen Leistungsnachweis erwerben oder eine Fachprüfung ablegen.
  - Leistungsnachweise über den erfolgreichen Besuch von Vorlesung und Übungen werden erteilt, sofern die Studierenden die von den Veranstaltern festgelegten Kriterien für eine erfolgreiche Bearbeitung der Übungsaufgaben erfüllen.
  - Eine Fachprüfung kann in Form einer mündlichen Prüfung am Ende des Semesters abgelegt werden.
  - Die Bearbeitung der Übungsaufgaben bereitet auf die Teilnahme an der Fachprüfung vor.

Master Informatik / Angewandte Informatik:

- Die Prüfungsleistung wird anhand der Modulprüfung in Form einer mündlichen Prüfung ermittelt.
- Die Studienleistung (= erfolgreiche Bearbeitung der Übungsaufgaben) ist Voraussetzung für die Teilnahme an der Modulprüfung.

Kontakt

- Jan Jürjens:
  - http://jan.jurjens.de
- Christian Wessel:
  - http://www-jj.cs.tu-dortmund.de/secse/pages/people/wessel
- Vorlesungsseite (bitte regelmäßig beachten wegen möglicher Vorlesungsausfälle o.ä..)
  http://www-jj.cs.tu-dortmund.de/secse/pages/teaching/ss12/mbse/index_de.shtml
- Inpud-Forum:
  - http://inpud.cs.uni-dortmund.de
- Übungsanmeldung
  - http://ess.cs.uni-dortmund.de/ASSESS

Vorstellung des Fachgebietes

- Lehrangebot
- Forschung
- Abschlussarbeiten und Hiwi-Jobs

Wer bin ich?

- Professor für Software Engineering an der TU Dortmund
- Wissenschaftskoordinator „Enterprise Engineering“ am Fraunhofer ISST
- Leiter der Fraunhofer-Attract-Projektgruppe „Architectures for Auditable Business Process Execution (Apex)“

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 an Univ. Bremen und Univ. Cambridge

Wer ist meine Forschungsgruppe?

- Misha Aizatulin (Microsoft Research Cambridge)
- H. Selcuk Beyhan (Logica (Germany))
- Francois Dupressoir (Microsoft Research Cambridge)
- Michael Giddings (Open University)
- Thorsten Humberg (Fraunhofer ISST)
- Christopher McLaughlin (Gartner)
- Martin Ochoa (TUD / Siemens)
- Sebastian Pape (TUD)
- Dr. Thomas Ruhroth (TUD)
- Andreas Schmitz (Fraunhofer ISST)
- Stefan Taubenberger (Münchener Rückversicherung)
- Daniel Warzecha (Fraunhofer ISST)
- Dr. Sven Wenzel (TUD)
- Christian Wessel (TUD)

Beispiel-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

Abschlussarbeiten

Abschlussarbeiten 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 Clouds / ClouDAT: Cloud-Software-Anbieter (LinogistiX), IT-Berater (Admeritia, ITESYS, TÜV-IT)

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

Hiwi-Tätigkeiten

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

- Unterstützung der folgenden Projekte (bespielsweise durch Java-Programmierung eines UML-Analyse Werkzeuges oder konzeptuelle Arbeiten im Bereich modell-basierte Sicherheitsanalyse):
  "Architectures for Auditable Business Process Execution (APEX)", SecureClouds, Seconomics, SecVolution, ProceSec, ClouDAT
- Unterstützung in der Lehre (Tutorien, Folienerstellung etc)

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

Weitere relevante Lehrveranstaltungen

Dieses Semester:

- Seminar „Ausgewählte Themen des Modell-basierten Sicherheits-Engineerings“.
  Bei Interesse bitte bei mir melden.
  (Vorbesprechung am 05. Apr., 10-11 Uhr, OH14/105)
- Master-Basismodul “Methodische Grundlagen des Software-Engineering” (4+2 SWS)

Zuordnung der Wahlveranstaltungen zu Schwerpunktgebieten (Diplom):

- Sicherheit und Verifikation
- Software-Konstruktion

Forschungsbereich Master: Software, Sicherheit und Verifikation

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

Auslandaufenthalte

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

- EU-Projekt Seconomics: Unis Trento (I), Aberdeen (UK), Madrid (S), Anadolu (TR); Firmen Atos Origin (F), National Grid (UK), Deep Blue (I), Barcelona Transport (S).

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.“

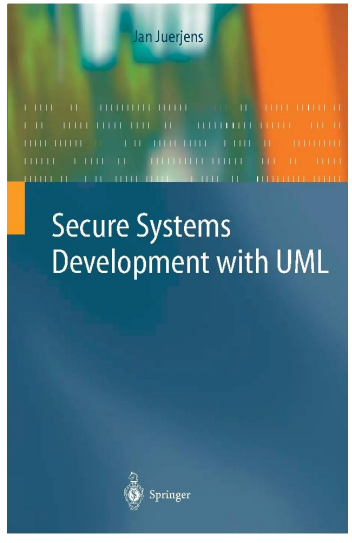
Und: Promotion projekt-begleitend möglich.

Kontakt: http://jan.jurjens.de

Einführung in Modell-basiertes Sicherheits-Engineering

- Überblick IT-Security: Was ist zu schützen ? Was sind die Angriffe ?
- Sicherheitsrelevante Workflows / Geschäftsprozesse, Bedrohungsanalysen
- Überblick IT-Sicherheitsmaßnahmen, Daten- und Dokumentensicherheit (z.B. Digitale Signatur)
- IT-Zugangsschutz, Netzwerksicherheit
- Modell-basierte Entwicklung mit UML
- Werkzeuge
- Industrielle Anwendungen (Biometrie, Smart-cards, …)

- Die in dieser Vorlesung betrachteten Architekturen werden mit der Sicherheitserweiterung UMLsec der Unified Modeling Language (UML) modelliert und auf ihre Sicherheitseigenschaften analysiert.
- Hintergrundliteratur:
  - Jan Jürjens, Secure Systems Development with UML, Springer-Verlag 2005, s. http://umlsec.de
  - TUD-Bibliothek:
    Signaturen L Sr 531 bis L Sr 531+4
- Allgemeiner Hintergrund:
  - Anderson: Security Engineering (2001)
    [UB-Inf: 3378/Ande, 3384/Ande]



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 gestiegenen Erwartungen bei gleichzeitig steigender Systemkomplexität nicht mithalten konnten.

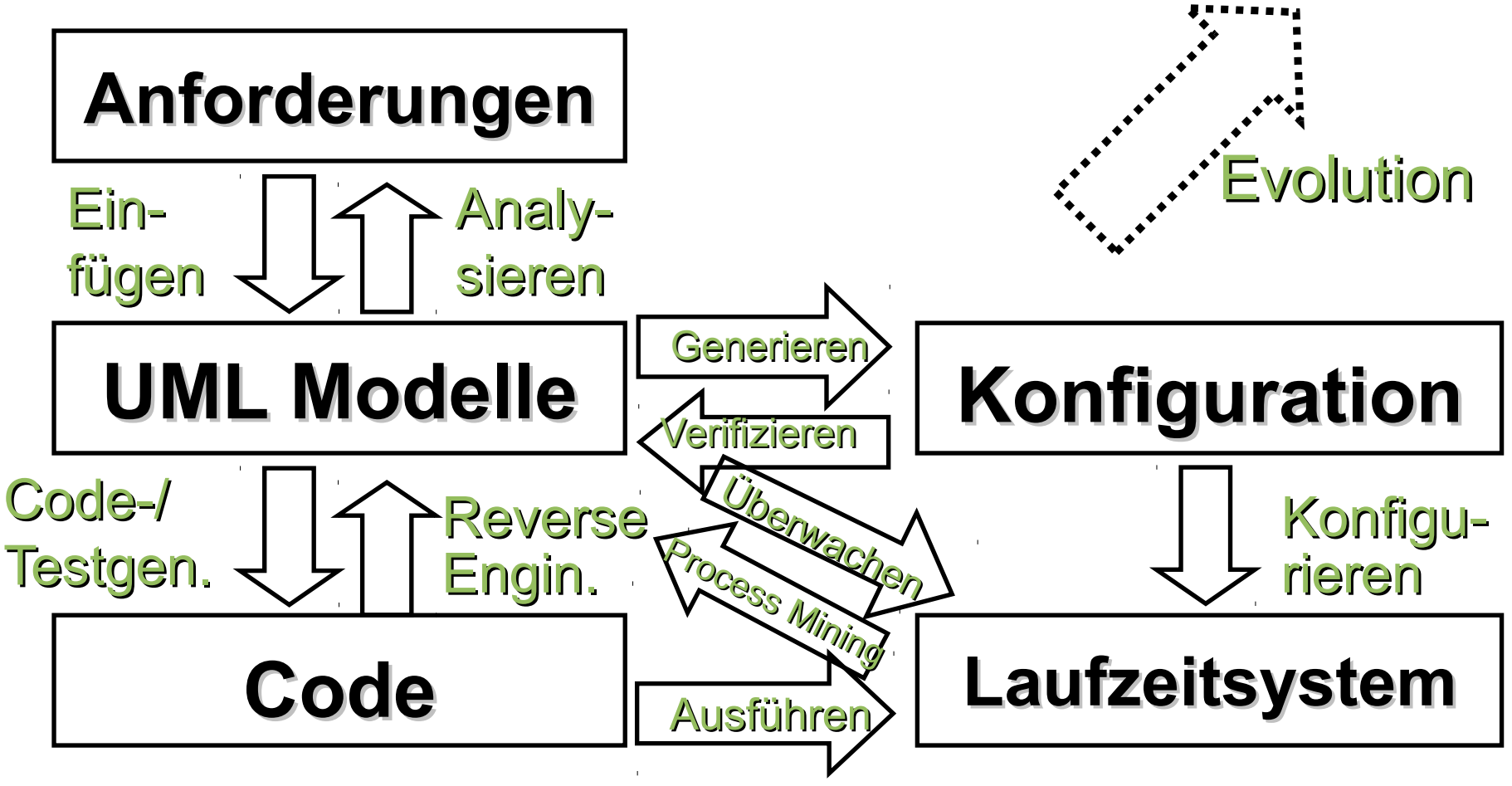
Offene Systeme

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

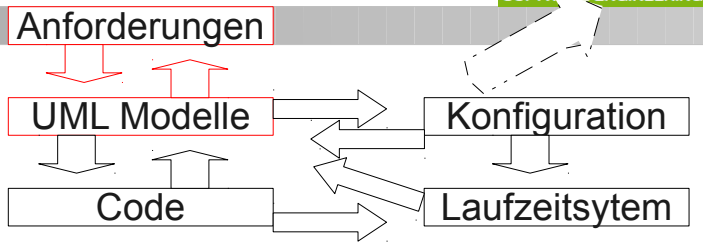
- Internet
- Mobile Netze

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

Modellbasierte Entwicklung



Modellierung mit UMLsec

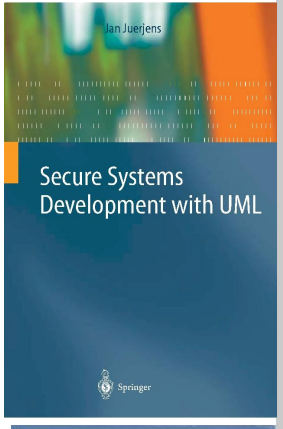


Ziel:

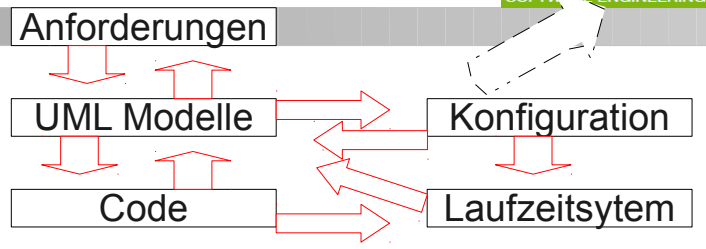
- Dokumentation und automatische Analyse von sicherheits-relevanten Informationen (z.B. Sicherheits-Eigenschaften und -Anforderungen) als Teil der Systemspezifikation.

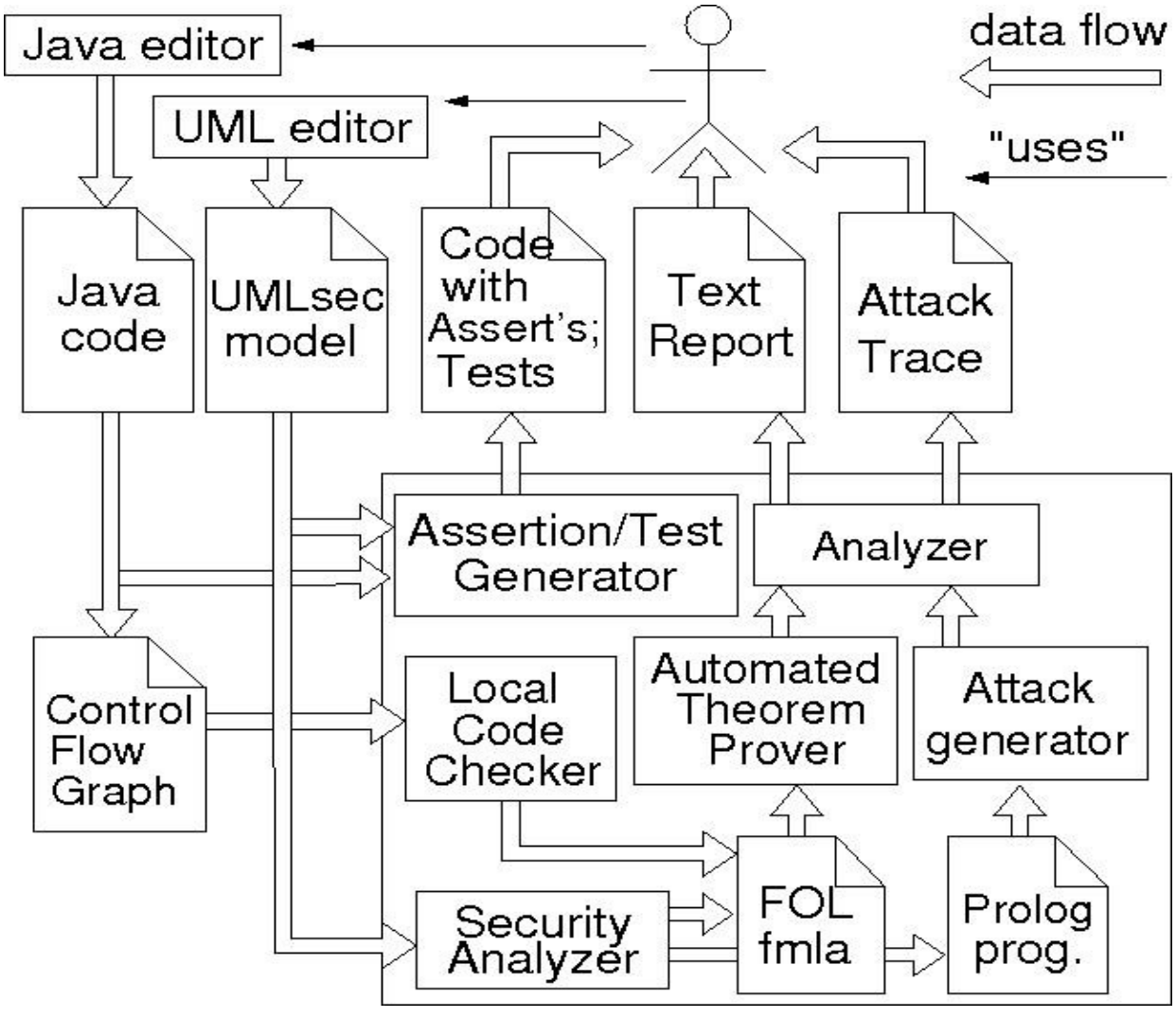
Idee:

- UML für System-Modellierung.
- Sicherheitsrelevante Informationen als Markierungen (Stereotypen) einfügen. Definiere dazu UML-Erweiterung UMLsec.
- Formale Semantik mit stromverarbeitenden Funktionen als Grundlage für Verifikation.

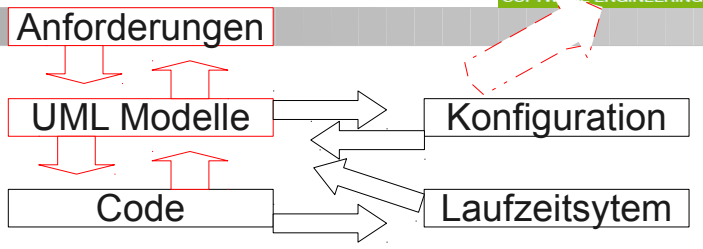


Werkzeugunterstützung

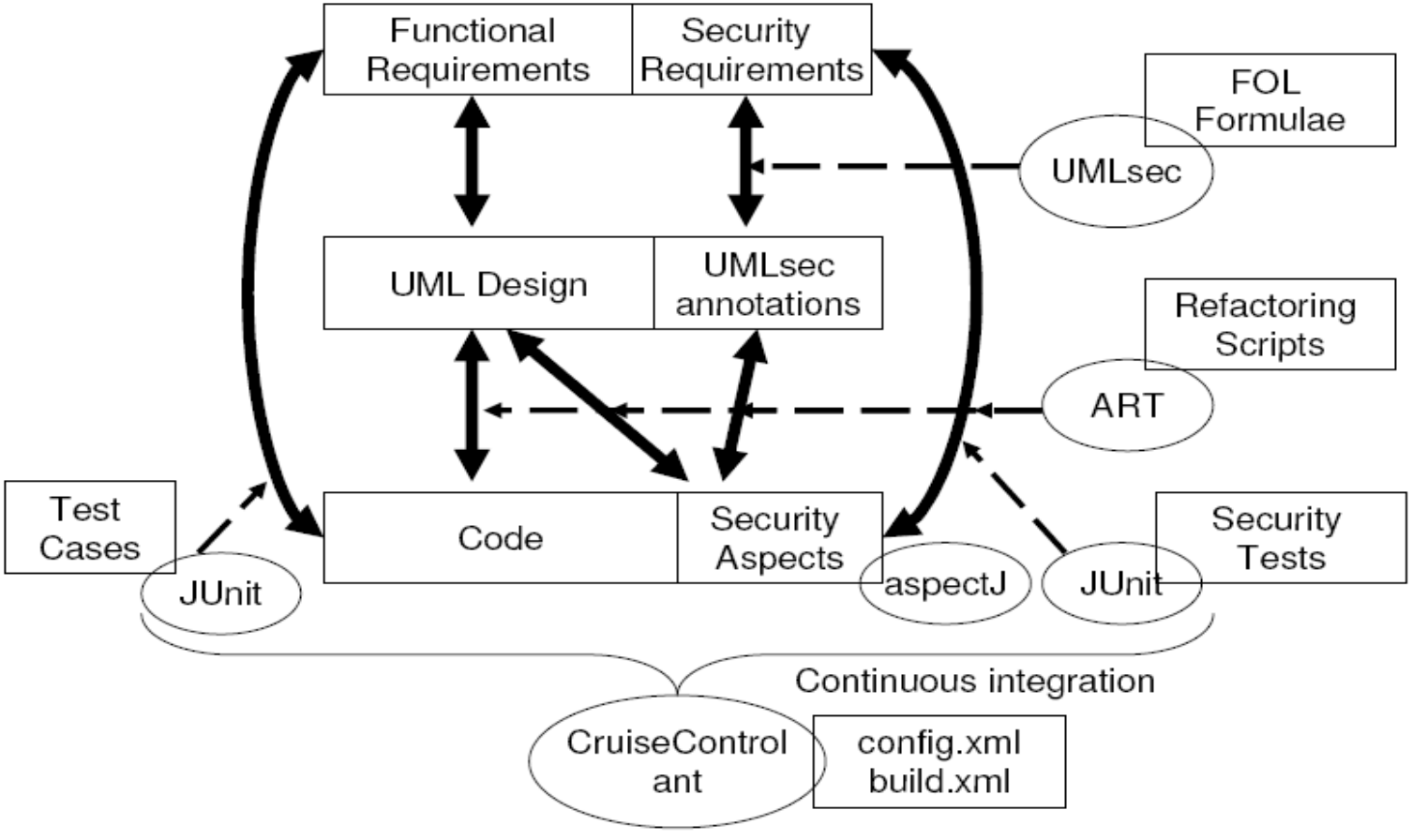




Werkzeugunterstützung: Sichere Evolution:



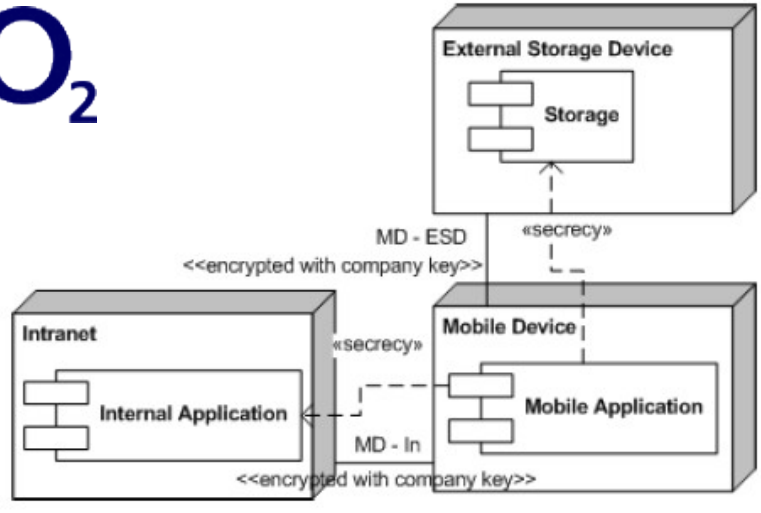
Nachverfolgbarkeit von Anforderungen vs. Implementierung bei Evolution durch Refactoring bewahren.



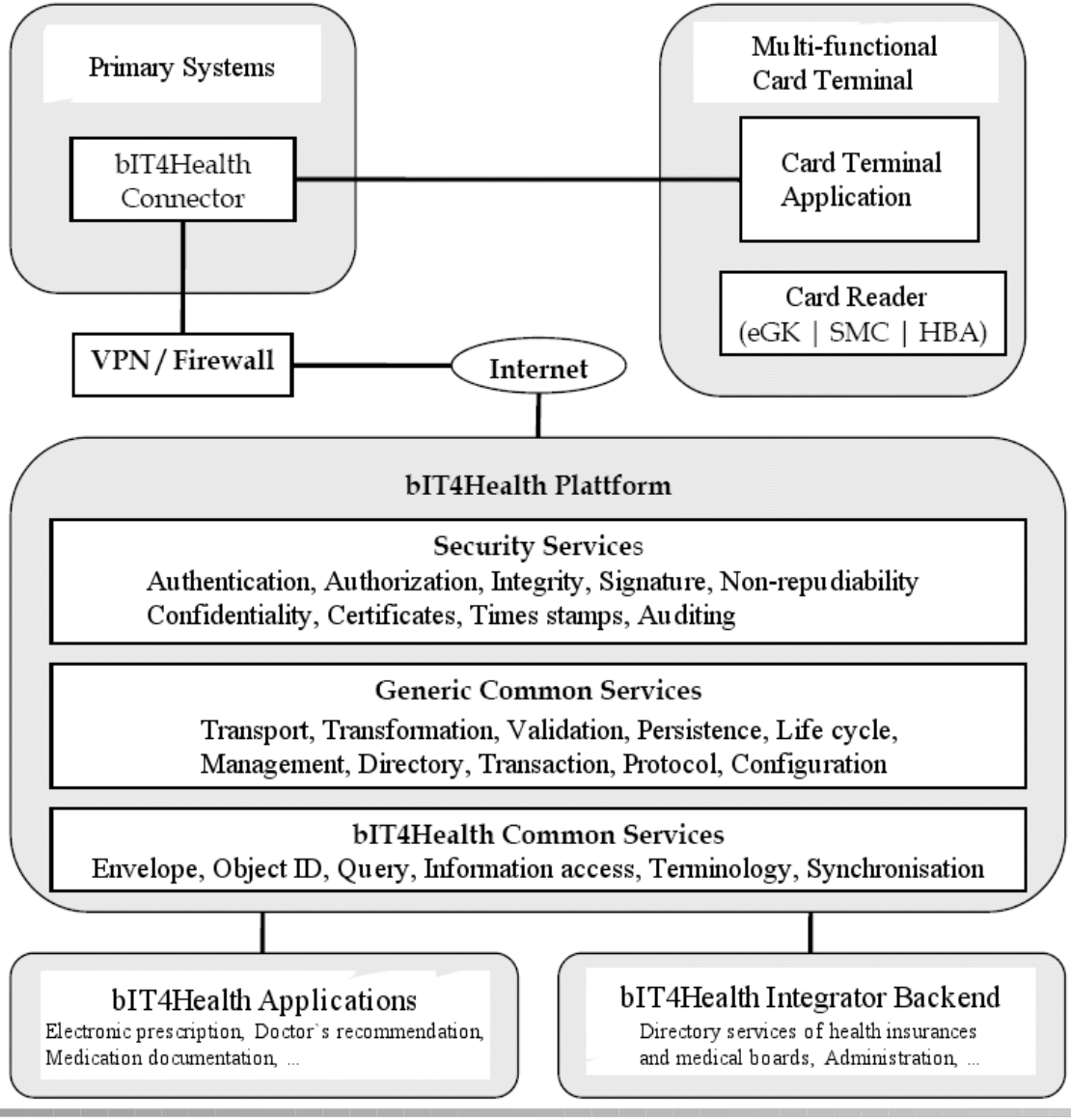
Mobile Informationssysteme bei O_2

- 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 Sicherheitsanforderungen und Konzentration auf kritische Architekturanteile (auch im Vergleich mit anderen Qualitätssicherungs-Ansätzen mit vergleichbarer Verlässlichkeit)
- UMLsec adäquat für mobile Architekturen.

O_2



- Architektur mit UMLsec analysiert.
- Einige Schwachstellen aufgedeckt (fehlender Vertraulichkeitsschutz für digitale Rezepte).



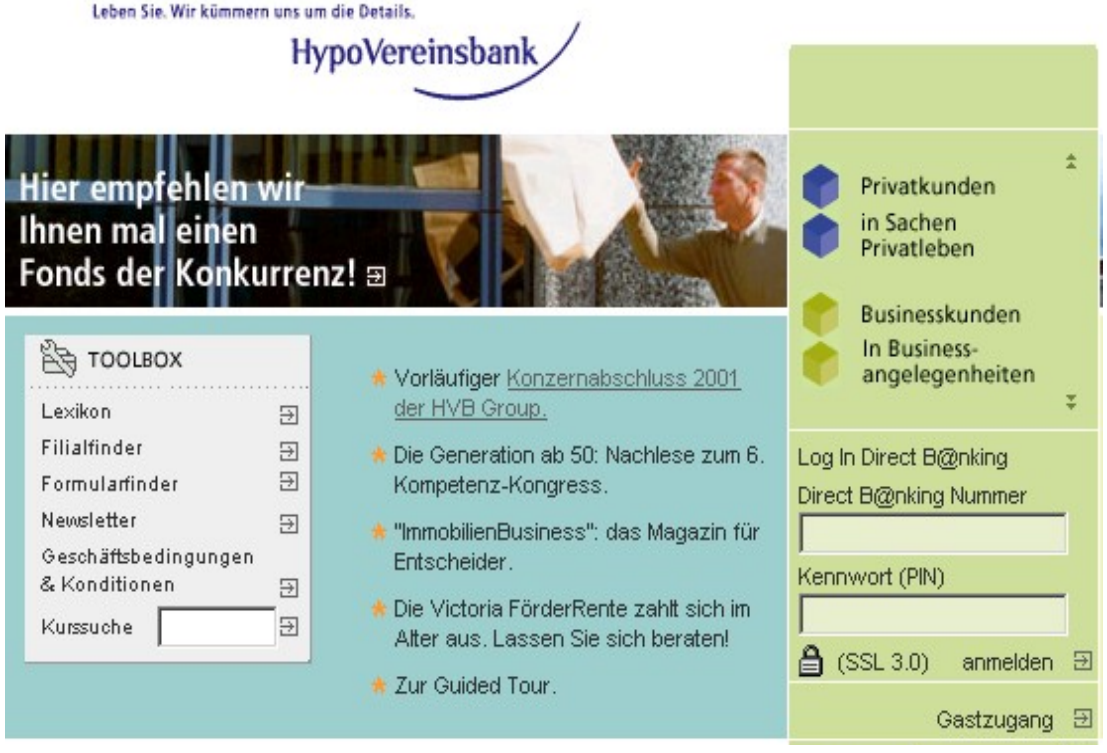
Bank-Informationssystem bei der HypoVereinsbank

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

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

Anforderungen:

- Vertraulichkeit
- Authentisierung

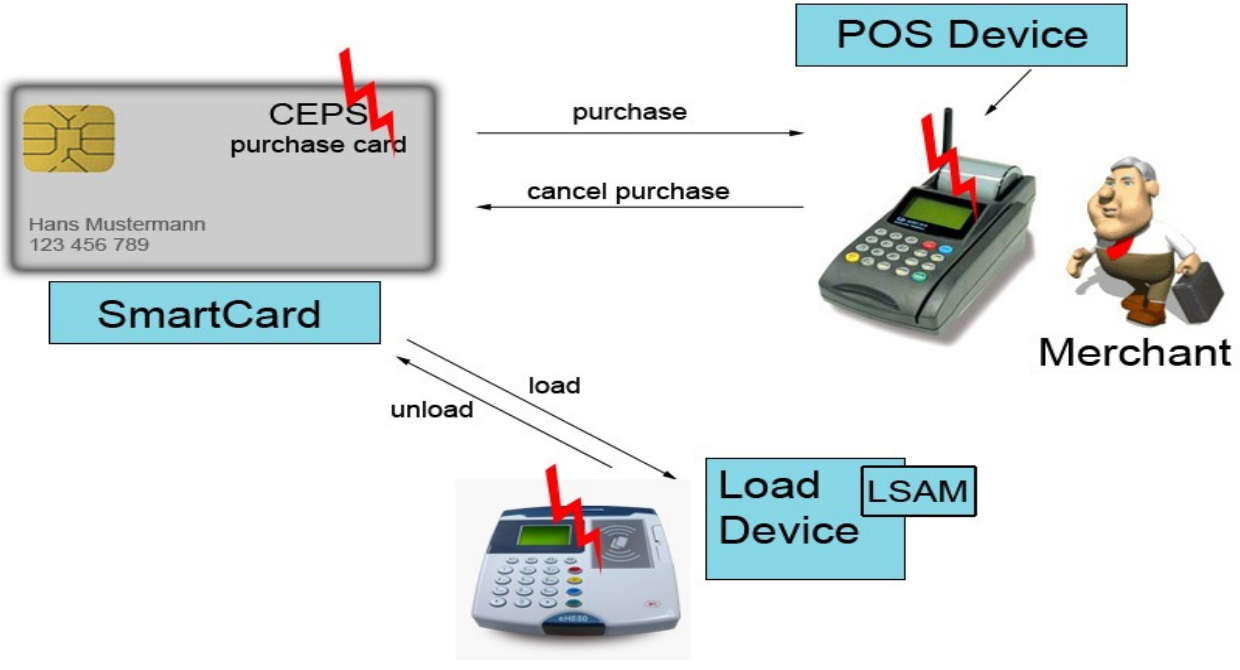


Mobiles Bezahlsystem

Common Electronic Purse Specifications:
Globaler Standard für e-Geldbörsen (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.



Biometrische Authentisierung

Smartcard basiertes System.

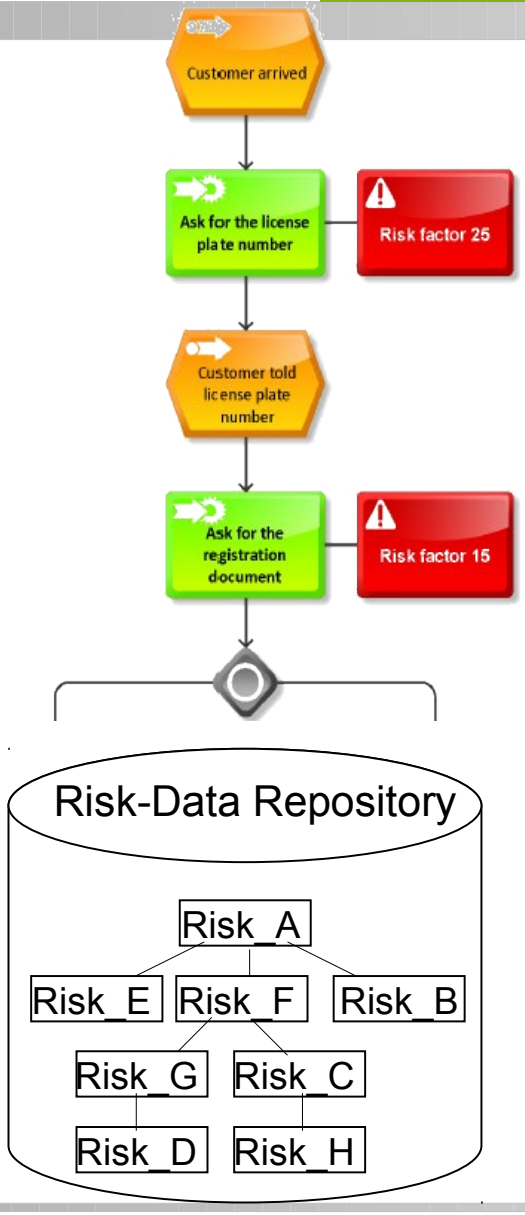
Analysiert mit UMLsec parallel zur Entwicklung durch Firma in gemeinsamem Projekt.

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.

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,
- automatische Risiko-Identifikation und -Bewertung
- Laufendes Projekt (Fraunhofer Attract): Architekturen für auditierbare Geschäftsprozessausführung (Apex).



Internes Informationssystem bei BMW

BMW Group

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

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.