Frühzeitige modellbasierte Risikoanalyse für mobile, verteilte Anwendungen

Wessel et al.

Einleitung

Bestehende Ansätze

Unsere Idee

Offene Fragen und Diskussion

Frühzeitige modellbasierte Risikoanalyse für mobile, verteilte Anwendungen

Christian Wessel, Thorsten Humberg,
Sven Wenzel, Jan Jürjens

28.02.2012

Gliederung des Vortrags

Frühzeitige modellbasierte Risikoanalyse für mobile, verteilte Anwendungen

Wessel et al.

Einleitung

Bestehende Ansätze

Unsere Idee

Offene Fragen und Diskussion

Einleitung

Bestehende Ansätze

Unsere Idee

Offene Fragen und Diskussion

Modellbasierte Entwicklung

Frühzeitige modellbasierte Risikoanalyse für mobile, verteilte Anwendungen

Wessel et al.

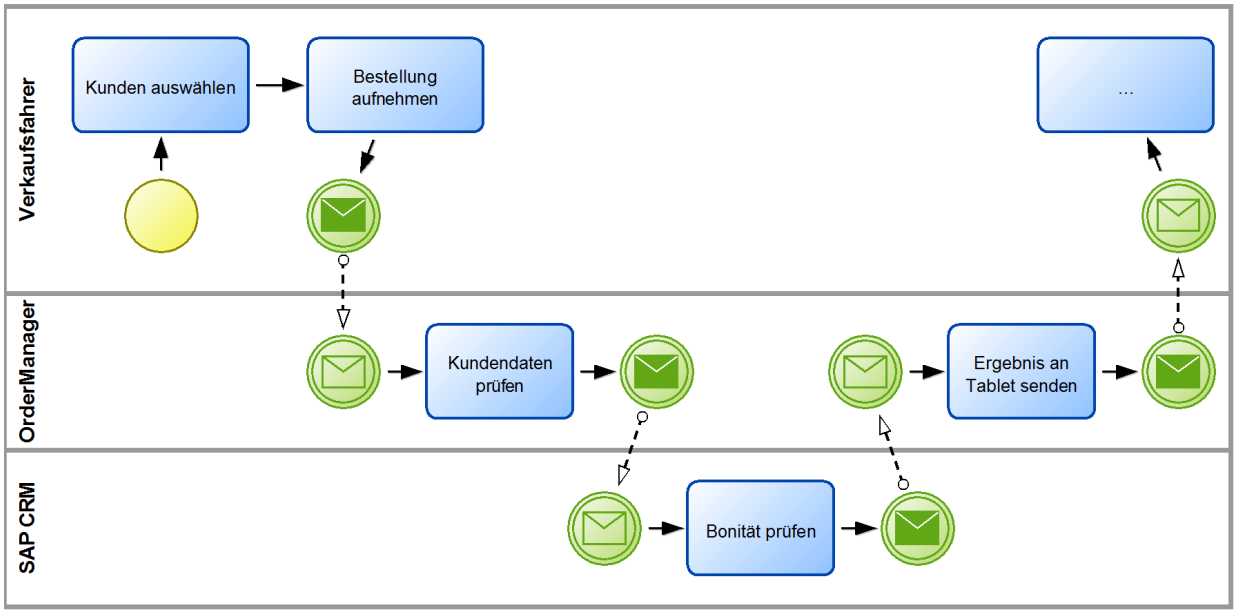
Einleitung

Bestehende Ansätze

Unsere Idee

Offene Fragen und Diskussion

- Bessere Unterstützung komplexer Systeme durch höhere Abstraktion
- Möglichkeit der automatischen Prüfung
- Automatische Codegenerierung



Mobile, verteilte Geschäftsprozesse

Frühzeitige modellbasierte Risikoanalyse für mobile, verteilte Anwendungen

Wessel et al.

Einleitung

Bestehende Ansätze

Unsere Idee

Offene Fragen und Diskussion

- Geschäftsprozesse sind nicht mehr nur auf Büroanwendungen beschränkt
- Auch Außendienstmitarbeiter einbezogen durch Nutzung mobiler Endgeräte

Mobile Geräte:

- Stark verbesserte Leistungsfähigkeit
- Immer mehr Einsatzmöglichkeiten

Aber:

- Abhörsicherheit nicht immer gegeben
- Verlust von mobilen Geräten
- Kritisch z.B. bei der Verarbeitung personenbezogener Daten
- Möglicher Verlust von Firmendaten

Bestehende Ansätze

Frühzeitige modellbasierte Risikoanalyse für mobile, verteilte Anwendungen

Wessel et al.

Einleitung

Bestehende Ansätze

Unsere Idee

Offene Fragen und Diskussion

Sicherheitsanforderungen in BPMN-Diagrammen annotieren

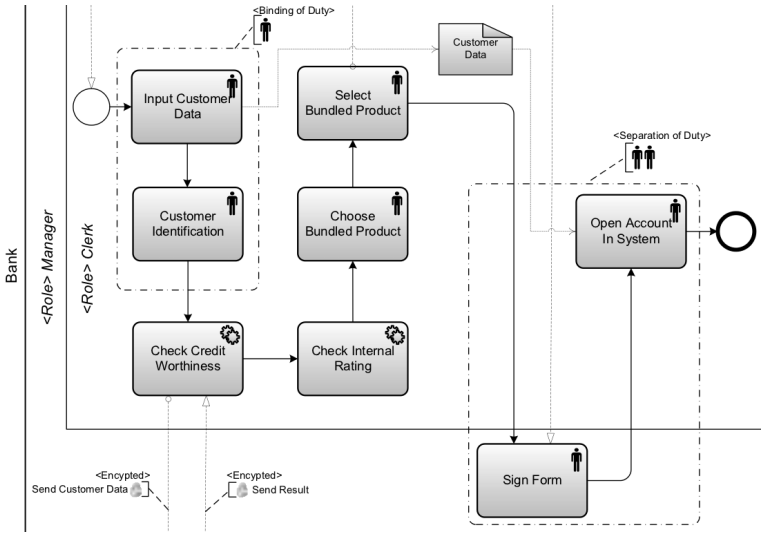


Abbildung: Wolter et al.

[Wol08]

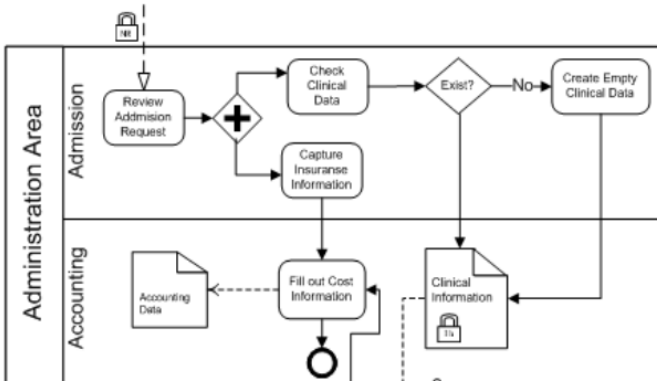


Abbildung: Rodriguez et al.

[Rod07]

Fokus dieser Ansätze liegt auf der Modellierung

Bestehende Ansätze

Frühzeitige modellbasierte Risikoanalyse für mobile, verteilte Anwendungen

Wessel et al.

Einleitung

Bestehende Ansätze

Unsere Idee

Offene Fragen und Diskussion

- UMLsec
  - Erweiterung des UML-Standards
  - Ermöglicht die Modellierung sicherheitskritischer Systeme
  - Beispiel: <<secure links>>

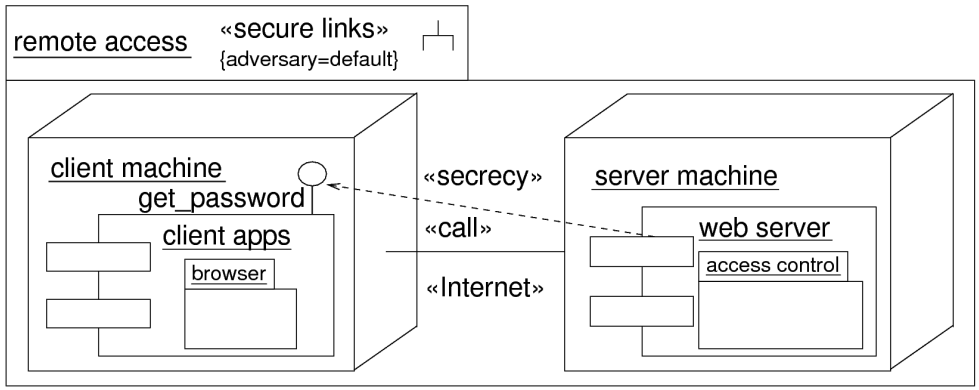


Abbildung: Jürjens

[Jür04]

Unsere Idee

Frühzeitige modellbasierte Risikoanalyse für mobile, verteilte Anwendungen

Wessel et al.

Einleitung

Bestehende Ansätze

Unsere Idee

Offene Fragen und Diskussion

- Sicherheit bereits in frühen Planungsphasen berücksichtigen
- Modellgetriebener Ansatz
- Kombinieren von Deployment und BPMN-Diagrammen führt zu Erkenntnisgewinn
- Automatische Prüfung auf Sicherheitslücken

Beispiel

Frühzeitige modellbasierte Risikoanalyse für mobile, verteilte Anwendungen

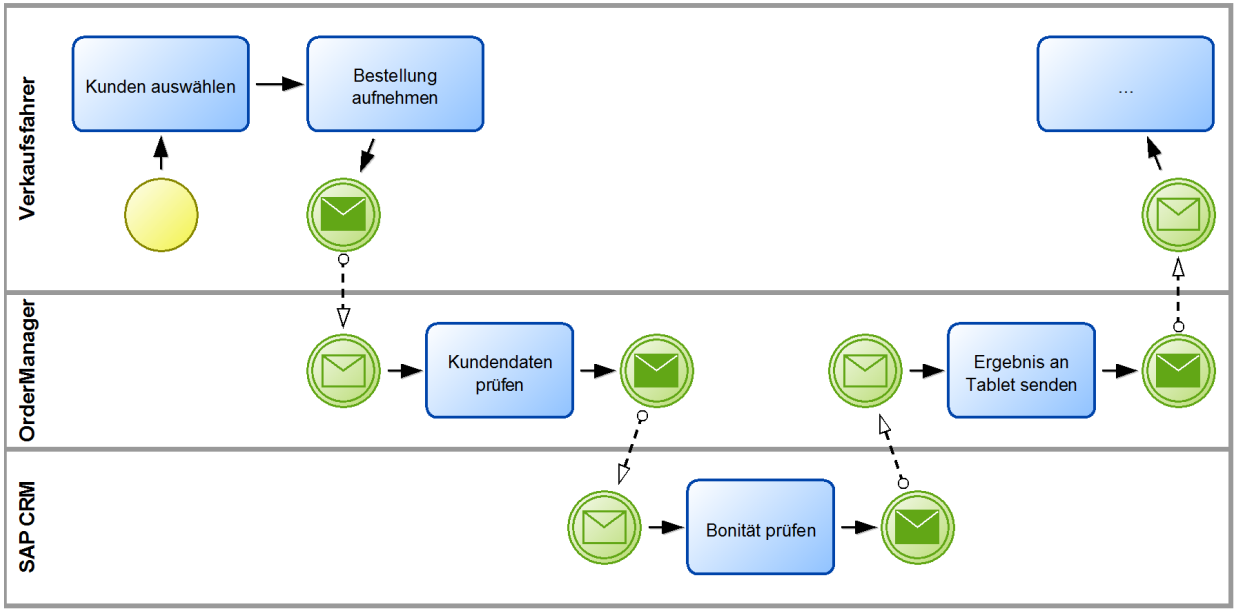
Wessel et al.

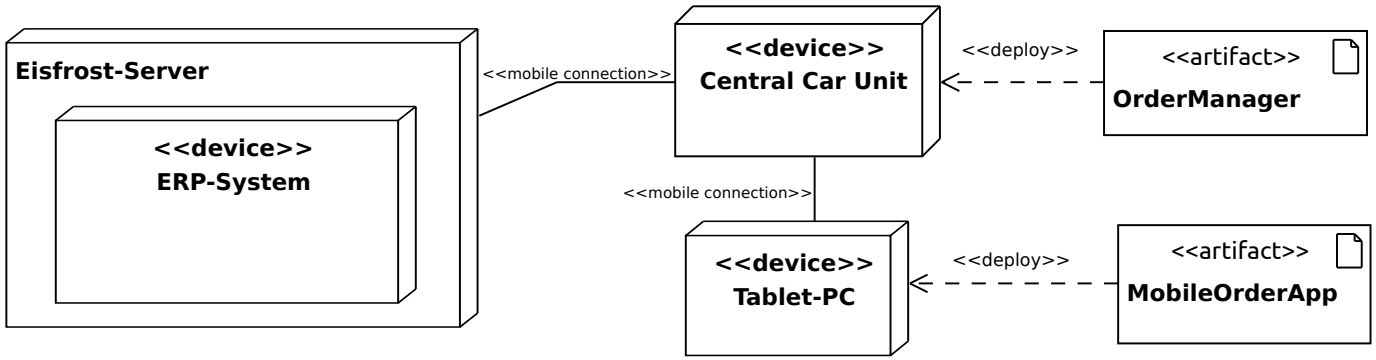
Einleitung

Bestehende Ansätze

Unsere Idee

Offene Fragen und Diskussion





Analyse in drei Schritten

Frühzeitige modellbasierte Risikoanalyse für mobile, verteilte Anwendungen

Wessel et al.

Einleitung

Bestehende Ansätze

Unsere Idee

Offene Fragen und Diskussion

1. Untersuchung der Verteilung
2. Untersuchung der Kommunikation
3. Analyse der Risiken

Untersuchung der Verteilung

Frühzeitige modellbasierte Risikoanalyse für mobile, verteilte Anwendungen

Wessel et al.

Einleitung

Bestehende Ansätze

Unsere Idee

Offene Fragen und Diskussion

- Betrachtung der Verteilung von Komponenten auf konkrete Systeme
- Trennung zwischen mobilen und stationären Systemen
  - Schutzbedarf unterschiedlich
- Zuordnung von BPMN-Akteuren auf Deployment-Komponenten
- Ermöglicht Kombinierte Sicht von Geschäftsprozess und Deployment
- Ziel: Identifizierung der Schutzbedarfe der beteiligten Komponenten

Geschäftsprozess	**Verteilungsdiagramm**
SAP CRM	Eisfrost-Server/ERP-System
OrderManager	OrderManager
Verkaufsfahrer	MobileOrderApp

Untersuchung der Kommunikation

Frühzeitige modellbasierte Risikoanalyse für mobile, verteilte Anwendungen

Wessel et al.

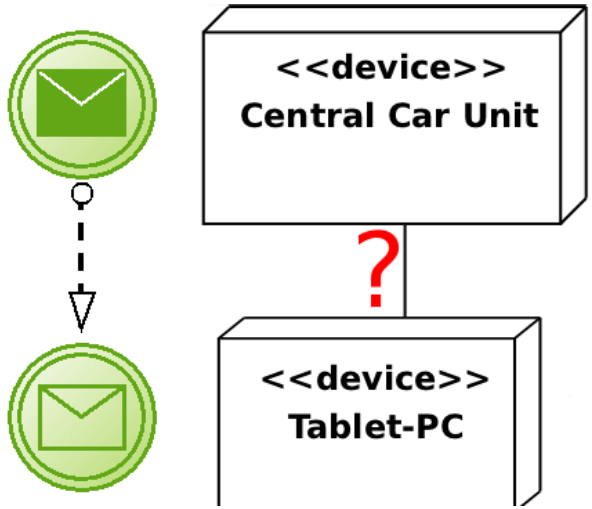
Einleitung

Bestehende Ansätze

Unsere Idee

Offene Fragen und Diskussion

- Betrachtung der Kommunikationsart
- Unterteilung bspw. möglich in
  - Funk
  - LAN
  - Internet
- Ziel: Klassifizierung der Kommunikationskanäle gemäß Schutzbedarf



Analyse der Risiken

Frühzeitige modellbasierte Risikoanalyse für mobile, verteilte Anwendungen

Wessel et al.

Einleitung

Bestehende Ansätze

Unsere Idee

Offene Fragen und Diskussion

- Betrachtung von Risiken durch die Ausführung der Aktivitäten
- Identifizierung sicherheitsrelevanter Aktivitäten mit *Riskfinder*-Algorithmus
- Untersuchen der Aktivitäten auf Übereinstimmungen mit BSI-Grundschutzhandbuch
  - Vergleich des Vokabulars mit Patternkatalog
  - Markieren von sicherheitskritischen Aktivitäten
  - Identifizierung von Risiken anhand fehlender Aktivitäten
  - Beispiele:
    - Zugriff auf personenbezogene Daten ohne sicheren Kommunikationskanal
    - Durchführen von Aktivitäten ohne vorangegangenes Login

Zusammenfassung

Frühzeitige modellbasierte Risikoanalyse für mobile, verteilte Anwendungen

Wessel et al.

Einleitung

Bestehende Ansätze

Unsere Idee

Offene Fragen und Diskussion

- Vorschlag zur Risikoanalyse in frühen Phasen des Softwareentwicklungsprozesses
- Lediglich Geschäftsprozesse und erste Entwürfe für Deployment nötig
- Keine Festlegung auf BPMN-Modelle, auch andere Datenquellen denkbar
- Einsatz von Textdatenbanken zur Präzisierung der Suche
  - Finden von Synonymen
  - Einbeziehung oft zusätzlich auftretender Begriffe

Offene Fragen

Frühzeitige modellbasierte Risikoanalyse für mobile, verteilte Anwendungen

Wessel et al.

Einleitung

Bestehende Ansätze

Unsere Idee

Offene Fragen und Diskussion

- Genauer evaluieren wie Schutzbedarf sinnvoll in Modelle integriert werden kann
  - Integration mit bestehenden Ansätze zur Sicherheitsannotation
  - Übertragung von UMLsec auf BPMN (*"BPMNsec"*)
  - Automatische Annotierung des BPMN-Diagrams
- Geeignete Heuristik für Schutzbedarf von Datenübertragungen entwerfen
  - Gilt inbesondere für Transitivität bzgl. der Prozessschritte
- Werkzeugunterstützung, d.h. Realisierung des Ansatzes
- Wie gut skaliert der Ansatz auf bereits vorhandene Prozesse?

LEHRSTUHL 14
SOFTWARE ENGINEERING

Fragen?

Frühzeitige modellbasierte Risikoanalyse für mobile, verteilte Anwendungen

Wessel et al.

Einleitung

Bestehende Ansätze

Unsere Idee

Offene Fragen und Diskussion

Vielen Dank für die Aufmerksamkeit

christian.wessel@cs.tu-dortmund.de

Frühzeitige modellbasierte Risikoanalyse für mobile, verteilte Anwendungen

Wessel et al.

Einleitung

Bestehende Ansätze

Unsere Idee

Offene Fragen und Diskussion

J. Jürjens.
Secure Systems Development with UML.
Springer, 1. Auflage, 11 2004.

Christian Wolter and Michael Menzel and Christoph Meinel.
Modelling Security Goals in Business Processes.
Modellierung, 2008.

Alfonso Rodríguez and Eduardo Fernández-Medina and Mario Piattini.
A BPMN Extension for the Modeling of Security Requirements in Business Processes.
IEICE Transactions 90-D(4): 745-752, 2007.