Geschäftsprozess-basiertes Risikomanagement

Jan Jürjens

Software & Systems Engineering
Informatik, Technische Universität München

juerjens@in.tum.de
http://www.jurjens.de/jan

Sichere Geschäftsprozesse

Analyse von sicherheitskritischen Geschäftsprozessen schwierig (komplexe organisatorische Abläufe).
Viele entwickelte und eingesetzte Systeme genügen nicht Sicherheitsanforderungen.
Sichere Produkte oft auf unsichere Weise eingesetzt.
Viele z.T. spektakuläre Angriffe.
Problem: Qualität vs. Kosten.

Modellbasierte Sicherheitsanalyse

Modellbasierte Sicherheitsanalyse von Geschäftsprozessen mit der Unified Modeling Language (UML):

- Einfache, intuitive Notation
- Komfortable Werkzeugunterstützung
- Automatische Sicherheits- und Risikoanalyse der modellierten Geschäftsprozesse unter Einbezugnahme des Unternehmensumfeldes
- Automatische Checks von System-konfigurationen (z.B. SAP-Berechtigungen, …)

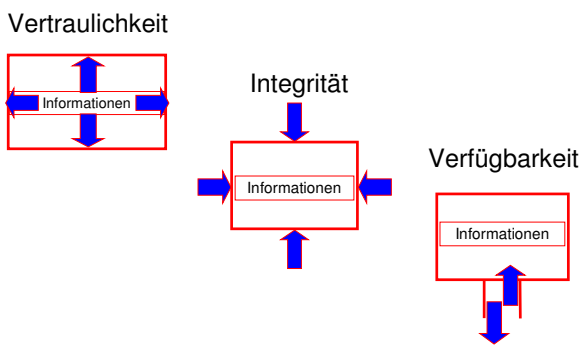
Einsatzfelder

- Systementwurf, -einrichtung, -konfiguration
  - z.B. Architekturbewertung (Beispiel: Teleworking), Plattformenwahl, Altsystemeinbindung.
  - spezielle Sicherheitsmechanismen wie Smartcards (Versicherungskarte).
- Laufender Betrieb
  - z.B. Konfigurationsmanagement, Überprüfung von Berechtigungen, Einrichtungen von Firewalls
- Sichere Geschäftsprozesse / Behördenvorgänge
- Einsatz in Sicherheitsaudits

Vorteile

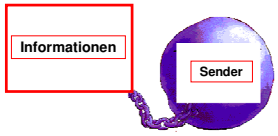
- Verwendung bewährter Regeln für sichere Geschäftsprozesse.
- Verwendbar ohne spezielle Ausbildung.
- Berücksichtigung von Sicherheit ab Geschäftsprozessentwurf.
- Erhöht Vertrauen in Korrektheit und Vollständigkeit von Audits.
- Unterstützt Zertifizierungen.

Sicherheitsanforderungen I

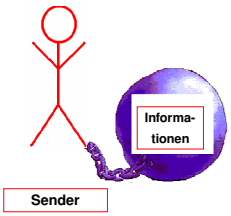


Sicherheitsanforderungen II

Authentizität



Nichtabstreitbarkeit



Sicherheitsanforderungen

Jeweils

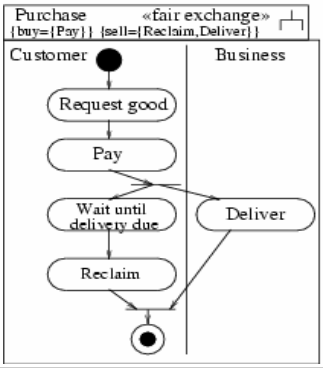
- verschiedene Sicherheitsstufen (Gewichtungen) bzgl. einzelner Daten
- Berücksichtigung verschiedener möglicher Angreifer

Sichere e-Transaktionen

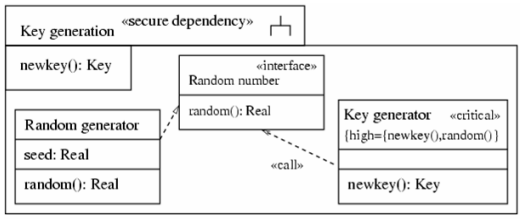
Sicherheit von Geschäftsprozessen z.B. bei e-Transaktionen.

Hier: Kunde kauft Ware beim Händler.

Nach Bezahlung bekommt Kunde Ware ausgeliefert oder kann Bezahlung zurückfordern.



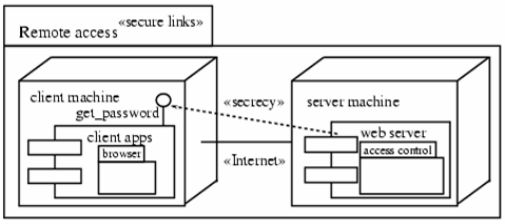
Datensicherheit



Sicherheitslevel definieren. Konsistenzanalyse.

Hier: Random generator und Kommunikation unterstützen Sicherheitsanforderung für random() in Key generator nicht.

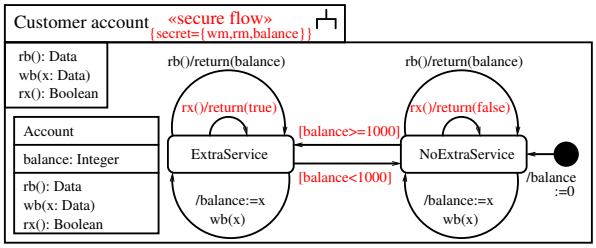
Sichere Systemarchitektur



Unterstützt Systemarchitektur Sicherheitsanforderungen ? Automatische Analyse bzgl. Bedrohungsszenario.

Hier: Bzgl. Standardangreifer unterstützt Internet-Verbindung nicht Vertraulichkeit.

Versteckte Informationsflüsse



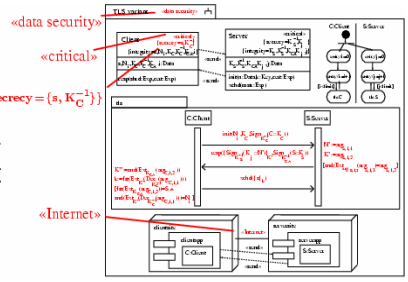
Können vertrauliche Daten heraussickern ? Oft ohne Werkzeugunterstützung nicht ersichtlich.

Hier: Indirekter Informationsfluss von vertraulichem wb() via nicht-vertraulichem rx().

Sichere Verwendung von Kryptomechanismen

Selbst für Experten oft schwierig zu beurteilen, daher automatische Analyse

Hier: Variante von TLS (INFOCOM 1999). Vertraulichkeit von s gegen Standard-angreifer verletzt (nicht-trivial).



Prinzipien für sichere Geschäftsprozesse

Saltzer, Schroeder (1975):

Design Prinzipien für sicherheitskritische Systeme.

- Anwendung auf Geschäftsprozesse ?
- Werkzeugunterstützung ?

"Keep it simple, stupid !"

Halten Sie das Design so einfach und klein wie möglich.

Oft werden Systeme kompliziert gemacht, um sie sicher aussehen zu lassen. Erhöht die Gefahr, dass sich Fehler im System befinden, die Angriffe ermöglichen.

Gleiches für Geschäftsprozesse. Werkzeuge zur Geschäftsprozessmodellierung helfen bei der Reduzierung unnötiger Komplexität.

"In dubio pro securitate"

Gründen Sie Zugriffsentscheidungen eher auf Verweigerung als auf Erteilung von Rechten.

Wenn eine Sicherheitsregel vergessen wird, führt dies nicht zu einer Sicherheitslücke.

Einhaltung der Regel automatisch überprüfen.

Vollständige Kontrolle

Jeder Zugriff auf jedes sicherheitskritische Objekt muss auf Berechtigung überprüft werden.

Sicherheit ist immer eine umfassende Eigenschaft – eine Kette ist so stark wie ihr schwächstes Glied.

Zugriffskontrollen können automatisch in Geschäftsprozessmodell eingefügt werden.

Keine "Sicherheit durch Obskurität"

Die Sicherheit eines Systems sollte nicht von der Geheimhaltung seines Aufbaues abhängen.

Allgemeine Informationen über sicherheits-kritisches System bleiben nicht auf Dauer geheim. Nur auf die Geheimhaltung einzelner Daten (kryptographische Schlüssel) bauen. Berücksichtigt in Geschäftsprozessanalyse.

4-Augen-Prinzip

Ein Schutzmechanismus, der zwei Schlüssel erfordert, ist robuster und flexibler als einer, der den Zugriff mit einem einzigen Schlüssel erlaubt.

Beispiel: Erteilung größerer Kredite im Bankenbereich nur möglich durch zwei Angestellte. Vermindert Missbrauchs-risiko. Berücksichtigt in Analyse.

Minimale Berechtigungen

Jedes Programm und jeder Benutzer des Systems sollte nur die zur Erledigung seiner Aufgaben nötigen Berechtigungen erhalten.

Jede unnötige Berechtigung verleitet zum Missbrauch.

Notwendige Berechtigungen können automatisch generiert werden.

Kleinster gemeinsamer Mechanismus

Minimieren Sie die Anzahl der Sicherheits-Mechanismen, die mehr als einen Benutzer gemeinsam haben und auf die sich alle Benutzer stützen.

“Schleichende” Übertragung von Berechtigungen und vertraulichen Informationen.

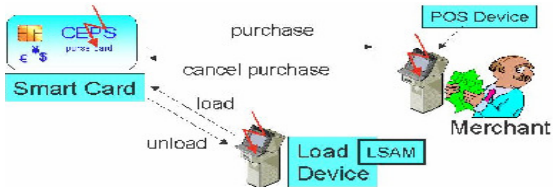
Benutzerfreundlichkeit

Benutzerschnittstellen müssen einfach konzipiert werden, so dass Benutzer Sicherheitsmechanismen problemlos korrekt anwenden.

Genauso für Geschäftsprozesse.

Fehler können zu Sicherheitsproblemen führen. Sicherheitsmassnahmen, die den normalen Betriebsablauf stören, werden erstaunlich erfolgreich umgangen…

Common Electronic Purse Specifications



Globaler Standard (90% des Marktes).

Smart card speichert Kontostand. Kryptographie auf Chip sichert Transaktionen.

Sicherer als Kreditkarten (transaktionsgebunden Autorisierung).

FAIRPAY

Load protocol

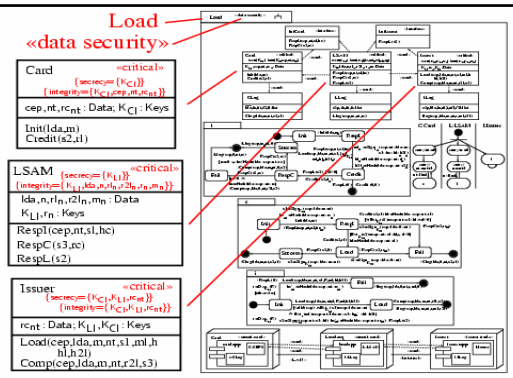
Karte mit Bargeld an Aufladestation laden (on-line).

Load Security Application Module (LSAM) speichert Transaktionsdaten.

Schickt Daten an Kartenemittent, der finanzielle Abwicklung übernimmt.

Symmetrische Verschlüsselung/Signatur.

Load protocol



Bedrohungsscenarien

Annahme: Card, LSAM manipulationssicher.
Mögliche Angreiferaktionen: Kommunikation abhören, Komponenten ersetzen.
Mögliche Motive:
Kartenbesitzer: Aufladen ohne zu bezahlen
Ladestation Betreiber: Geld des Kartenbesitzers einbehalten
Kartenausgeber: Geld vom Ladestation Betreiber verlangen
Gemeinsamer Angriff möglich.

Sicherheitsanalyse

Keine direkte Kommunikation zwischen Karte und Inhaber. Manipulation der Aufladestation möglich.

➔ Post-Transaktions-Abrechnungsystem.

➔ Gespeicherte Transaktionsdaten sicherheitskritisch.

➔ Modell-basierte Analyse dieses Teiles.

Sicherheitsanforderungen (informell)

Kartenbesitzer: Wenn Karte laut Log mit Betrag *m* aufgeladen wurde, kann Kartenbesitzer dem Emittenten beweisen, dass Ladestation-Betreiber ihm *m* schuldet.

Ladestation-Betreiber: Ladestation-Betreiber muss Betrag *m* dem Kartenausgeber nur zahlen, nachdem vom Kartenbesitzer erhalten.

Emittenten: Summe der Guthaben von Karteninhaber und Ladestation Betreiber unverändert.

Schwachstelle

Analyse: Keine Sicherheit für Ladestation gegen interne Angreifer.

Änderung: asymmetrischer Schlüssel in ml_n, Signatur für hc_{nt}.

Modifizierte Version sicher laut Analyse.

Sicherheitsanalyse im Bankenbereich

Sicherheitsanalyse für webbasiertes Kundensystem in grosser deutschen Bank.

Eigenes Authentisierungsprotokoll über SSL (für Vertraulichkeit). Korrektheit kaum von Hand nachweisbar.

Verifikation des Protokolles, Verbesserungsvorschläge für die Architektur.

SAP Berechtigungen

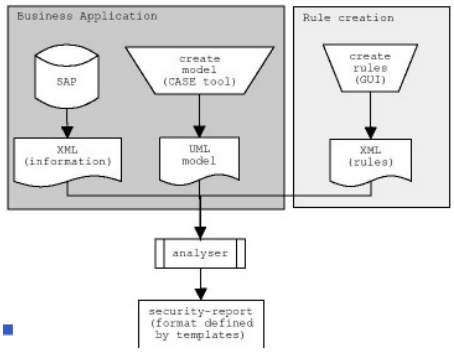
Auf Anregung von grosser deutscher Bank.

SAP Berechtigungen auf Regeln überprüfen (z.B. Gewaltenteilung). Nicht von Hand machbar:

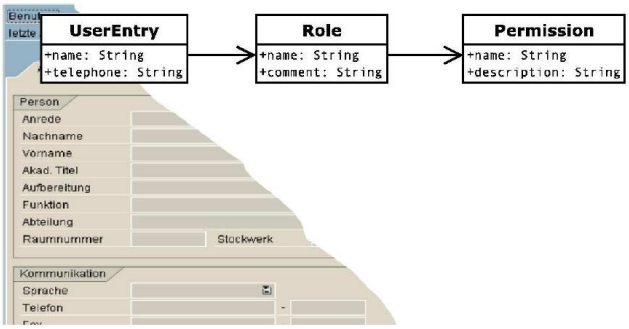
- grosse Datenmenge (60.000 Datensätze)
- komplexe Querverbindungen zwischen Berechtigungen auf verschiedenen Ebenen
- dynamische Änderungen, Delegation

Automatische Überprüfung erhöht Sicherheit an zentraler Stelle

Werkzeugarchitektur



Screenshot Analysewerkzeug



Biometriesysteme

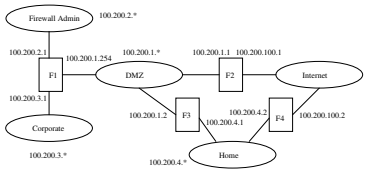
Analyse eines Biometriebasierten Zugangssystem in Entwicklung bei T-System (Verisoft Projekt, Bundesministerium für Bildung und Forschung).

Modell-basierte Analyse basierend auf Geschäftsprozessen mit UML.

Firewallkonfigurationen

Fehlkonfiguration häufige Schwachstelle beim Einsatz von Firewalls.

Modell-basierte Analyse: Mit Netzwerk-modell automatisch überprüfen, dass Konfigurationen Security Policy umsetzen.



IT-Risiken vs. KontraG/Basel II

Basel II (bis 2006): risikogerechtere Regelung der Eigenkapitalanforderungen

Genauere Analysemethoden (Kreditrisiko, operationelles Risiko, *internal-ratings-based).* Offenzulegen.

Insbesondere IT Risiken (*unexpected loss,* z.B. Virenbefall, Hackerangriff, …)

➔ modellbasierte IT-Risiko-Bewertung

Verbindung mit Analyse-Werkzeug

CASE Werkzeug mit UML-ähnlicher Notation: AUTOFOCUS

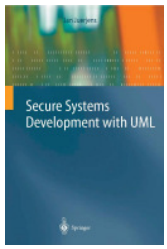
- Simulation
- Validierung (Konsistenz, Testen, Modellprüfung)

➔ automatische Risikobewertung

Anbindung an UML, GP Werkzeuge (Rose, Aris, Adonis…).

Weitere Informationen

Buch: Jan Jürjens, Secure Systems Development with UML, Springer-Verlag, März 2004



Tutorials: z.B. SAC (April, Zypern)

Folien, Werkzeugwebinterface etc.:

http://www4.in.tum.de/~juerjens/csdumltut
(Benutzer Participant, Passwort Iwasthere)

Zum Abschluss

Wir sind immer an Problemen aus der Praxis für unsere Werkzeuge und Methoden interessiert.

Mehr Info: http://www4.in.tum.de/~secse

Kontakt: hier oder via Internet.

Danke für Ihre Aufmerksamkeit !

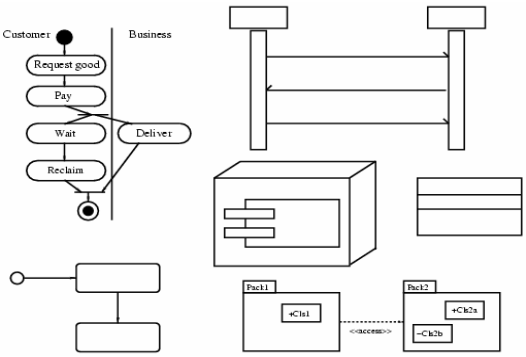
Backup

Unified Modeling Language

Unified Modeling Language (UML):

- visuelle Modellierungsnotation
- verschiedene Ansichten eines Systems
- hoher Abstraktionsgrad möglich
- de-facto Industrie-Standard (OMG)
- Standard Erweiterungs-Mechanismen

UML: Überblick



UML Diagrammarten

Aktivitätsdiagramm: Kontrollfluß zwischen Systemkomponenten (Geschäftsprozesse)

Klassendiagramm: Datenstruktur des Systems

Sequenzdiagramm: Interaktion zwischen Komponenten durch Nachrichtenaustausch

Zustandsdiagramm: dynamisches Verhalten von Komponenten

Einsatzdiagramm: Systemumgebung

Package: System-Teile zusammenfassen

UML Erweiterungs-Mechanismen

Stereotyp: Modellelemente mit ≪label≫ markieren.

Tagged Value: {tag=wert} Paar an stereotypisiertes Element anfügen.

Constraint: Bedeutung von stereotypisiertem Element spezialisieren.

UMLsec

UML Erweiterung für sicherheitskritische Geschäftsprozesse.

Sicherheitsanforderungen als Stereotypen mit Tags in Geschäftsprozessmodell einfügen.

Assoziierte Constraints für automatische Analyse des Geschäftsprozesses nach möglichen Schwachstellen.

Ziel: Geschäftsprozess erfüllt Security Policy im Systemkontext.

≪Internet≫, ≪encrypted≫, ≪LAN≫, …

Markieren Verbindungen bzw. Systemknoten.

Für Angriffstyp A, Stereotyp s: $Threats_A(s) \in$ {delete, read, insert, access} -- Angreiferaktionen.

Standard-angreifer:

Stereotyp	$Threats_{default}()$
Internet	{delete, read, insert}
encrypted	{delete}
LAN	∅
smart card	∅

≪secure links≫

Physikalische Ebene erfüllt Sicherheitsanforderungen an Kommunikation.

Constraint: für Kommunikation *d* mit Stereotyp $s \in$ {≪secrecy≫, ≪integrity≫} zwischen Komponenten auf Knoten $n \neq m$ existiert Verbindung *l* zwischen *n* und *m* mit Stereotyp *t* sodass:

- falls *s* = ≪secrecy≫: read $\notin Threats_A(t)$.
- falls *s* = ≪integrity≫: insert $\notin Threats_A(t)$.

≪secure dependencies≫

Kommunikation zwischen Komponenten bewahrt Sicherheitsanforderungen {secrecy}, {integrity} an ausgetauschte Daten.

Constraint: Für Kommunikation von *C* zu *D*:

- Jede Nachricht *n* markiert {secrecy} in *C* genau dann wenn in *D*.
- Analog für {integrity}.

≪secure flow≫

Kein indirekter Informationsfluss.

Constraint:

- {secrecy} markierte Daten können nur {secrecy} markierte Daten beeinflussen.
- {integrity} markierte Daten können nur durch {integrity} markierte Daten beeinflusst werden.

≪data security≫

Sicherheit von ≪critical≫ Daten gegenüber Bedrohungsszenario in Einsatzdiagramm.

Constraint:

- Vertraulichkeit von {secrecy} Daten bewahrt.
- Integrität von {integrity} Daten bewahrt.

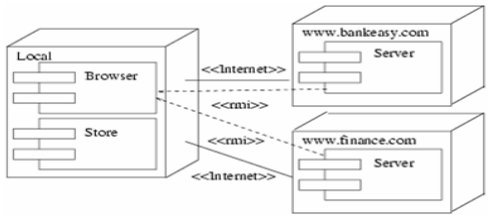
≪fair exchange≫

Mehrseitige Sicherheit von e-Commerce Transaktionen.

Constraint: nach {buy} Zustand in Aktivitätendiagramm irgendwann {sell} Zustand.

(Kann nicht für System zugesichert werden, die Angreifer vollständig stoppen können.)

CORBA-Anwendung



Objektbasierte Zugangskontrolle, abhängig vom Ausführungszusammenhang.

Schwer nachzuvollziehen ➔ Automatische Analyse von Modell / Implementierung