Vorlesung (WS 2014/15)

Sicherheit: Fragen und Lösungsansätze

Dr. Thomas P. Ruhroth

TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

“Security Engineering“

**[mit freundlicher Genehmigung basierend
auf einem Foliensatz von
Prof. Dr. Claudia Eckert (TU München)]**

Literatur:

Claudia Eckert: IT-Sicherheit: Konzept - Verfahren - Protokolle, 7., überarb. und erw. Aufl., Oldenbourg, 2012.

E-Book: http://www.ub.tu-dortmund.de/katalog/titel/1362263

Agenda

- Vorgehen beim Sicherheitsengineering
- UMLsec

Ziele

Ziele

- Secure by Design: Systematische Integration von Sicherheits-aspekten bei der Entwicklung von IT-Systemen.

  Secure Programming ist Teilaspekt, wird hier **nicht** behandelt
- Aber auch: Systematische Härtung und Absicherung bereits entwickelter und im Betrieb befindlicher Software und Systeme

Secure Engineering:

- umfasst (Vorgehens-)Modelle, Methoden und Maßnahmen, um sichere IT-Systeme zu entwickeln **und** zu betreiben.
- Vorgehensprozesse sind angelehnt an Methoden aus dem Software-Engineering und dem Bereich Fehlertoleranz

Allgemeine Design-Prinzipien

Allgemeine Design-Prinzipien sicherer Systeme

- Erlaubnis-Prinzip *(fail-safe defaults)*

  Zugriffe sind verboten, falls nicht explizit erlaubt
- Vollständigkeits-Prinzip *(complete mediation)*

  Jeder Zugriff ist zu kontrollieren
- Prinzip der minimalen Rechte *(need-to-know)*

  Subjekt erhält nur die benötigten Rechte
- Prinzip des offenen Entwurfs *(open design)*

  Geheimhaltung darf nicht Voraussetzung für Sicherheit sein
- Benutzerakzeptanz *(economy of mechanism)*

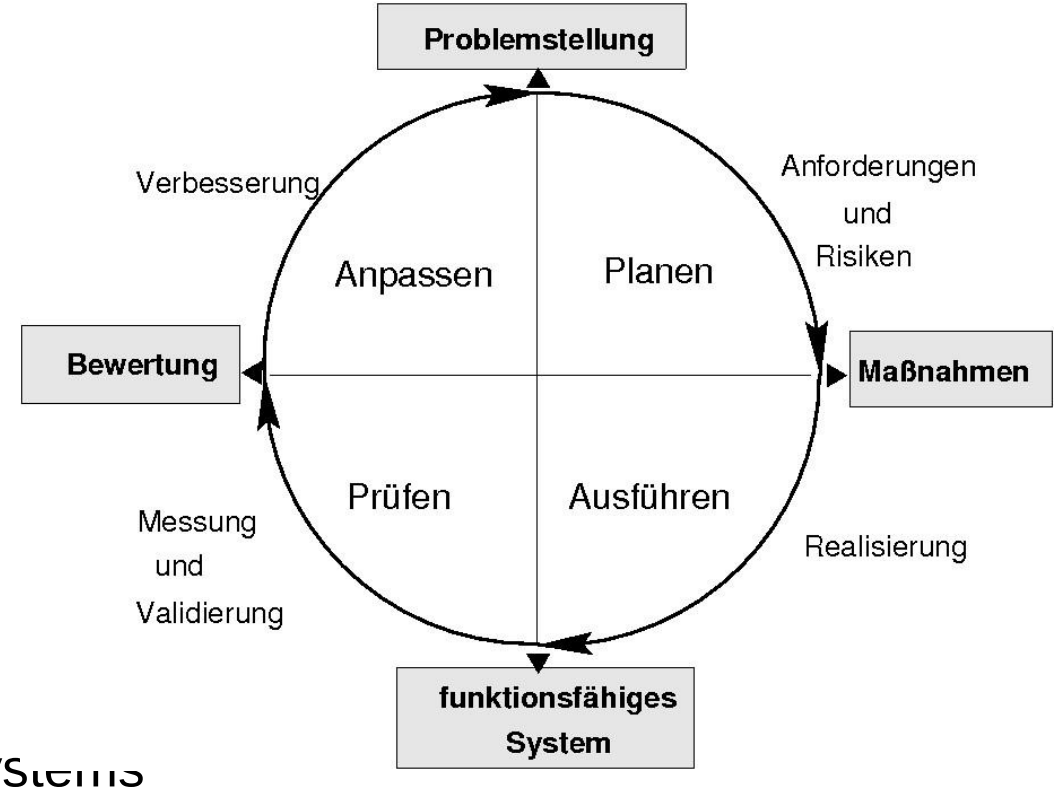
  einfach zu nutzende Mechanismen, Verfahren

7.1 Phasen des Security-Engineerings

Phasen (stark vergröbert) des Security-Engineerings

Iterierend durchzuführen

1. Strukturanalyse und Pflichtenheft
2. Ermittlung des Schutzbedarfs
3. Bedrohungsanalyse
4. Risikoanalyse
5. Erstellen einer Sicherheits-Policy
6. Modellierung des Systems
7. Entwurf einer Systemarchitektur
8. Feinentwurf und Implementierung
9. Validierung und Evaluierung des Systems
10. Wartung und Überprüfung im laufenden Betrieb



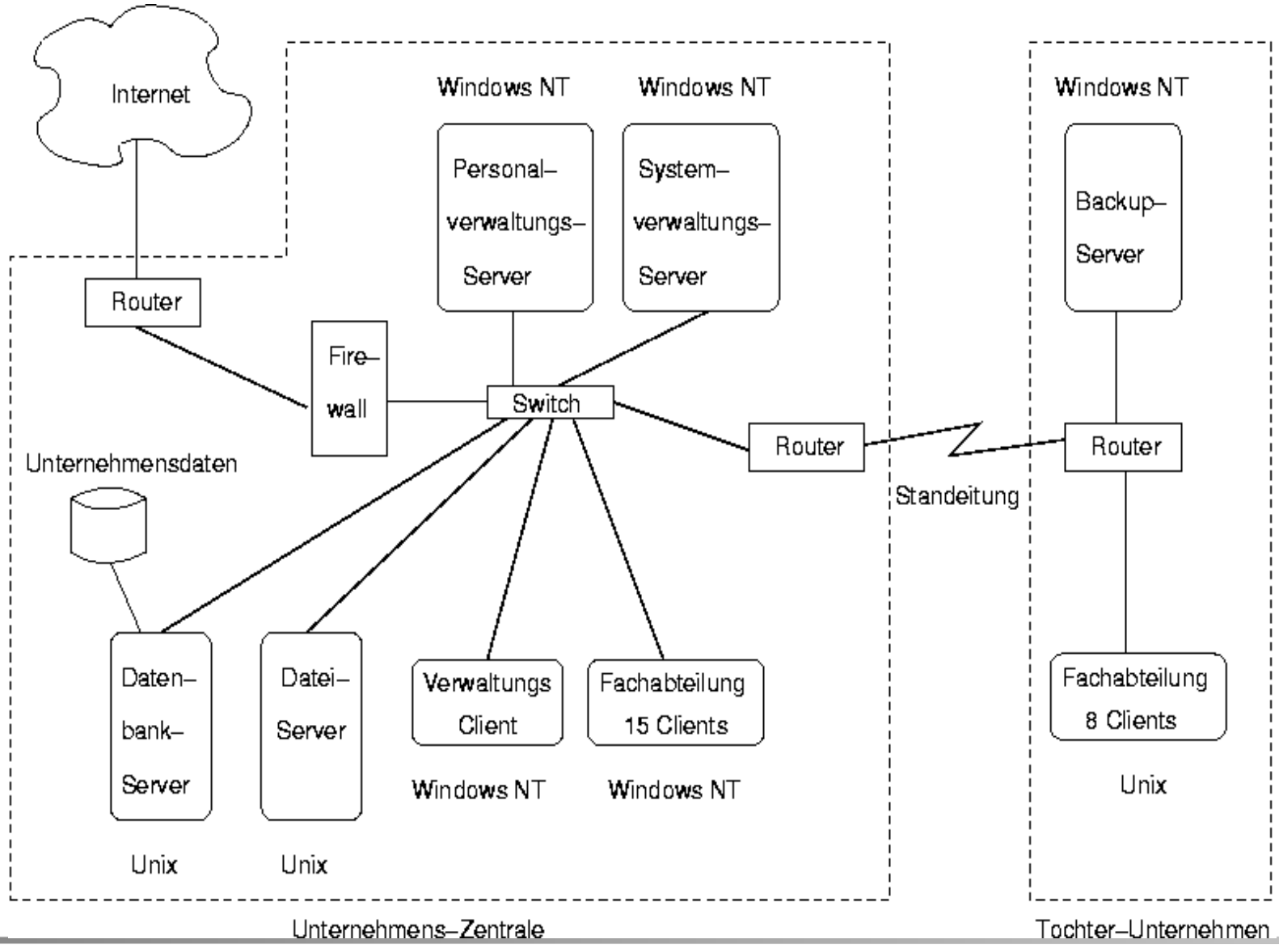
Strukturanalyse

Strukturanalyse

Beschreibung des (vorhandenen bzw. geplanten) IT-Systems:

- Beschreibung der Systemfunktionalität
  - Beschreibung vorhandener bzw. einzusetzender Systemkomponenten und -dienste
- Beschreibung des Pflichtenhefts
  - Systemanforderungen und Einsatzumgebung des Systems
- Erstellung eines Netztopologieplans
  - grafische Übersicht aller Teilkomponenten (z.B. PCs, Server, DBs, Hubs) und deren Verwendungszweck
  - Vorhandene Dienste u. Verbindungen (LAN, WLAN, …)
  - Technische Details (z.B. Hardware, MAC-Adresse, ...)

Beispiel für einen Netztopologieplan



Schutzbedarfsermittlung

Ziel: Klären: Was sind schützenswerte Objekte, was sind die Schutzziele, wie wichtig sind sie?

- Schutzbedarfsfeststellung anhand von Schadensszenarien, z.B. orientiert an Grundschutzhandbuch des BSI
- meist nicht quantitative sondern qualitative Aussagen:

  niedriger bis mittlerer, hoher, sehr hoher Bedarf

niedrig bis mittel	Die Schadensauswirkungen sind begrenzt und überschaubar
hoch	Die Schadensauswirkungen können beträchtlich sein
sehr hoch	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß annehmen

Schadensszenarien

Schadensszenarien: (6 Kategorien nach BSI Handbuch)

Hier nur ein Beispiel, Rest siehe Buch IT-Sicherheit

Kategorie (1): Verstoß gegen Gesetze/Vorschriften/Verträge

- Beispiele: Grundgesetz, Bundesdatenschutzgesetz, Urheberrechtsgesetz, IuKDG, Dienstvorschriften, …

Erhebung des Schutzbedarfs mit : Was wäre wenn ... Fragen

- **Beispiel:** niedriger/mittlerer Bedarf für die Kategorie (1): Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen, geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen.
- **Beispiel:** Schutzbedarf für Gesundheitsdaten? Was wäre wenn Vertraulichkeit verletzt? Integrität verletzt?

Bedrohungsanalyse

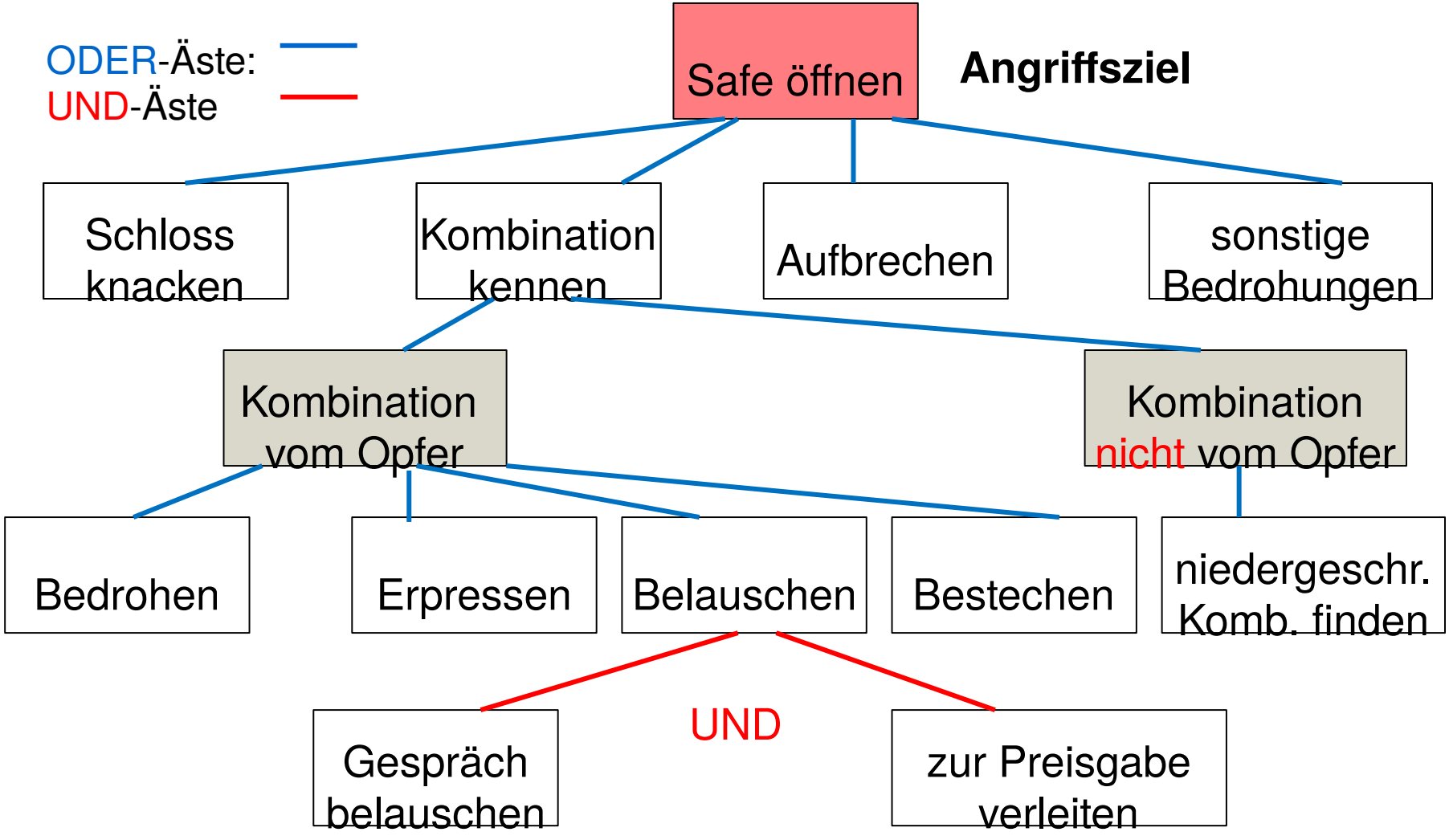
Bedrohungsanalyse Strukturierte Analyse z.B. mittels

Bedrohungsbäumen (*attack tree*)

Angelehnt an Fehlerbäumen, HAZARD-Analyse (Zuverlässigkeit)

- Ziel: verschiedene Angriffsmöglichkeiten mit Baum modelliert
- Pro Angriffsziel ein Baum:
  - Wurzel beschreibt ein Angriffsziel, z.B. Safe knacken
  - Blatt beschreibt einen einzelnen Angriffsschritt
  - Pfad von Blatt zur Wurzel: Angriff zum Erreichen des Ziels
- Beschreibung von Situationen, in denen
  - mehrere Angriffsschritte zusammen notwendig sind: UND
  - alternative Angriffsschritte: ODER-Äste (Teilbäume)
- Zur systematischen Erstellung: Festlegen von Teilzielen

Beispiel: Bedrohungsbaum



Risikoanalyse

Risikoanalyse: Bewertung der Bedrohungen

- Sicherheitsrisiko $R = S \cdot E$ mit:
  - Schadenshöhe *S*,
  - Eintrittswahrscheinlichkeit *E*

Beispiele:

S=1.000.000€;	E=0,01:	R=10.000€
S=30.000€;	E=0,5:	R=15.000€

Schadenshöhe *S*:

- Primäre Schäden: Produktivitätsausfall, Wiederbeschaffungs-, Personalkosten, Wiederherstellungskosten, …
- Sekundäre Schäden (schwer zu quantifizieren): Imageverlust, Vertrauensverlust bei Kunden, ….

Eintrittswahrscheinlichkeit E ($0 \leq E \leq 1$):

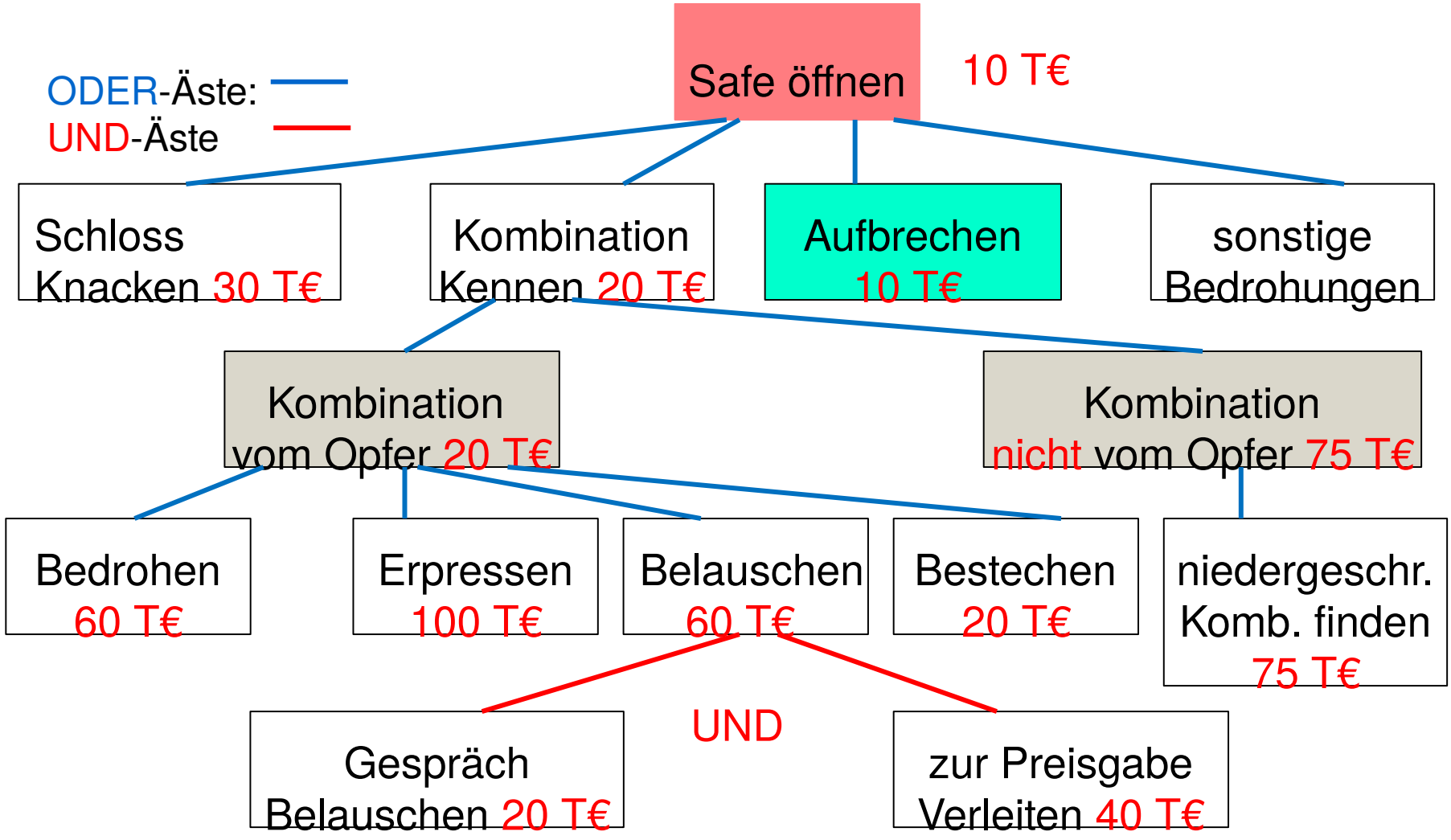
- Eigene Erfahrungen (z.B. aus Auditprozessen)
- Öffentliche Statistiken (CERT, ...) (was heißt CERT?)
- Einschätzung des Nutzens für den Angreifer und des
- geschätzten Aufwands für erfolgreichen Angriff
  - Basis: Erstellen von **Angreifermodellen**

Angreifermodell: beschreibt u.a.

- Angreifertyp (Hacker, Spezialist, ...),
- Budget (Unternehmen, Regierung, Privatperson, …)
- Kenntnisse (keine, Insider-Wissen, Expertenwissen, ...),
- Ziele (Gewinn, Schaden, Rache, …)

Methodik: z.B. Attributierung des Baumes mit *S* und *E*-Werten

Beispiel: Bedrohungsbaum (Fortsetzung)



Ziel: finde die kritischen Pfade!

DREAD-Methode

Risikoanalyse mit DREAD-Methode

- **DREAD-Kriterien**
  - D amage: Schadenspotential, der Schwachstellen
  - R eproducibility: Schwierigkeit zur Angriffs-Reproduktion
  - E xploitability: Schwierigkeit, einen Angriff durchzuführen
  - A ffected: Einschätzung wie groß der Kreis der potentiell betroffenen Benutzer ist
  - D iscoverability: Schwierigkeitsgrad, mit dem die Sicherheitslücke aufgedeckt werden kann.
- für jedes DREAD-Kriterium erfolgt eine Qualifizierung nach
  - hoch (3), bei Risiko-Wert zwischen 12 und 15
  - mittel (2), bei Risiko-Wert zwischen 8 und 11
  - gering (1), bei Risiko-Wert zwischen 5 und 7
- **Risikobewertung**: Summe der Einzelbewertungen

Penetrationstests

Penetrationstests als Methode zur Risikoanalyse

- Simulation des Verhaltens eines vorsätzlichen Angreifers
- Schwachstellen und potentielle Schäden ermitteln
- **Verschiedene Vorgehensweisen: Ansätze:**
- Blackbox: keine/geringe System-Kenntnisse vorhanden
- Whitebox: detaillierte Kenntnisse über interne Strukturen, Anwendungen, Dienste, Source-Code etc.
- **Typische Penetrationstests** umfassen: u.a.
- Erraten von Passwörtern oder Wörterbuchattacken,
- Aufzeichnen und Manipulieren des Netzverkehrs,
- Einspielen gefälschter Datenpakete (Fuzzy-Techniken) oder
- Ausnutzen bekannter Schwachstellen

7.2 Kriterien zur Bewertung

Kriterien zur Bewertung der IT-Sicherheit

Ziele:

Einheitliche Bewertungskataloge, Vergleichbarkeit:

- Maßnahmenkatalog: Menge von Sicherheitsgrundfunktionen
- Qualität (der Realisierung)**:** z.B. getestet, ..., formal verifiziert
- Güte (der verwendeten Mechanismen)**:** ungeeignet, ..., unüberwindbar
- Bewertung durch unabhängige Stelle:

  Evaluation und Zertifizierung, Beispiele für Zert.-Instanzen?
- Leitlinien für Hersteller bzw. Entwickler: worauf ist zu achten
- Leitlinien für Anwender bei Produktwahl: Vergleichbarkeit, …

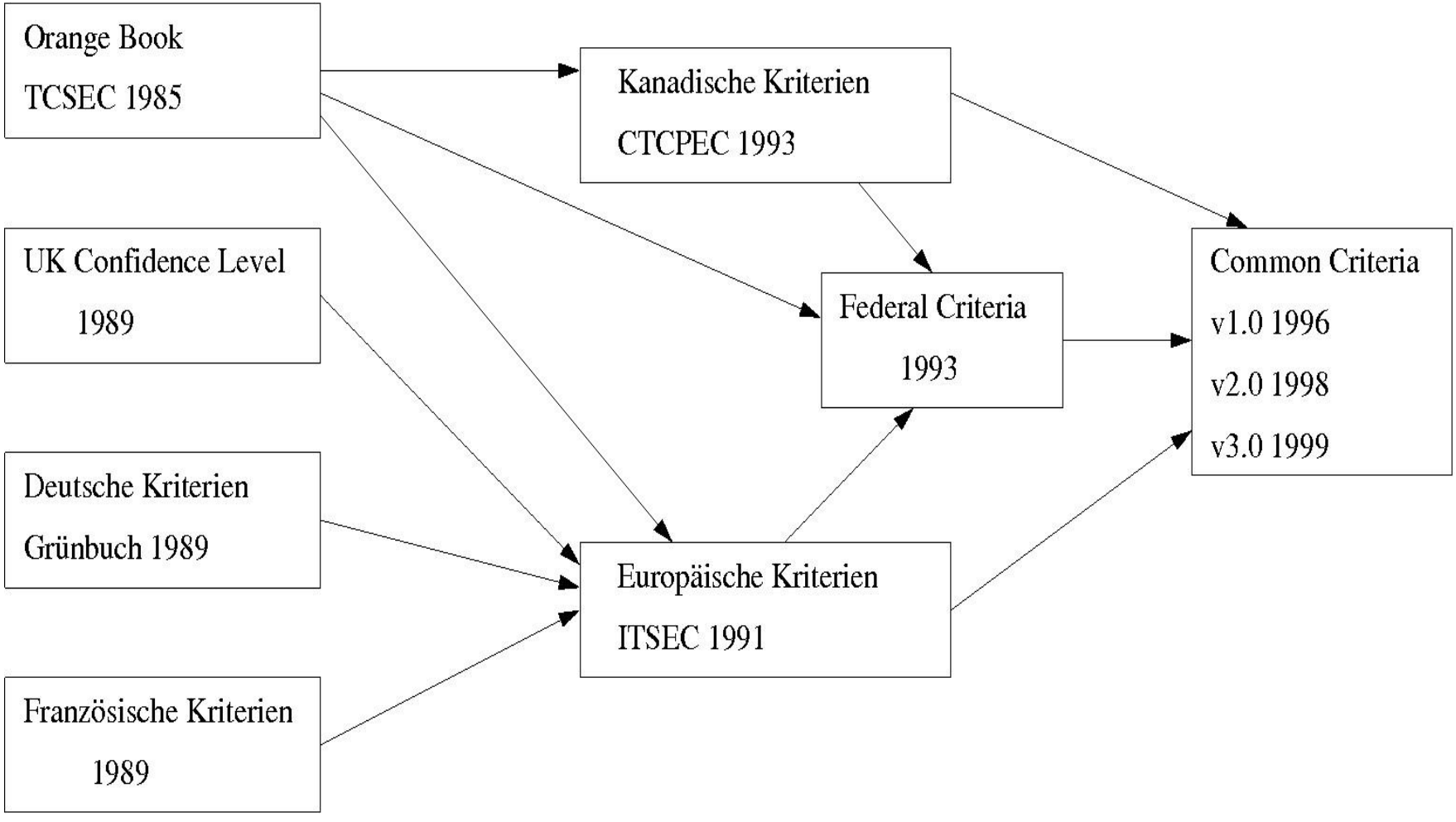
Kriterienkataloge

Entwicklungsstufen der bekanntesten Kriterienkataloge

- Trusted Computer System Evaluation Criteria (Orange Book)
  - 1980 entwickelt
  - 4 Sicherheitsstufen (hierarchisch): (D < C1 < ... < B3 < A1)
  - fehlende Trennung zwischen Funktion und Qualität
- Deutsche IT-Kriterien (Grünbuch): 1989
  - Bewertung der eingesetzten Mechanismen:

    ungeeignet, schwach, mittel, stark, sehr stark, unüberwindbar
  - Funktionsklassen F1–F10
  - Qualitätsstufen Q0–Q7 (unzureichend - formal verifiziert)
- Europäische ITSEC-Kriterien
- Internationale Common Criteria (CC) for Information Technology Security Evaluation

Übersicht: nationale und internationale Bewertungskriterien



Common Criteria

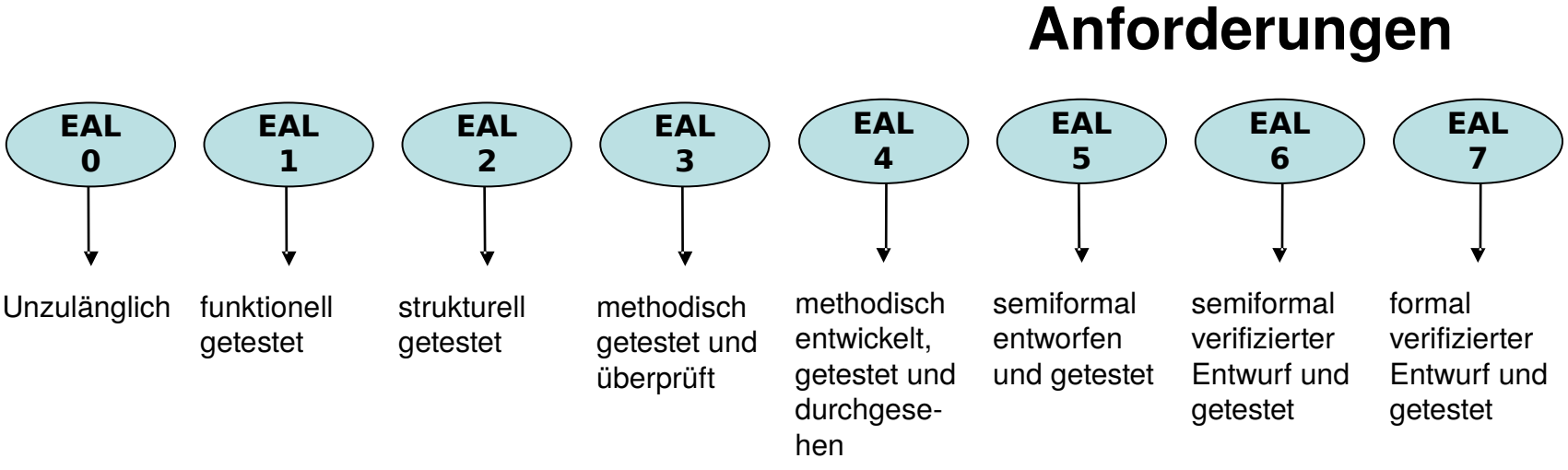
Common Criteria, seit 1996 entwickelt

- Target of Evaluation (TOE): IT-Produkt oder -System und die zugehörige Begleitdokumentation, die zu evaluieren sind.
  Auf deutsch: EVG: Evaluationsgegenstand
- Security Target (ST): Menge von Sicherheitsanforderungen, die Grundlage der Evaluation eines TOE sind.
- Protection Profile (PP): Implementierungsunabhängige Menge von Sicherheitsanforderungen eines TOE.
- TOE Security Policy (TSP): Regelwerk, beschreibt, wie ein Asset im TOE verwaltet, geschützt und verteilt wird.
- TOE Security Function (TSF): Hardware, Software u. Firmware, die zur Durchsetzung der TSP benötigt werden.
- Evaluation Assurance Level (EAL): Evaluationsstufe

CC: Evaluationsklassen

Common Criteria: Evaluationsklassen EAL

- 8 EAL- Klassen (Evaluation Assurance Level)
- **Beispiel:** RFID-Chip in nPA: EAL5 hoch zertifziziert



CC: Funktionsklassen

Common Criteria: Funktionsklassen

11 Funktionsklassen mit funktionellen Familien

- Sicherheitsanforderungen in Klassen strukturiert:
- Klasse ist in Familien aufgeteilt:
  - Komponente einer Klasse definiert konkrete Anforderungen: z.B. Identifikation, Zugriffskontrolle, Beweissicherung
  - Sicherheitsanforderungen spiegeln Best-Practice wider
  - empfohlen zur Beschreibung der Funktionalität von Produkten bzw. Systemen

Beispiel: für Sicherheitsklassen (siehe Buch IT-Sicherheit)

- **Klasse FAU:** Security Audit: Protokollieren und Analysieren sicherheitsrelevanter Events

Schutzprofile

Schutzprofile (Protection Profiles)

- anerkannte Lösung für Standard-Sicherheitsprobleme einer Produktgruppe, z.B. derzeit PP für Smart Meter in Arbeit
- implementierungsunabhängig,
- Verallgemeinerung der CC-Sicherheitsvorgaben
- PPs beschreiben ein Sicherheitskonzept
- Anwender-Sicht:
  - gute Vergleichbarkeit verschiedener Produkte, die auf Basis des Schutzprofils entwickelt und evaluiert wurden
- IT-Hersteller-Sicht:
  - erfolgreiche Evaluierung eines Schutzprofils bescheinigt, dass das PP ein sinnvolles, im Markt gewünschtes Konzept für ein IT-Sicherheitsprodukt darstellt

Aufbau eines Schutzprofils

PP-Einführung:

- eindeutige Identifikation und allgemeiner Überblick über das Schutzprofil

EVG-Beschreibung:

- Beschreibung des EVG bzw. der Produktgruppe, auf die sich das Schutzprofil bezieht
- Einsatzmöglichkeiten, die allgemeinen IT-Sicherheits-eigenschaften und Grenzen der Benutzung

EVG-Sicherheitsumgebung:

- Beschreibung der Sicherheitsaspekte der beabsichtigten Einsatzumgebung und die erwartete Art der Nutzung des EVG

EVG-Sicherheitsumgebung (Fortsetzung)

- Durchführung einer Art Risikoanalyse
- Identifikation der möglichen Angriffe und der Schutzmethoden
- Identifikation der Bedrohungen, denen nicht durch den EVG entgegengewirkt wird
- organisatorische Sicherheitspolitiken: Annahmen über den sicheren Betrieb des EVG

Sicherheitsziele:

- Definition der Sicherheitsziele des EVG in seiner Einsatzumgebung
- Angaben, wie den Bedrohungen entgegengewirkt werden soll bzw. die Sicherheitspolitiken erfüllt werden sollen

IT-Sicherheitsanforderungen:

- Definition der Anforderungen an die Funktionalität und an die Vertrauenswürdigkeit des EVG
- Rückgriff auf die Anforderungen der Teile 2 und 3 der CC oder freie Formulierung

PP-Anwendungsbemerkungen: optionale Informationen

Erklärungsteil des PP:

- Zeigen, dass ein zu diesem Schutzprofil konformer EVG eine wirksame Menge von IT-Sicherheitsgegen-maßnahmen in seiner Sicherheitsumgebung bereitstellt: Sicherheitskonzept ist in sich schlüssig
- Beziehungen zw. Sicherheitsumgebung, den Sicherheitszielen und den IT-Sicherheitsanforderungen werden beschrieben

Fazit

Fazit

- 4-stufige Prozess der Bewertung der Vertrauenswürdigkeit des Entwicklungsprozesses
  - Anforderungen, Architekturentwurf,
  - Feinentwurf und Implementierung
- Wirksamkeit: Eignung und Zusammenwirken der Funktionalität
  - Stärke der EVG-Sicherheitsfunktionen entspricht Mechanismenstärke: niedrig, mittel oder hoch
  - getrennte Prüfung und Bewertung der Funktionalität und der Vertrauenswürdigkeit.

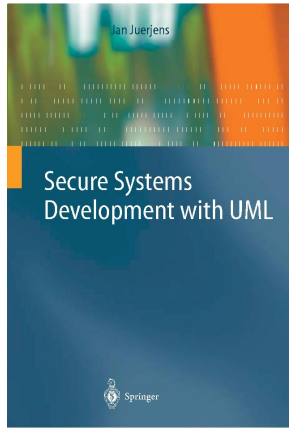
Pros/Cons CC-Evaluierung?

Beispiele CC evaluierter Systeme?

Modell-basierte Sicherheit mit UMLsec

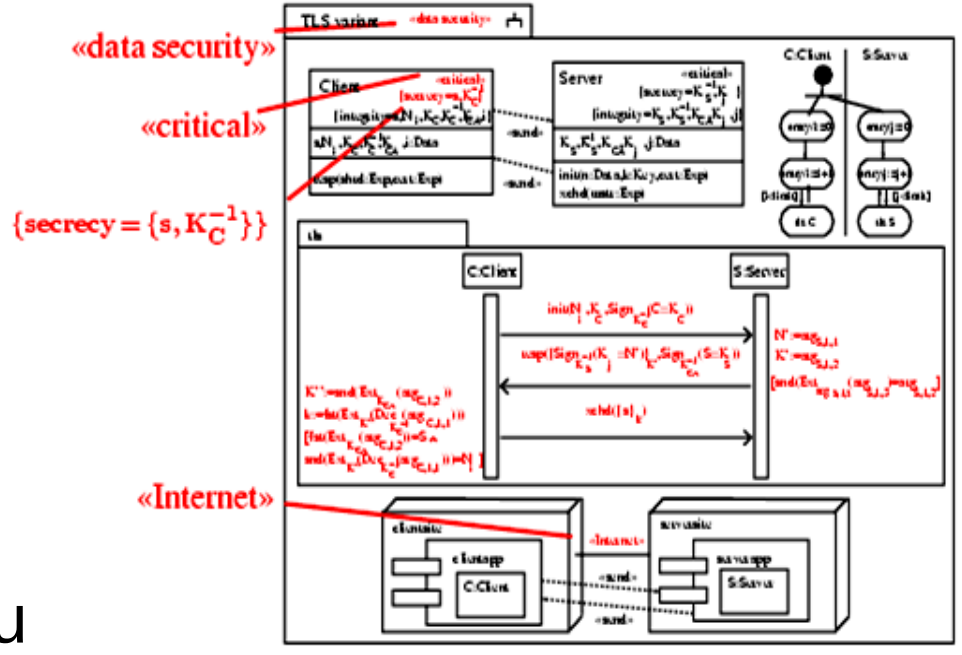
Erweiterung der Unified Modeling Language (UML) für sichere Systementwicklung.

- Evaluiert UML Modelle auf ihre Sicherheit.
- Fasst bestehende Regeln des gewissenhaften sicheren Entwickelns zusammen.
- Macht diese Entwicklern zugänglich die nicht auf sichere Systeme spezialisiert sind.
- Diskutiert Sicherheitsanforderungen aus frühen Designphasen im Systemkontext.
- Kann auch in der Zertifizierung benutzt werden.



UMLsec

Fügt wiederkehrende Sicherheits-anforderungen, feindliche Szenarios, und Sicherheit-mechanismen als vordefinierte Marker hinzu.



Nutzt verknüpfte logische constraints um die Spezifikation zu verifizieren. Dabei kommen Model-Checker und ATPs, die auf formalen Semantiken basieren, zum Einsatz.

Stellt sicher das die die Modellspezifikation in UML die Sicherheitsanforderungen im Kontext des Dolev-Yao Angreifermodells durchsetzt.

Was deckt UMLsec ab ?

Sicherheitsanforderungen: <<secrecy>>,…

Bedrohungsszenarien: Vewende $\text{Threats}_{\text{adv}}(\text{ster})$.

Sicherheitskonzepte: Zum Beispiel <<smart card>>.

Sicherheitsmechanismen: Z.B. <<guarded access>>.

Grundlegende Sicherheit: eingebaute Verschlüsselung

Physikalische Sicherheit: Im Verteilungsdiagramm.

Sicherheitsmanagement: Im Aktivitätsdiagramm.

Technologie spezifisch: Java, CORBA Sicherheit.

Der NSA-Skandal