Security Engineering with Patterns

Markus Schumacher

TU Darmstadt
Fachbereich Informatik
IT Transfer Office (ITO)

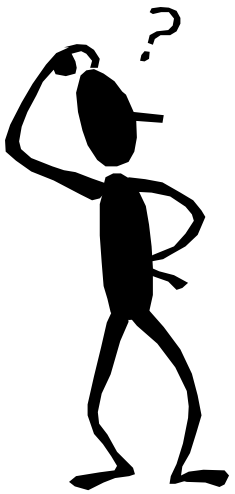
Übersicht

- Motivation
  - Schutzziele
  - Fallstudien
- Problemstellung
- Entwurf sicherer Systeme mit Patterns
  - Grundlagen Security Patterns
  - Theoretisches Modell
  - Neue Techniken
- Zusammenfassung & Ausblick

Schutzziele

- Vertraulichkeit
  - keine Preisgabe sensitiver/privater Informationen
- Integrität
  - keine unauthorisierte Modifikation or Zerstörung von Information
- Kein Denial of Service
  - ärgerlich, teuer
- Keine Imitation, kein Abstreiten
  - rechtliche Relevanz

Wichtigere Ziele?



- Der Kunde ist König:
  - Funktionalität
  - Performanz
  - Kosten
  - Wartbarkeit
  - Verfügbarkeit
  - Interoperabilität
  - Integrationsfähigkeit
  - Erweiterbarkeit
  - …

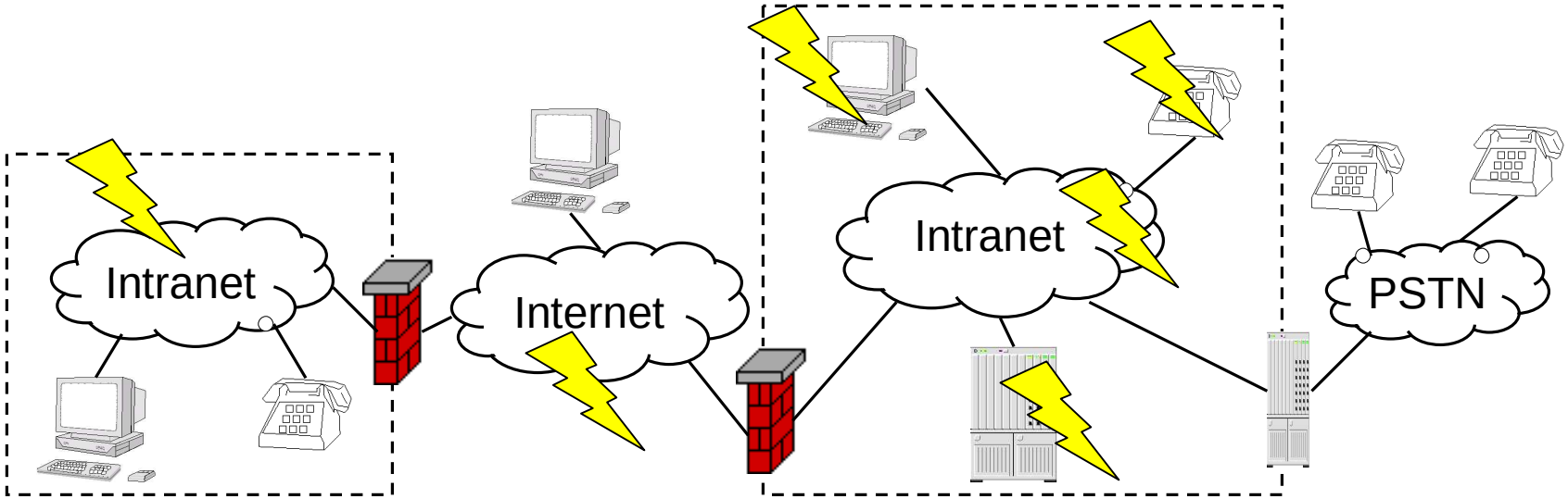
RIAA Defacement

- Betroffen: RIAA Web-Seite
  - Installation illegaler Musikdateien
- Ursache
  - Elementarer Fehler im Konzept
  - **`robots.txt`** enthält Pfad zu Admin-Schnittstelle
  - Admin-Schnittstelle ohne Passwort
- Fazit
  - Falsche (oder keine) Konfiguration
  - Sicherheitsmechanismen nicht genutzt

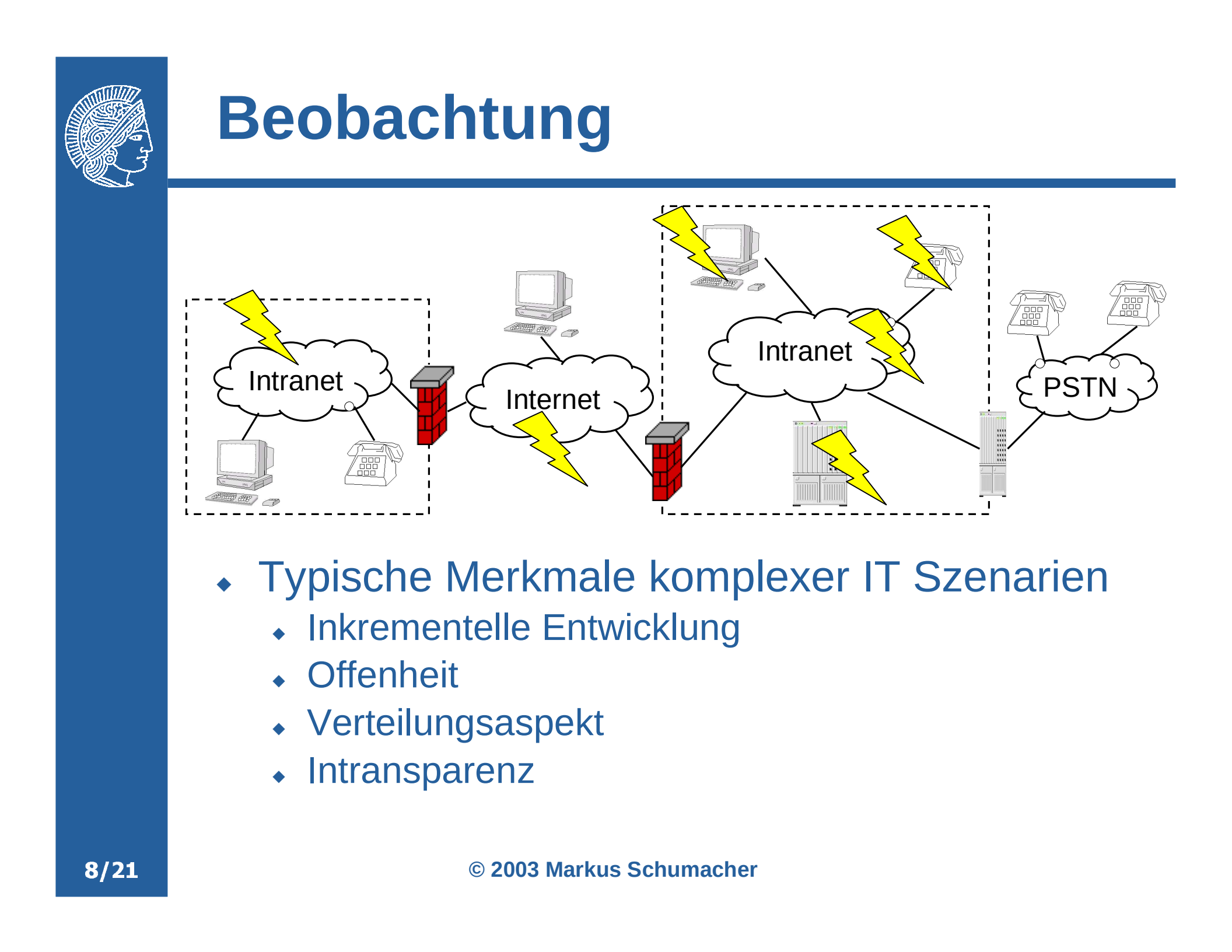
Wireless LAN “Feature”

- Betroffen: Diverse WLAN Accesspoints
  - WEP Keys
  - Passwort
  - MAC Filter
- Ursache
  - Testroutine (oder Wartungsroutine) in OEM Chip
  - Broadcast an UDP Port 27155
  - Payload **`gstsearch`**
- Fazit
  - Security by Obscurity? Fehler bei Freigabe?
  - Falsches Sicherheitsgefühl
  - System nicht verlässlich

Fallstudie IP Telefonie



- Schwache Passwörter
- Denial-of-Service
- Imitation
- Lauschen



Beobachtung

- Typische Merkmale komplexer IT Szenarien
  - Inkrementelle Entwicklung
  - Offenheit
  - Verteilungsaspekt
  - Intransparenz

Fazit

- Situation
  - Problemraum nicht mehr überschaubar
  - Immer wieder *bekannte* Schwachstellen
  - Sicherheit wird zweitrangig behandelt
- Nur *erfahrene* Experten können
  - Zuverlässig Schwachstellen aufdecken/abwenden
  - Systeme mit *guter* Sicherheit entwerfen/betreiben
- Problemstellung
  - Analyse & Konstruktion sicherer Systeme
  - Nutzung von Expertenwissen

Lösung: Pattern-Ansatz

- Patterns beschreiben bewährte Lösungen von wiederkehrenden Problemen in bestimmten Situationen
- Patterns erfassen die kollektive Erfahrung von qualifizierten Experten
- Patterns fördern optimale Verfahren

Übertragen des Pattern-Ansatzes auf Sicherheitsprobleme

Pattern Elemente

Symmetric Encryption

Alice and Bob want to exchange large amounts of data over a public network such as the Internet.

How to prevent data from being eavesdropped?

Public encryption algorithms are widely tested and usually they are crypt-analyzed. On the other hand, secret algorithms aren't more secure; they can (and usually will) be reverse engineered.

Symmetric cryptography is more efficient than asymmetric cryptography in the means of key length and the usage of resources.

Encryption will cost you. Encryption must not be more expensive than the value of the data being encrypted.

Therefore, Alice and Bob use a public symmetric algorithm for encrypting data.

They need much less CPU power with symmetric than asymmetric encryption. Alice uses some keying material to encrypt all data before transmission. Bob decrypts the data at the other end after receipt.

Next patterns: KEY GENERATION and SECURE KEY EXCHANGE

Name

Kontext

Problem

Lösung

Verwandte Patterns

Weitere Elemente

- Enterprise Patterns
  - Prozessdiagramme
  - Organigramme
  - Aktivitätsdiagramme
- Designs Patterns
  - Sequenzdiagramme
  - Klassendiagramme
- Idioms
  - Quelltextbeispiele

Sichere Systeme mit Patterns

- Sicherheit ist nicht-funktional
- Abwesenheit von Sicherheitsfehlern nicht nachweisbar
- Add-on Sicherheit funktioniert nicht
- Prinzip Hoffnung funktioniert nicht
- Viele, nicht integrierte Konzepte

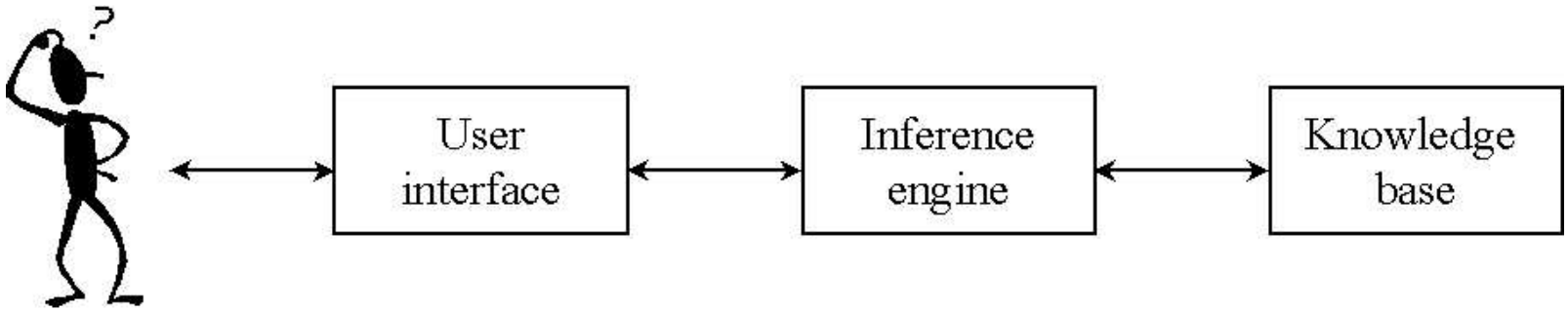
Sichere Systeme mit Patterns

- Herausforderungen
  - Schwerpunkt bisher: überwiegend Notation
  - Suchen & Verwenden von Security Patterns
  - Integration Struktur und Abstraktionsgrad

- Potential für Anwender
  - Was sind die grundsätzliche Probleme?
  - Typische Anforderungen?
  - Anwendbarkeit der Lösung?
  - Konsequenzen einer Lösung?
  - Welche Neben- und Fernwirkungen?

www.securitypatterns.org

- Portal für Security Patterns
  - Ermöglicht semantische Suche
  - Integration aller bekannten Security Pattern
  - Mailingliste
  - Kontakte zu den Peer-Experten
  - Launch: Q3/2003



Administration

- Sicherheitsontologie
  - Kontext (Schicht, Zeit, etc.)
  - Problem (Bedrohung, Angriff)
  - Lösung (Gegenmaßnahmen)
- Annotation
- Anfragen an Wissenbasis
- Inferenzregeln

Dokumentation

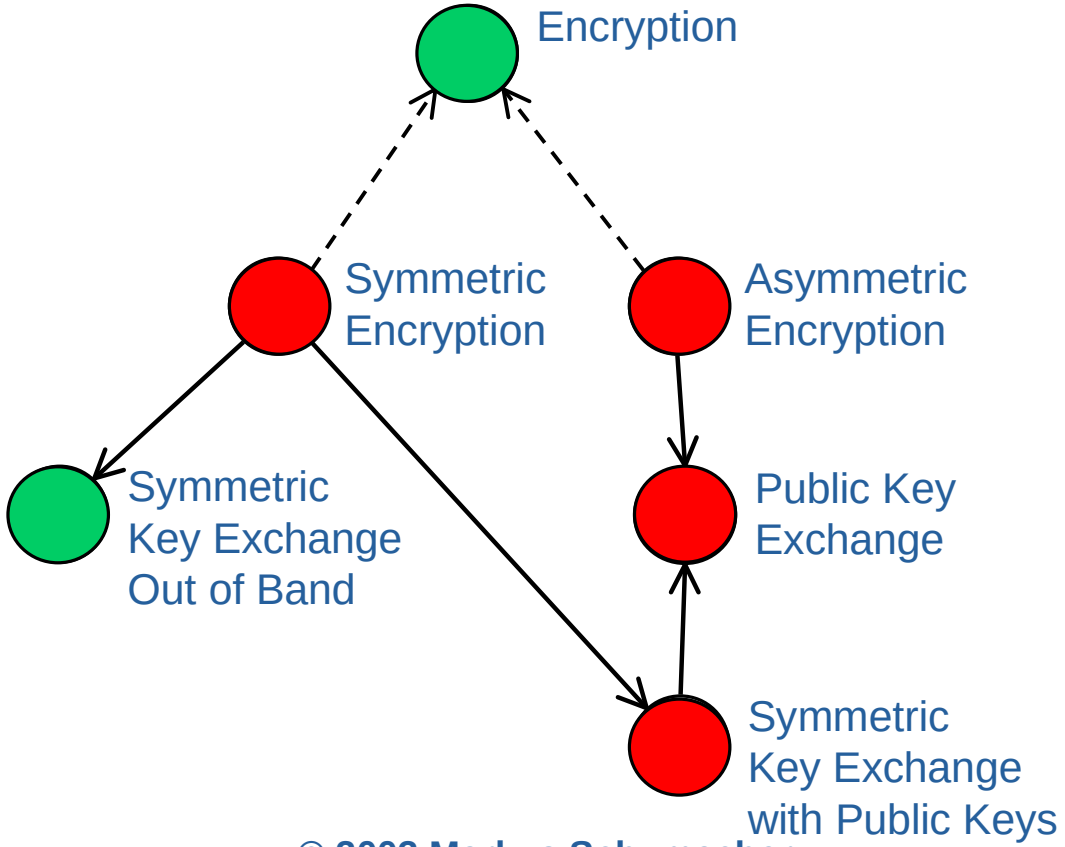
- Qualitätssicherung von Experten durch (Pattern-) Experten
- Shepherding
  - Erfahrener Autor hilft Neulingen bei der initialen Dokumentation (Format, Konventionen, Inhalt).
- Writer‘s Workshops
  - Disskussion im Kreis anderer Experten
  - Fachliche Korrektheit?

Nutzung: gezielte Suche

- Anfrageparameter Begriffe aus Ontologie
  - Kontext/Problem → allgemeiner/spezieller
  - Gegeben Angriff x → Suche Probleme
  - Gegeben Kontext x → Suche Probleme
  - Gegeben Kontext x, Problem y → Suche Lösung
  - Gegeben Lösung x → Suche Alternativen
- Anfrageparameter aus Pattern System
  - Gegeben Pattern X → allgemeiner/spezieller
  - Gegeben Pattern X → abhängige Patterns
  - Gegeben Pattern X, Y → Qualitativer Vergleich

Nutzung: Fehlersimulation

- Allgemein → speziell
- Vorausgesetzt → abhängig



Zusammenfassung & Ausblick

- Neuer Sicherheitsansatz

→ Strukturierte Lösung bekannter Sicherheitsprobleme

- Beiträge
  - Security Patterns
  - Modell für Sicherheitswissen
  - Analytische und konstruktive Nutzung

- Ausblick
  - Ergänzung herkömmlicher Sicherheitsansätze
  - Werkzeugunterstützung im Entwurfprozesses
  - Vervollständigung der Pattern-Sammlung
  - Adaption auf weitere Wissensdomänen

Kontakt

Dr. Markus Schumacher

TU Darmstadt
Fachbereich Informatik
IT Transfer Office (ITO)
http://www.ito.tu-darmstadt.de

ms@ito.tu-darmstadt.de
+49 6151 16 62 15 (fon)
+49 6151 16 62 28 (fax)