Security and Privacy Challenges in the Smart Grid User Domain

Prof. (FH) DI Mag. Dr. Dominik Engel
Josef Ressel Center for
User-Centric Smart Grid Privacy, Security and Control
Fachhochschule Salzburg

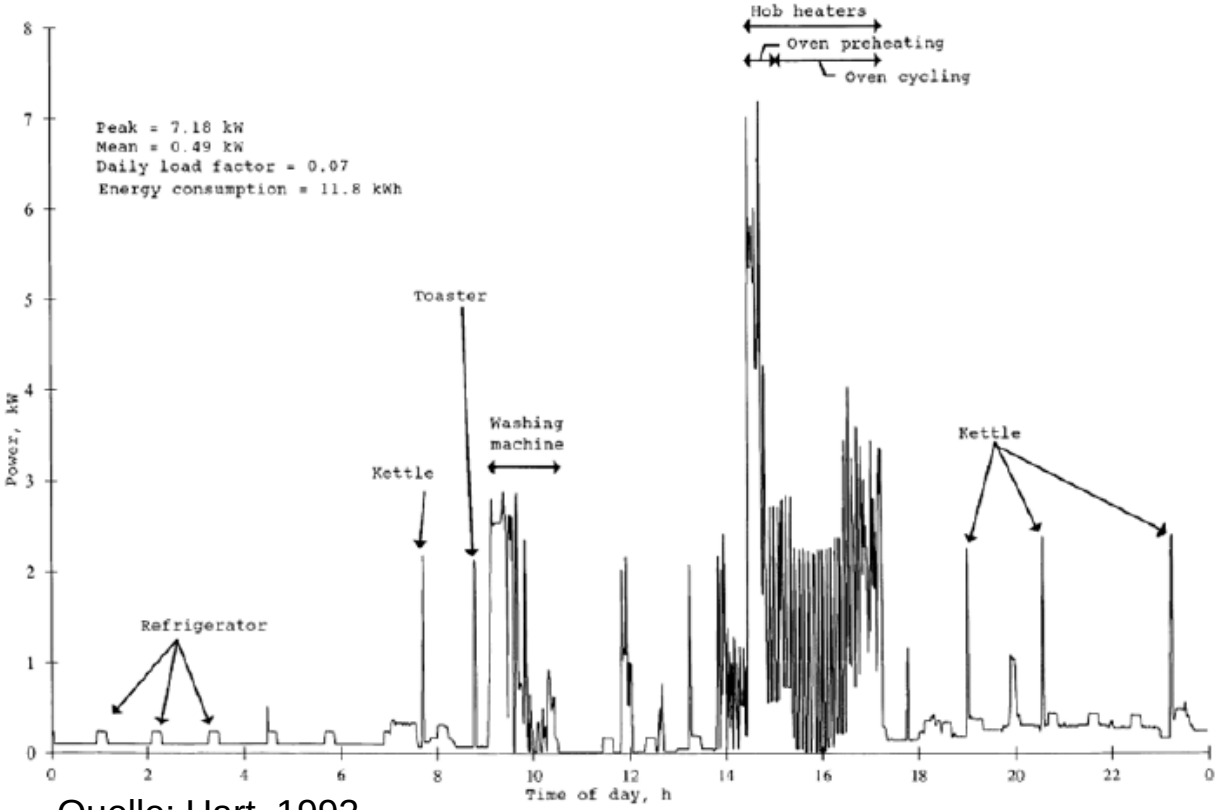
Herausforderungen

I. PRIVATSPHÄRE UND DATENSCHUTZ

II. IT-SECURITY

III. BENUTZERAKZEPTANZ

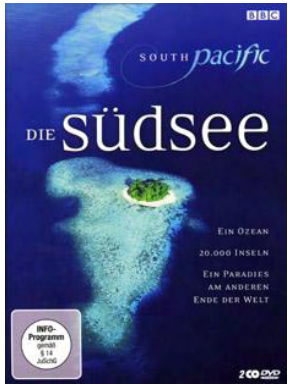
Privatsphäre

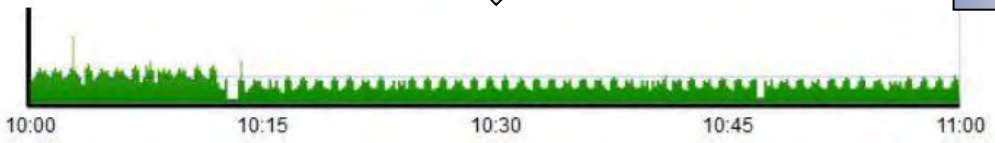


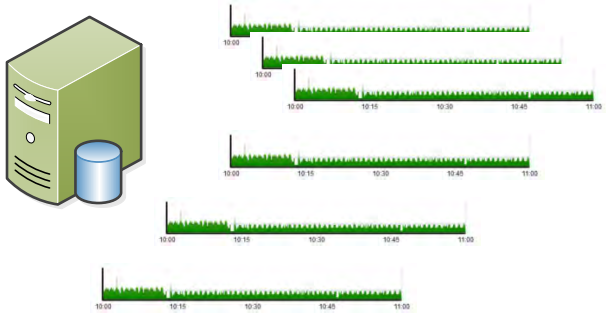
Quelle: Hart, 1992

Quelle: Wikipedia Commons

Laborversuch: Fernsehprogramm





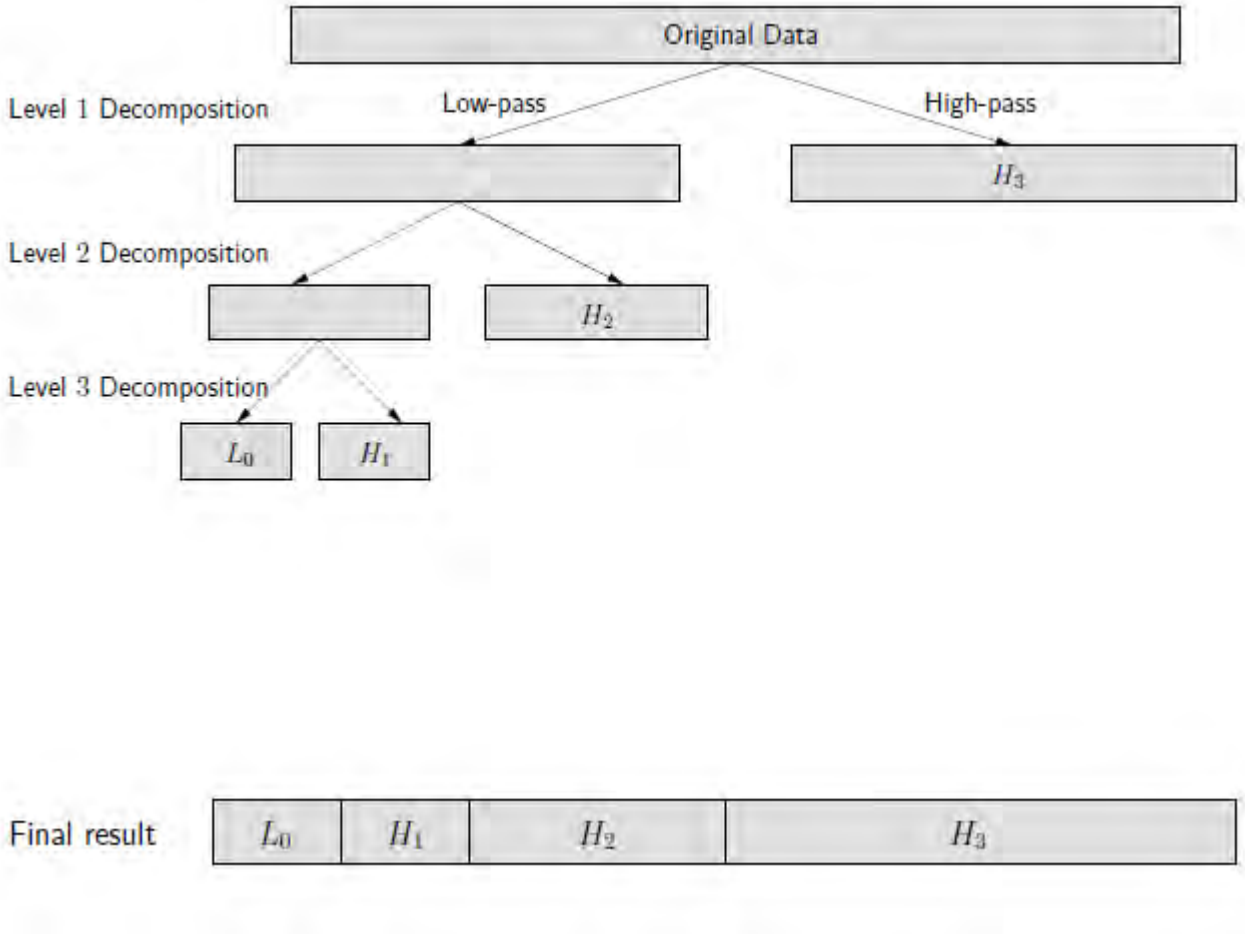


Quelle: Greveler, 2012

Herausforderungen Privacy

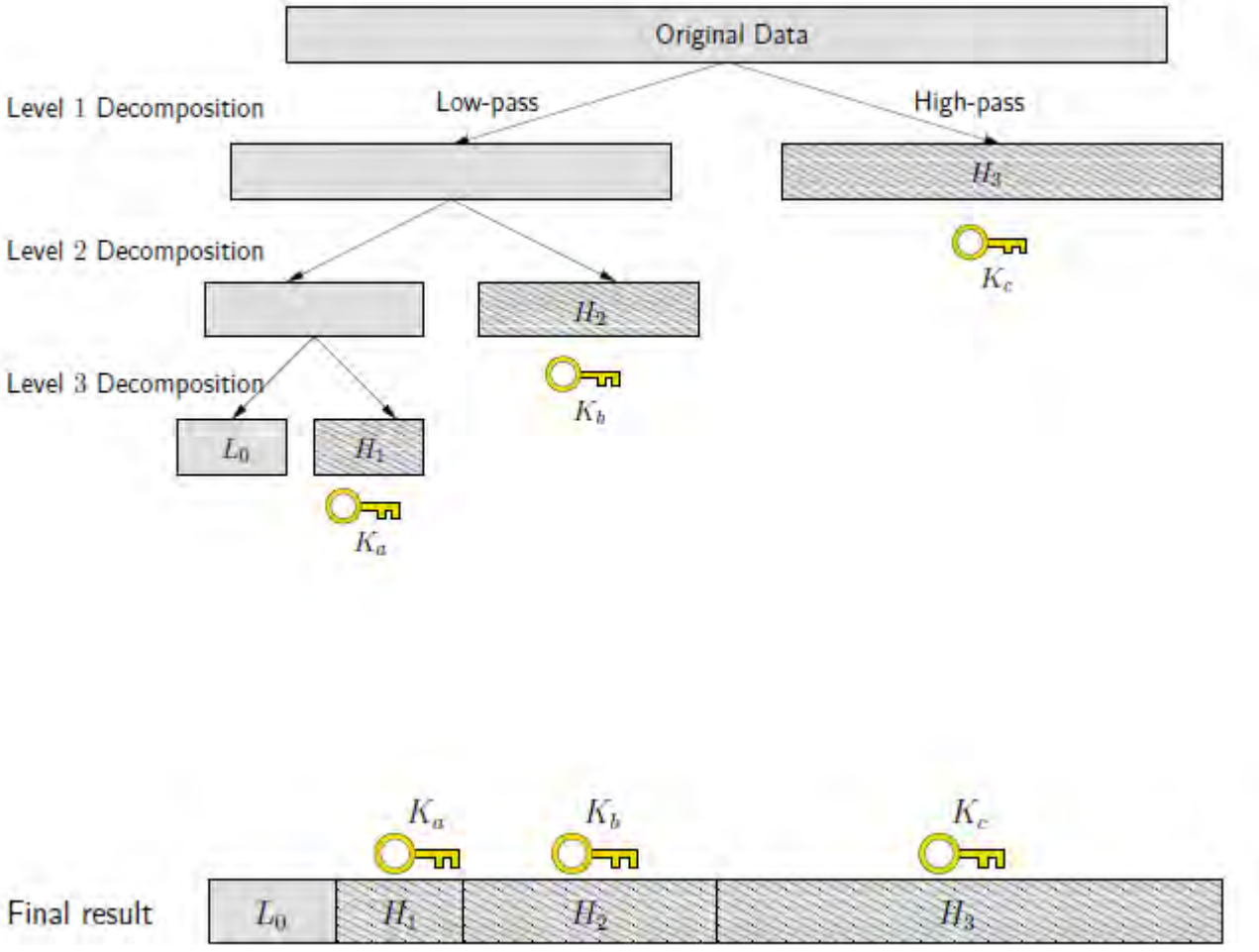
- Welche persönlichen Daten sind bei welcher Auflösung tatsächlich erschließbar?
- Welche Daten ist der Benutzer bereit weiterzugeben und zu welchen Bedingungen? (*user-managed privacy*)
- Wie kann der Benutzer umfassend informiert werden welche Daten wo verwendet werden? (*information transparency*)
- Wie kann eine Balance zwischen Funktionalität und Datenschutz erreicht werden?

Lösungsansatz:
Multi-resolution Representation



Quelle: Engel, 2013

Conditional Access

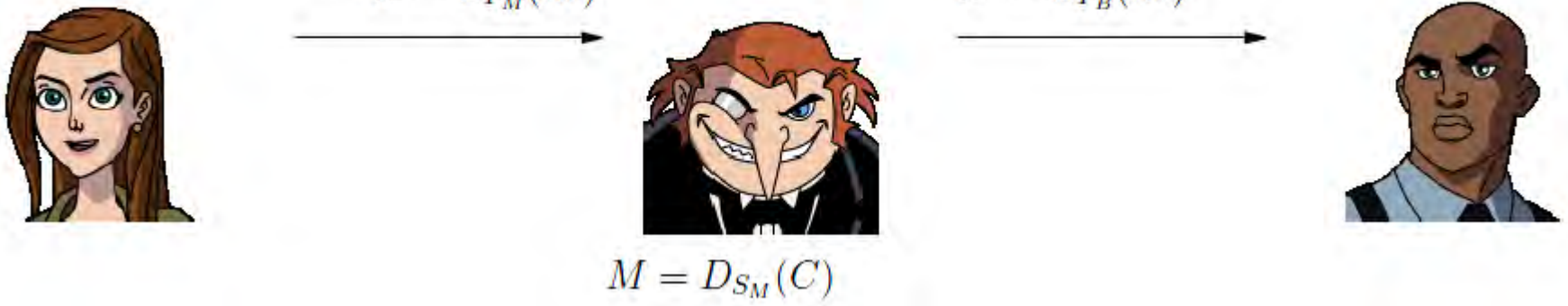


Quelle: Engel, 2013

Herausforderungen im Bereich Security

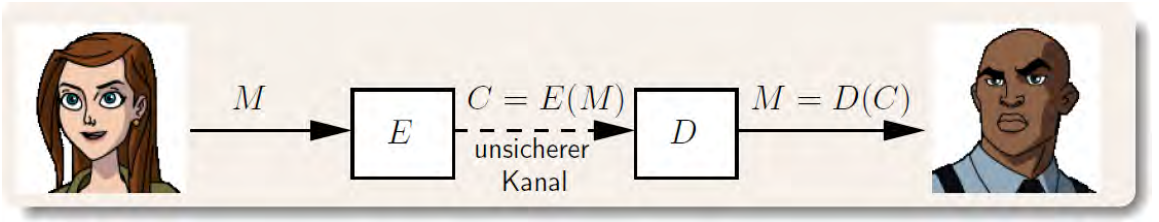
- „Remote Off-Switch“ – Fernwirkausschaltung auf jedem Smart Meter aktiv
  - Oft nicht abgesichert
  - Angedacht: Schnittstelle zu Smart Home
- Man-In-The-Middle Attacken
  - Gefälschte Datenströme
- Unerkannte Angriffe

Man-In-the-Middle Attacke

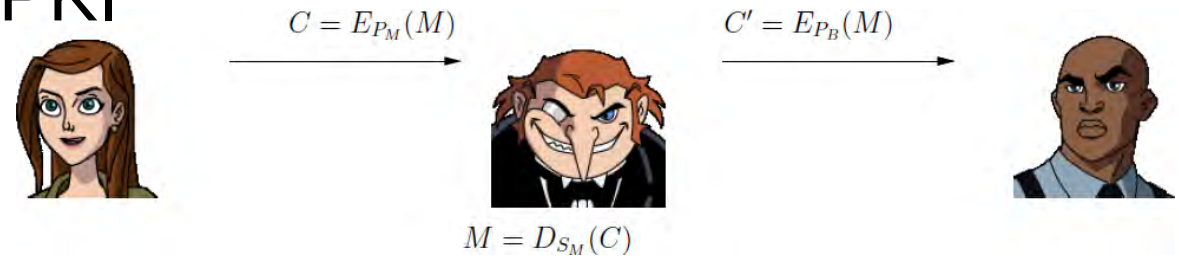


Anforderungen Smart Grid Security

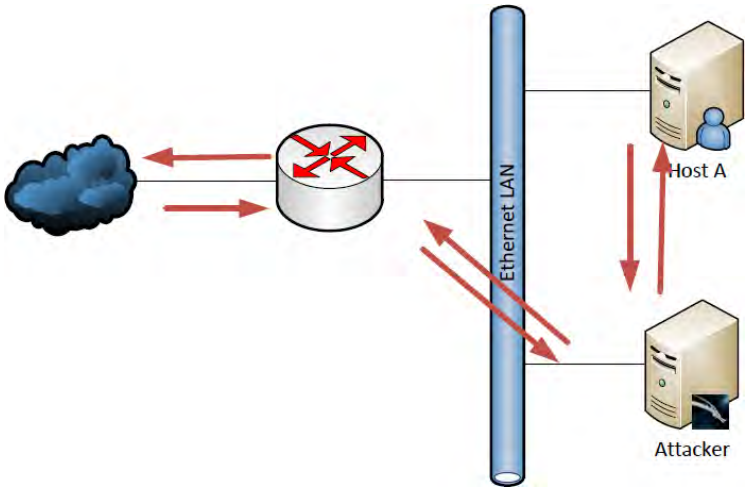
- Verschlüsselung



- Authentifizierung, PKI



- Integrität
- Intrusion Detection

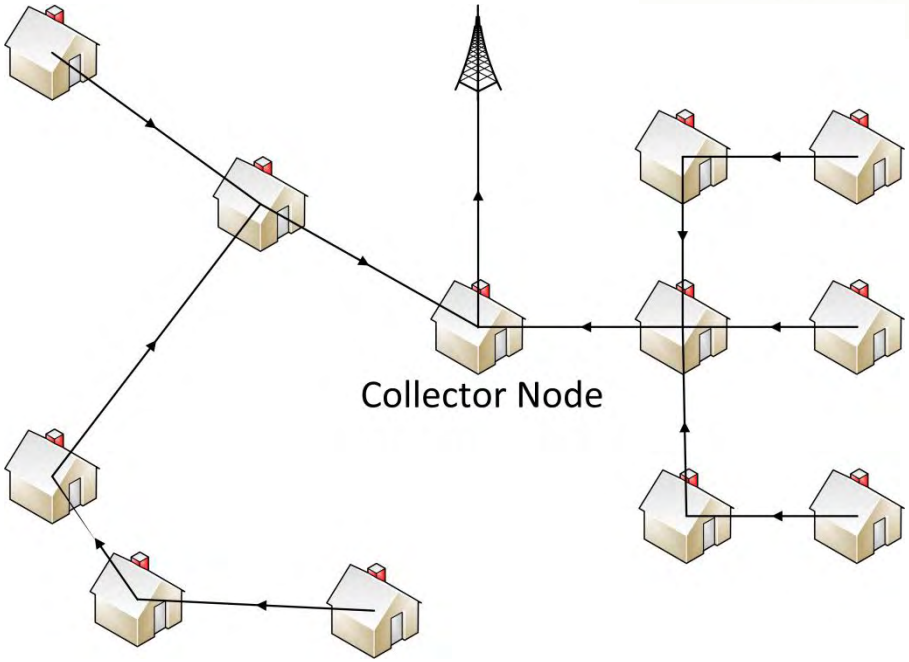


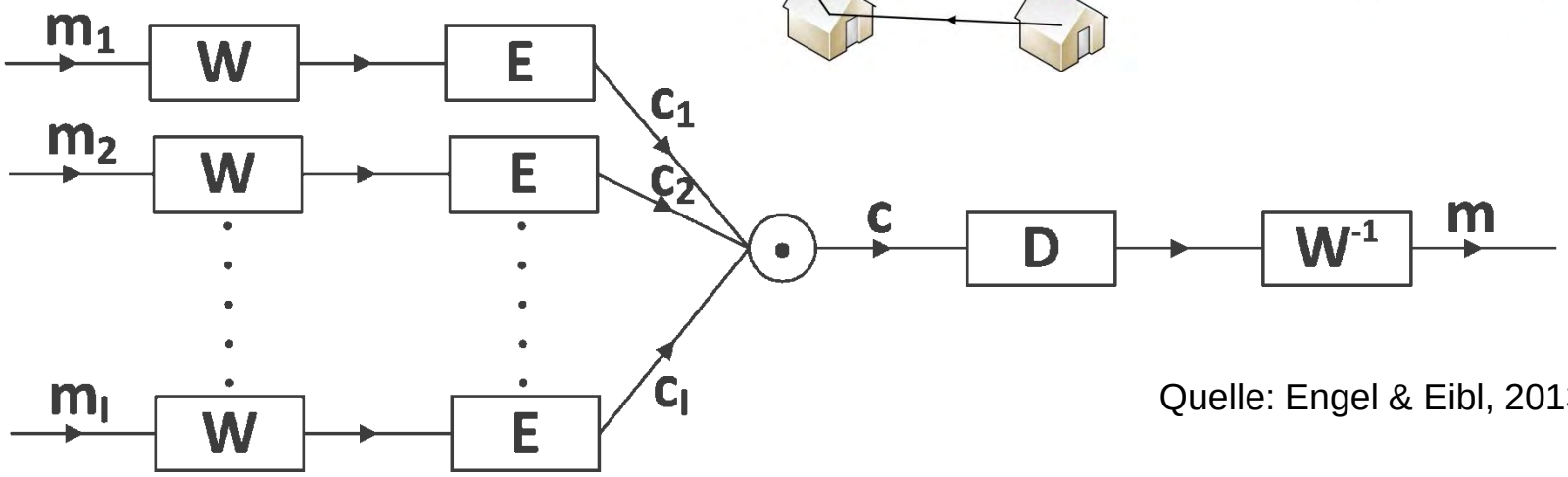
Herausforderung Verschlüsselung

- Geeignet für low-cost Hardware, trotzdem sicher
- Key revocation?
- „Privacy-aware“

Lösungsansatz: Homomorphe Verschlüsselung

- Aggregation im verschlüsselten Zustand möglich

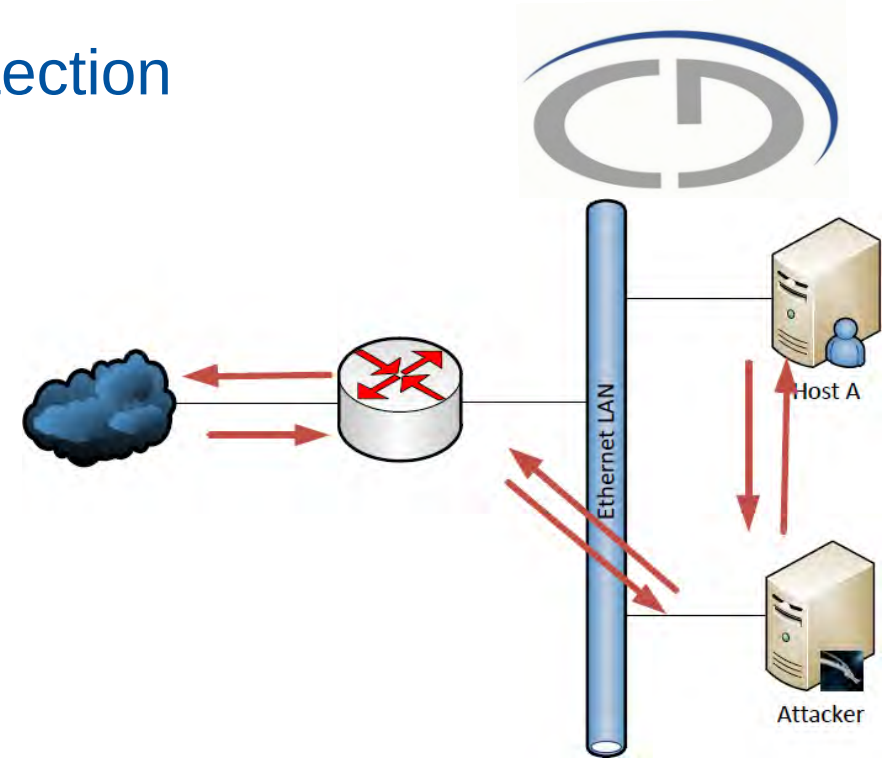




Quelle: Engel & Eibl, 2013

Herausforderung Intrusion Detection

- Kostenfaktor
- Finden der „Base-line“
- Fehlalarm
  - Geringe Wahrscheinlichkeit für Attacke
  - Sehr viele Messdaten
  - > brauche extrem hohe Genauigkeit



Beispiel „Base-Rate Fallacy“

IDS-Tests: 99% Genauigkeit

100.000.000 Messdaten

Attacken: ~ 100

False Positives: 1.000.000

→ p(keine Attacke|Alarm) ~ 99,99%

Herausforderung Datenintegrität

- Vertrauen in beide Richtungen
- Tamper resistance notwendig
- „Trusted Computing“ immer schwierig

Conclusio

- Security und Privacy sind notwendige Voraussetzung für Benutzerakzeptanz
- Technische Lösungen existieren, Ansätze zur Adaption vorhanden
- Wohl größte Herausforderung: „User Awareness“