

Embedded Security — Mehr als Kryptografie und TPM

Dr. Reinhard Schwarz, Fraunhofer IESE (Kaiserslautern)



ÜBERSICHT

- Unterschiedliche Security-Kulturen bei ES und IS
- Verschwimmende Grenzen — Neue Herausforderungen
- Forschungs- und Entwicklungsbedarfe

EINGEBETTETE SYSTEME — ÜBLICHE SICHTWEISE

- Funktion als wesentliches Asset
 - Sensorik /Aktorik
 - Daten Mittel zum Zweck: moderater Zustandsraum
- Hardware-dominiertes Design
 - Hardware als wesentlicher Kostenfaktor
- Geschlossene Architektur, tiefe Systemverankerung
 - Überschaubare Angriffsfläche
 - Betrieb ohne Nutzerintervention
 - Wenige dynamische Anpassungsmöglichkeiten

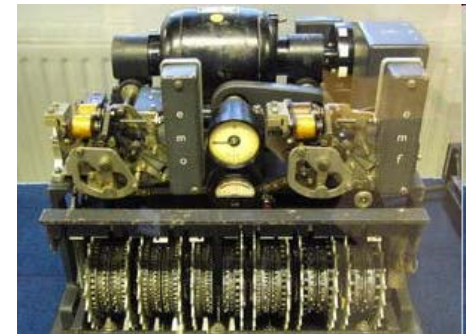
ES SECURITY BISHER: EHER SICHERHEITSMECHANISMEN

Vorherrschende Security-Funktionen:

- Ressourcenschonende Kryptographie
- Vertrauenswürdige Hardware-Module
- Sichere Zufallszahlen
- Sichere Datenerfassung (z.B. Fahrtenschreiber)
- Zugangs- und Zugriffsschutz, Diebstahlsicherung
- Sichere Komponentenidentifikation, Konterfei-Abwehr



Kryptografie als Schlüsseltechnologie



ANGRIFFSSICHERHEIT EINGEBETTETER SYSTEME?

- Oft eher Safety als Security der Realisierung im Blick
 - Korrekte, ausfallsichere Implementierung der Security-Mechanismen
 - Ausreichende kryptologische Sicherheit (z.B. Schlüssellänge)

Security-Mechanismen + Safety = Security ?



SECURITY-KULTUR IN DER ES-ENTWICKLUNG

- Fokus auf Sicherheit als Mechanismus
 - Security als Menge funktionaler Merkmale
 - Abwehr von Fehlfunktion und Funktionenmissbrauch
- Security by Design
 - Kein Nachbessern, keine Sicherheitsadministration im laufenden Betrieb
 - Security als Produkt
- Security als Mittel zur Safety
 - Eher Korrektheit/Robustheit als umfassende Angriffssicherheit
 - Eingeschränkte Bedrohungsszenarien: eher technisch als geschäftlich

INFORMATIONSSYSTEME — ÜBLICHE SICHTWEISE

- Information als wesentliches Asset
 - Umfangreiche Daten: sehr großer Zustandsraum
- Software-dominiertes Design
 - Jedes IT-System als individuell konfiguriertes Unikat
 - Flexible Anpassungen an individuelle Einsatzkontexte
- Offene Architektur
 - Reichhaltige Nutzerschnittstellen
 - Große Angriffsfläche
 - Kontinuierliches Adaptieren an sich wandelnde Anforderungen

IS SECURITY: ABSICHERUNG VON SYSTEMEN

- Bedrohung auf allen Ebenen
 - Anwendung: Anforderungen, Entwurf, Implementierung
 - Betriebsplattform: z.B. Konfigurationsmängel
 - Betreiber und Nutzer: z.B. Social Engineering
 - Geschäftsmodell: z.B. Missbrauch von Vertragskonditionen
- ➔ Erfordert umfassende Bedrohungsanalyse entlang des Lebenszyklus
- ➔ Kryptografie nur ein Aspekt unter vielen

SECURITY-KULTUR IN DER IS-ENTWICKLUNG

- Fokus auf Sicherheit als Eigenschaft
 - InfoSec: Vertraulichkeit, Integrität, Nichtabstreitbarkeit ...
 - Abwehr von Unterwanderung

 - Security on Demand
 - Plattform- u. Perimeter-Schutz kompensiert Applikationsmängel
 - Stetiges Nachbessern: Sicherheitsadministration im laufenden Betrieb
 - Risiko-basierter Security-Ansatz
 - Security als Prozess

 - Umfassende Security
 - Komplexe logische Bedrohungsszenarien: technisch und geschäftlich
-

VERGLEICH DER SECURITY-KULTUREN

- Asset: Technik und Umwelt
 - Fokus: Funktionssicherheit
 - Security **für** Systeme
 - Analyse-Ebene: Komponente
 - Einmalige Security-Analyse
 - **Security als Produkt**
 - Integritätsverletzung, Missbrauch
 - Überschaubare Angriffsfläche
 - Krypto-/hardware-lastiger Schutz
 - **Gewissheits-Kultur**
- Asset: Information
 - Fokus: Informationssicherheit
 - Security **von** Systemen
 - Analyse-Ebene: System
 - Kontinuierliches Security Mgmt.
 - **Security als Prozess**
 - Logische Unterwanderung
 - Komplexe Angriffsfläche
 - Umfassender logischer Schutz
 - **Risiko-Kultur**

ES / IS — VERSCHWIMMENDE GRENZEN

■ Eingebettete Systeme

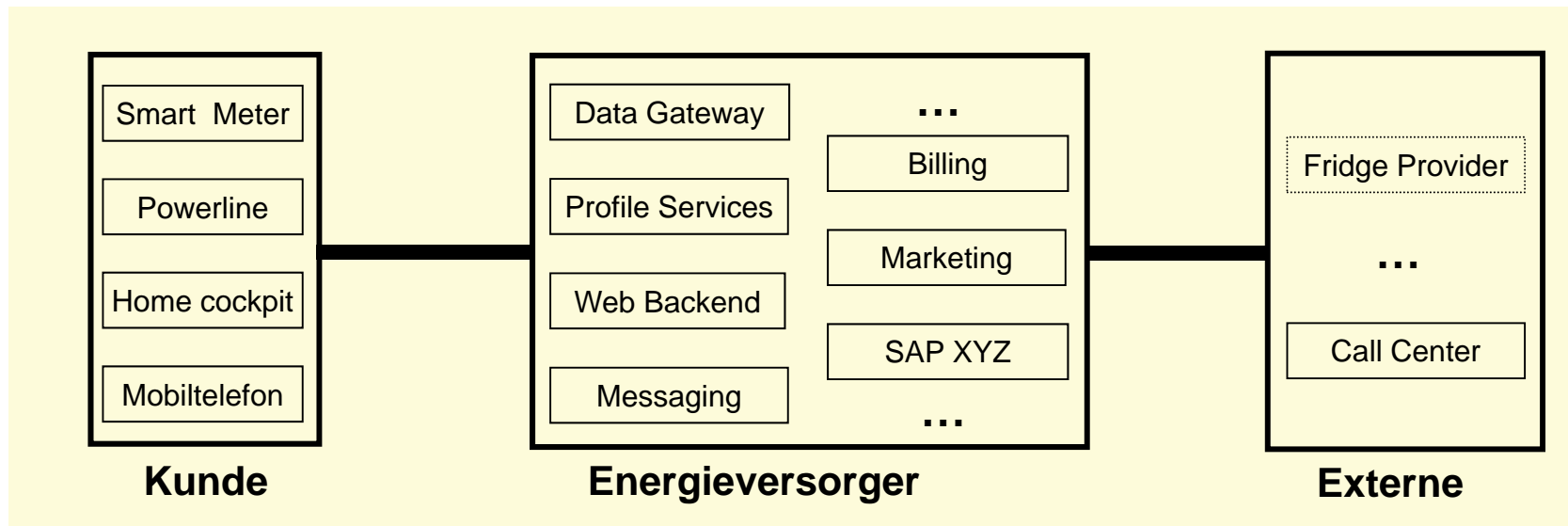
- Zustandsraum immer komplexer
- Immer mehr sensitive Information Assets
- Immer vernetzter, offener
- Immer häufiger Teil umfassender Informationssysteme

■ Informationssysteme

- Immer mehr ES-Komponenten
- Verlässlichkeit und Verfügbarkeit immer wichtiger
- Nachbessern immer aufwändiger

ES/IS INTEGRATION: SYSTEMGRENZEN UNGEWISS

Smart Metering: Viel mehr als ein manipulationssicherer Stromzähler!



ES ANGRIFFSSZENARIOEN VON MORGEN

- Security-Schwachstellen aufgrund mangelnder Implementierungsqualität
 - Unterwanderung durch Pufferüberläufe, unzureichende Eingabedatenvalidierung ...
 - Hintertüren, Seitenkanäle, ...
- Angriffe auf das logische Geschäftsmodell
 - Unsicher trotz robuster Komponenten
 - Verpflanzen zuvor sicherer ES in unvorhergesehenen Kontext
- Mehrstufige und kombinierte Angriffe auf ES/IS-Verbundsysteme
 - Spoofing + Fishing + physische Manipulation + ...

BESONDERE HERAUSFORDERUNGEN FÜR ES SECURITY

- Keine Nutzerbeteiligung bei Sicherheitsfunktionen
 - Fehlende Interventionsschnittstellen
 - Fehlende Interventionskompetenz
- Ungünstige Realisierungsvoraussetzungen
 - Hardware-getriebener Systementwurf
 - Ressourcenknappheit, Echtzeitbetrieb
 - Unsichere Programmiersprachen
 - Mangelnde Standardisierung der HW/SW-Plattformen

FORSCHUNGS- UND ENTWICKLUNGSBEDARF

Herausforderung: **Einfluss der ES Security auf ES Safety**

- Erweiterte Fehlermodi, Schwachstellen- und Bedrohungsmodelle
- Quantitative Security-Analysen

FORSCHUNGS- UND ENTWICKLUNGSBEDARF

Herausforderung: **Wachsender Bedarf für ES Informationssicherheit**

- Neue Modelle und Mechanismen für Nutzungskontrolle
 - Kontrollbasiert: Unterbinden von Zuwiderhandlungen
 - Beobachtungsbasiert: Strafandrohung bei Zuwiderhandlungen

FORSCHUNGS- UND ENTWICKLUNGSBEDARF

Herausforderung: **Wachsender ES/IS Assurance-Aufwand**

- Integriertes Sicherheits-Engineering
 - Integration Safety / Security Engineering
 - Integration ES / IS Security Engineering
 - Harmonisierte oder integrierte Sicherheitsstandards

- Integrierte Validierungsumgebungen
 - Spektrum spezialisierter Modellierungstechniken
 - Einheitliche Handhabung, Konvertierbarkeit, Kopplung solcher Modelle

FORSCHUNGS- UND ENTWICKLUNGSBEDARF

Herausforderung: **Fehlende Möglichkeit zu ES Sicherheitsintervention**

- [Unbedingte Sicherheit: Verifizierbare Security by Design]

beziehungsweise

- Selbstüberwachung und Selbstheilung (ID[R]S)
 - Dynamisch rekonfigurierte Safety & Security

FORSCHUNGS- UND ENTWICKLUNGSBEDARF

Herausforderung: **Wachsende ES-Komplexität**

- Bessere Darstellung von Security-Merkmalen für »normale« Entwickler

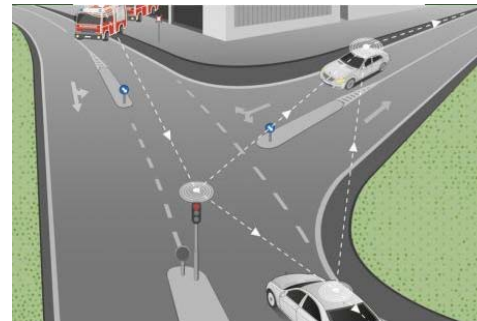
- Kompositionale Security
 - Kombinierbare Security-Entwurfsmuster
 - Inkrementelle Verifikation und Validierung

- Security als Prozess
 - Einplanung von Nachbesserungsmöglichkeiten zur Laufzeit
 - Angepasste ES Security-Prozessreife (BSIMM, SAMM, SSE-CMM)

FORSCHUNGS- UND ENTWICKLUNGSBEDARF

Herausforderung: **Wachsende ES/IS Integration — ES-Perspektive**

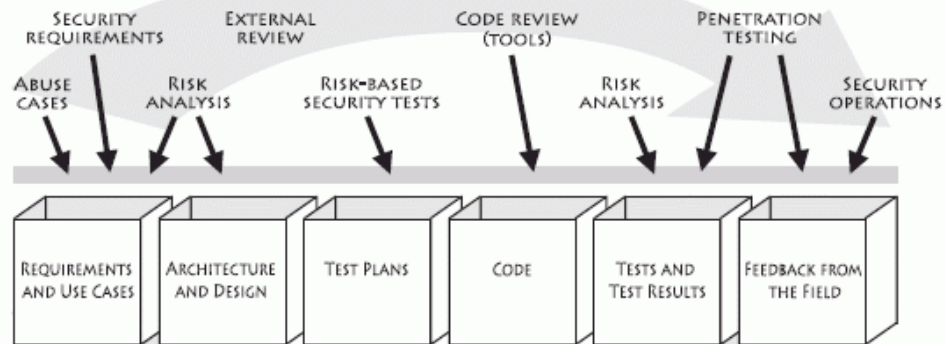
- Stärkere Berücksichtigung nicht-technischer Bedrohungen
- Stärkere Betonung der System- statt Komponentensicht



FORSCHUNGS- UND ENTWICKLUNGSBEDARF

Herausforderung: **Wachsende ES/IS Integration — IS-Perspektive**

- Stärkere Berücksichtigung physischer Schwachstellen
- Produktzentriertere Security Assurance: Security by Design
- Quantitative Security



Quelle: McGraw, Gary, "Software Security", IEEE Security and Privacy, March 2004

FORSCHUNGS- UND ENTWICKLUNGSBEDARF

Herausforderung: **Wirtschaftlichkeit der Security**

- Security Qualitätsmodelle
 - Indikatoren, Metriken für Produkt-Security
 - Aufwandsschätzverfahren, Kosten-Nutzen-Modelle für Security

- Aussagekräftigere Security-Zertifikate und Prüfsiegel
 - Trennschärfere Zertifizierungskriterien (Protection Profiles)
 - Effizientere und effektivere Prüfverfahren und Prüfwerkzeuge
 - Inkrementelles Nachzertifizieren

Fazit

- Status Quo:
 - Bisher unterschiedliche Sicherheitsanforderungen für ES / IS
 - Unterschiedliche Sicherheitskulturen für ES / IS
- Trend: Zunehmende ES/IS-Integration
 - Grenzen verschwimmen
 - Probleme an den Nahtstellen
- Security ist eine nichtkompositionale Eigenschaft des Gesamtsystems
 - Heute: Schwerpunkt auf ES-Komponentensicherheit
 - Zukunft: Systemsicherheit durch Zusammenführen der ES / IS-Kulturen

Danke für Ihre Aufmerksamkeit!

reinhard.schwarz@iese.fraunhofer.de