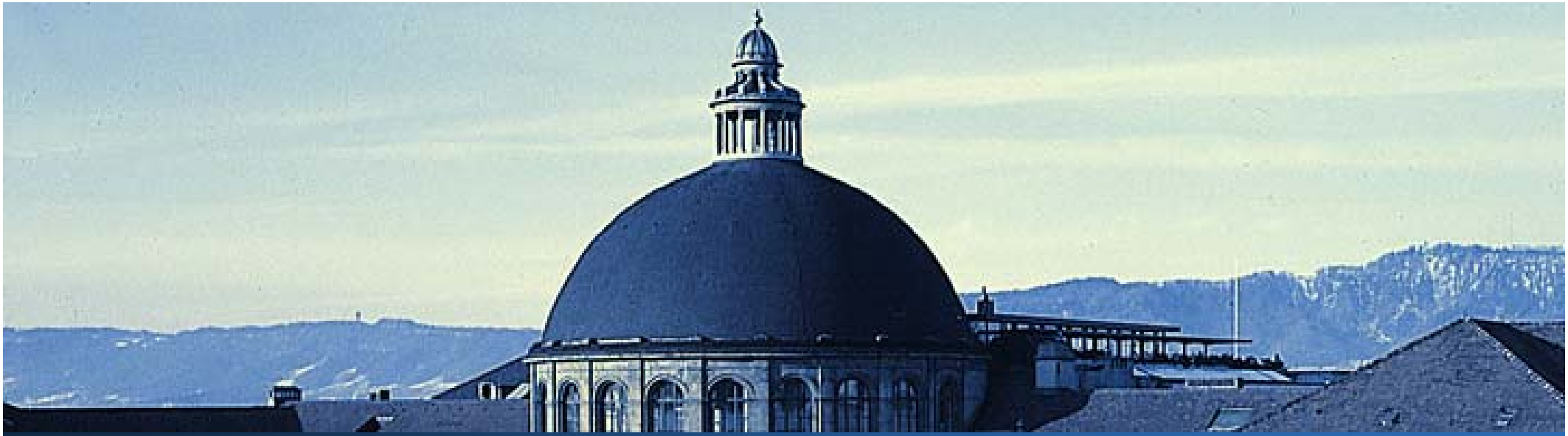
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Fälschungsschutz mit RFID

Dr. Thorsten Staake | D-MTEC IM

FAEL-Seminar, Zürich, 7. November 2007



Vorstellung unserer Forschungsgruppe

- Lehrstuhl von Herrn Fleisch an der Universität St. Gallen und der ETH Zürich

- Forschungsschwerpunkt: Betriebswirtschaftliche Anwendungen des Internets der Dinge

Agenda

- Einführung in das Thema „Produktfälschungen“
- RFID als Sicherheitsfeature: Lösungsansätze und Herausforderungen
- Ausblick

Was versteht man unter Produktfälschungen?

- Als Produktfälschungen werden Güter bezeichnet, die ohne Genehmigung des Rechte-Inhabers geschützte (Erkennungs-)Merkmale tragen.
- Merkmale können sein: Markennamen, Firmennamen, Prüfzeichen, geschützte Designs / Farbkombinationen, etc.

Der Handel mit gefälschten Produkten hat erhebliche Ausmasse angenommen.

- OECD 1998: “5% to 7% of world merchandise trade is in counterfeit goods“.
- Ein weltweiter Mittelwert von 1% ist wahrscheinlicher.
- Diese Korrektur soll aber nicht über die Schwere des Problems hinwegtäuschen.
- Problematisch ist insbesondere die qualitative Entwicklung des Fälschungsmarktes.

Entwicklung der “Fälschungs-Industrie”

Offensichtliche Fälschungen ➔ Zunehmend auch gefährliche “deceptive Counterfeits“

Geringe Produktkomplexität ➔ Zunehmend auch anspruchsvolle Produkte

Schlechte Qualität ➔ Breites Spektrum, auch Produkte mit funktionalem Nutzen

Weitere Trend ➔ Wachsende Bedeutung der Heimatmärkte, Fertigung in grossen Stückzahlen, Arbeitsteilung, effiziente Logistik

Die Folgen sind erheblich.

Bürger:

- Marke als “Qualitätssiegel”
- Marke zur Reduktion von Suchkosten
- Marke zur Kommunikation von Werten

Staat:

- Steuereinahmen
- Arbeitsplätze
- Innovationskraft
- Organisierte Kriminalität

Unternehmen:

- Umsatzverluste (Substitutionseffekte und Preisdruck)
- Beschädigung des Markennamens
- Return on Investment von Entwicklung, Marketing, Qualitätsmanagement
- Marktposition in „emerging markets“
- Lerneffekte der Fälscher
- Produkthaftung
- Kosten für Produktsicherheit etc.

Probleme mit bestehenden Produktschutz-Technologien

- Die meisten Hologramme, Microprintings etc. sind *an und für sich* sicher…
- … aber eine *schlechte* Nachahmung ist meist ausreichend:
  - Kein Zollbeamter oder Kunde kann alle Merkmale kennen
  - Die Zeit für Kontrollen fehlt
- Grosszahlige Test sind erforderlich!
  - Mit etablierten Features nicht machbar
- RFID bietet einige Vorteile:
  - Automatisierte Tests
  - Sicherheitslevel kann angepasst werden
  - Einfaches, stabiles User-Interface

Source: Valerio Reggi, Organisation Mondiale de la Santé

Die Echtheit eines Produktes festzustellen oder zu widerlegen ist in den seltensten Fällen ein Problem – sofern die Zeit und die notwendigen Mittel zur Verfügung stehen.

Prinzipielle Lösungsansätze

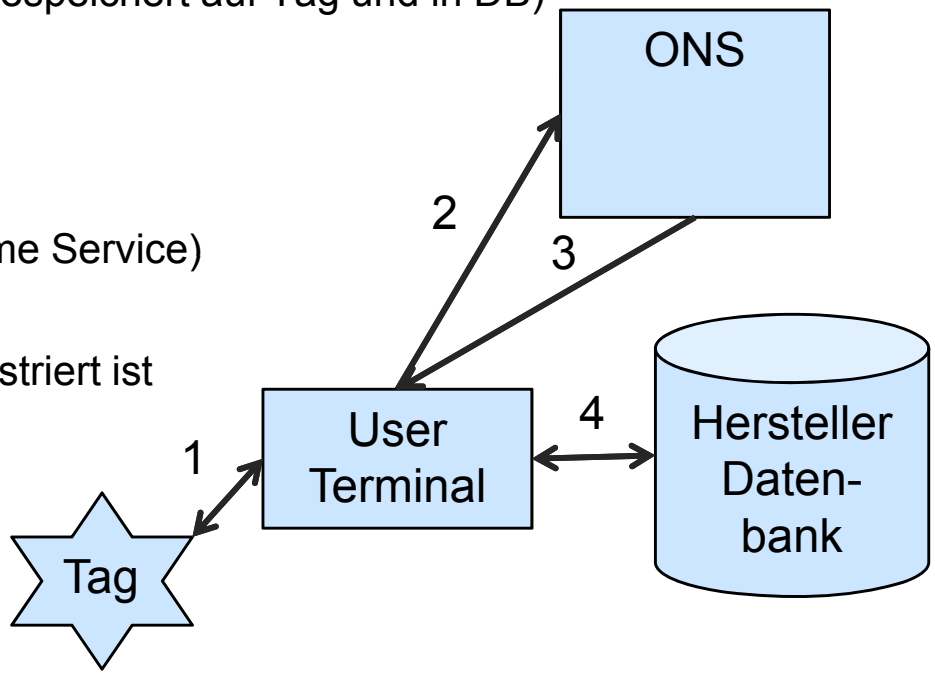
- Unique ID
  - Eindeutige Nummer, in Herstellerdatenbank hinterlegt
- Track & Trace
  - Plausibilitäts-Check über Produkthistorie
- Authentifizierung des Tags
  - Challenge-Response-Verfahren

Allgemeine Eigenschaften:

- Automatisierte Test möglich
- Unterschiedliche Sicherheitsstandards zu unterschiedlichen Kosten
- Existierender Migrationspfad
- Ein stabiles Benutzer-Interface
- Erheblicher Zusatznutzen z.B. zur Verbesserung der Logistik
- Enge Verknüpfung von Tag und Produkt möglich.

Ansatz: Unique ID

- Produktion:
  - Eine zentrale Instanz (z.B. EPCglobal) vergibt Nummernkreise an Hersteller
  - Hersteller verknüpft Artikel mit Nummer (ID) (gespeichert auf Tag und in DB)
- Überprüfung:
  1. Benutzer liest ID von Tag
  2. Benutzer sendet Nummer an ONS (Object Name Service)
  3. Benutzer erhält Hersteller-Adresse von ONS
  4. Benutzer erfragt beim Hersteller, ob die ID registriert ist
- Erforderlich: Authentifizierung der Parteien
- Bemerkungen:
  - Praktikabel auch für grosse Lieferungen
  - Low-Cost Tags
  - Aber: Geringe Sicherheit – Die Nummern können gefälscht oder erraten werden.



Ansatz: Track & Trace

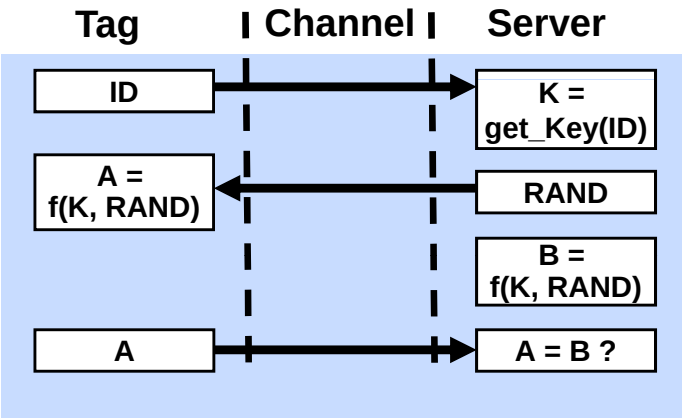
- Die Produkt-Historie wird aufgezeichnet:
  - ID auf Transponder dient als Referenz zum Datensatz
  - Hersteller, Logistikunternehmen, Distributoren etc. vermerken Erhalt, (Dis)-Aggregation, Verkauf, Gebrauch, Entsorgung.
  - Aussage über Echtheit basiert auf Plausibilitätsprüfung der Historie

- Bemerkungen:
  - Low-Cost Transponder
  - Zusätzliche Sicherheit und Zuordnung von Verantwortlichkeiten
  - Zusatznutzen in der Produktion und beim Vertrieb
  - Aber: In einigen Industrien entsteht ein extrem hohes Datenaufkommen
  - Wie mit duplizierten IDs umgehen?
  - Wie sollen die Schreib- und Leserechte zugeteilt werden?
  - Und: Wie soll der Umgang mit den wertvollen Daten gehandhabt werden?

Ansatz: Authentifizierung des Tags

➔ Problemstellung: es soll sichergestellt werden, dass die ID tatsächlich vom Hersteller vergeben wurde.

- Challenge-Response Verfahren:
  - Ein Geheimnis, dass nur der Tag und der Server kennen, wird verglichen, ohne es direkt zu übermitteln.



- Herstellung:
  - Der Server generiert eine ID und ordnet sie dem Tag zu.
  - Tag oder Server generieren einen Schlüssel K, der im Tag und im Server gespeichert wird.
  - Der Tag kann nicht direkt aus dem Tag ausgelesen werden.
- Überprüfung:
  - Lesegerät sendet ID an Server
  - Der Server holt den zur ID gehörenden Schlüssel K aus einer Datenbank
  - Der Server generiert eine Zufallszahl RAND und sendet sie an das Tag (Challenge)
  - Tag und Server berechnen das Ergebnis der Funktion F(K, RAND)
  - Das Ergebnis wird verglichen. Wenn A=B kennt der Tag das zu ID gehörende Ereignis

Ansatz: Authentifizierung des Tags (Fortsetzung)

- Bemerkungen:
  - Sowohl für symmetrische als auch für asymmetrische Systeme geeignet
  - Hardware-Komplexität stark abhängig von Schlüssellänge und Algorithmus
  - Relativ hohe Tag-Kosten (Gate-Count)
  - Relativ hohe Kommunikationskosten (Bulk-Reading etc.)
  - Grössere Anforderungen an die Energieversorgung der Transponder (Lesereichweite)
  - Hohes Sicherheitsniveau
  - Geringerer organisatorischer Aufwand als bei T&T

Eine Demo-Applikation

Phase 1
PDA / RFID Reader

Phase 2
Cell-phone
NFC Reader

Phase 3
Cell-phone
NFC/EPC Reader
EPC Network

Ausblick

- Herausforderungen
  - Prozess-Integration
  - Kollaboration der Akteure (Zoll, Supply-Chain Partner etc.)
  - Kosten
  - Umgang mit Lesefehlern
  - Preis pro Sicherheitsmerkmal vs. Preis pro Check
  - Schutz der Privatsphäre

- Eine persönliche Einschätzung
  - Grosses Potential für viele Produktkategorien
  - Viele organisatorische Herausforderungen insbesondere bei T&T Ansätzen
  - Insellösungen nur in seltenen Fällen wirkungsvoll
  - Kontrolle möglichst durch den Kunden oder den Zoll
  - Auch praktikable Low-Security Lösungen sind effektiv
  - Kontrollen wirken auch als Präventivmassnahmen

Vielen Dank für Ihre Aufmerksamkeit.

Kontakt:

ETH Zurich

Department of Management, Technology, and Economics

Thorsten Staake
Information Management
Sonneggstrasse 63 (SOW F 11)
CH-8092 Zurich

mail: tstaake@ethz.ch
phone: +41 44 632 8919
mobile: +41 76 235 8008
fax: +41 44 632 1045