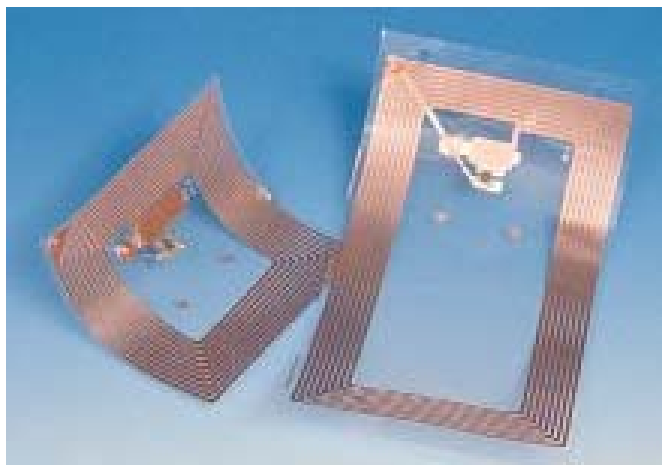
Risiken und Chancen des Einsatzes von RFID-Systemen

RFID – alles sicher?



Prof. Dr. Lorenz Hilty
Abteilung Technologie und Gesellschaft
EMPA, St. Gallen

EMPA

Übersicht

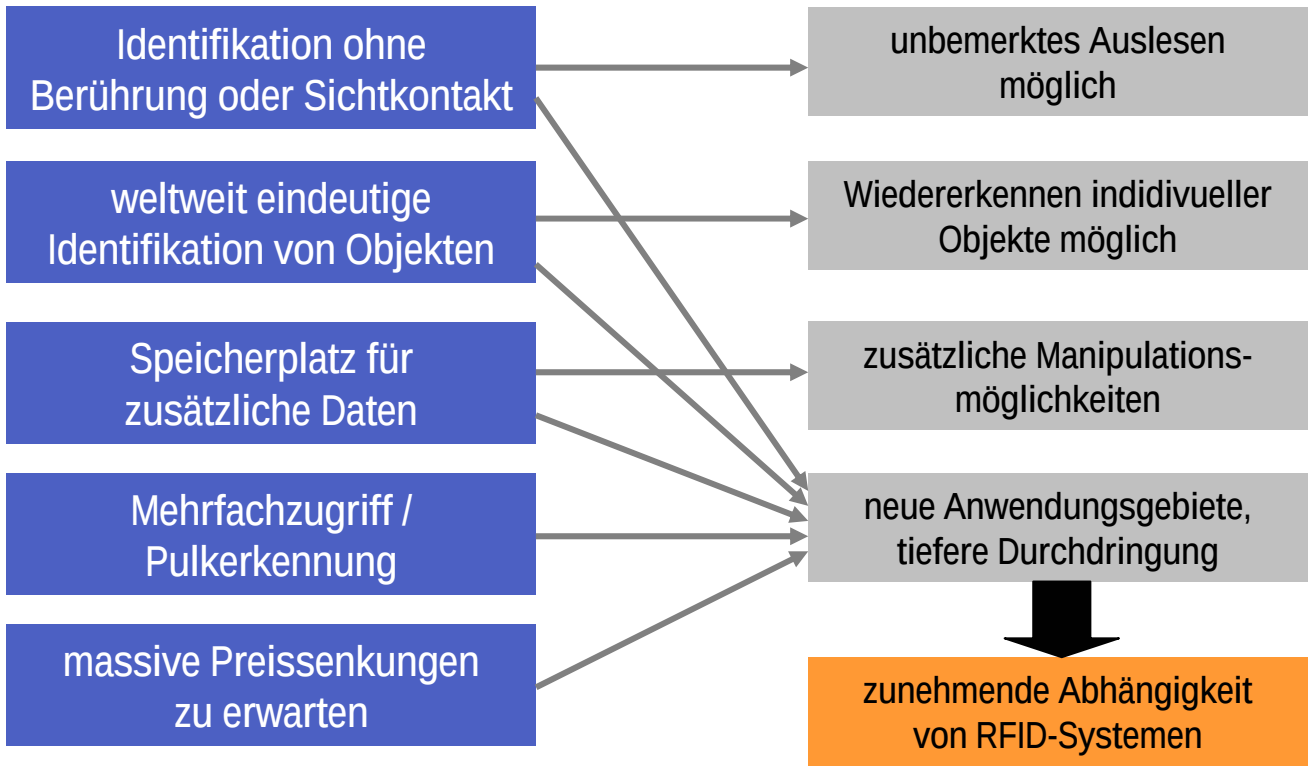
- Problemaufriss
- Bedrohungslage
- Wirksamkeit von Sicherheitsmaßnahmen

EMPA

Problemaufriss

Spezifisch im Vergleich zu anderen ID-Systemen

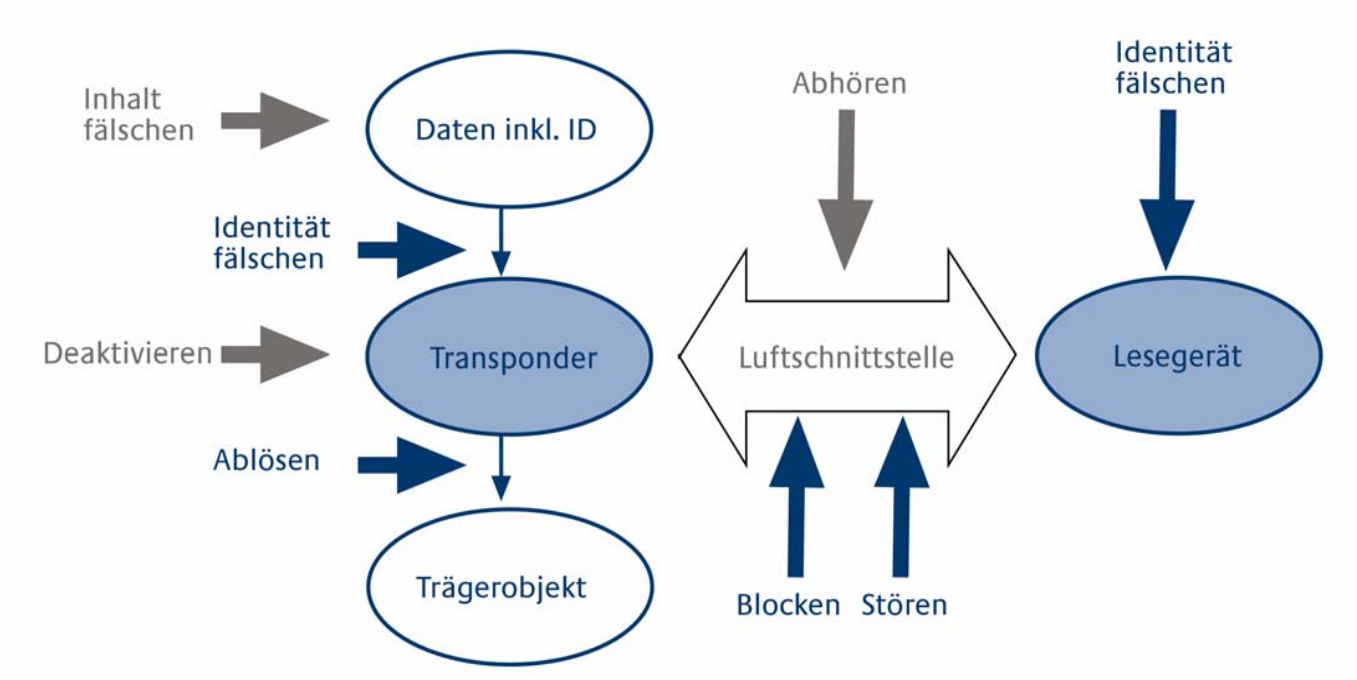
Sicherheitsrelevante Konsequenzen

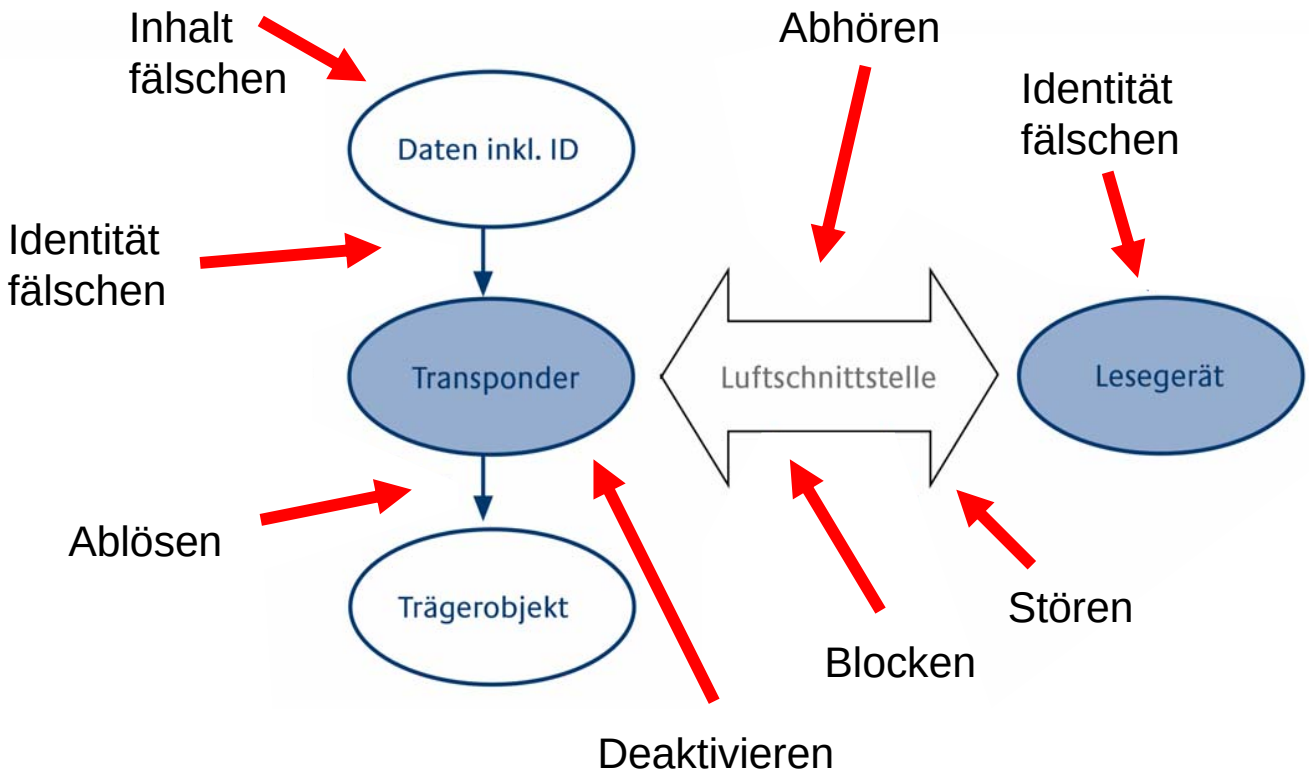


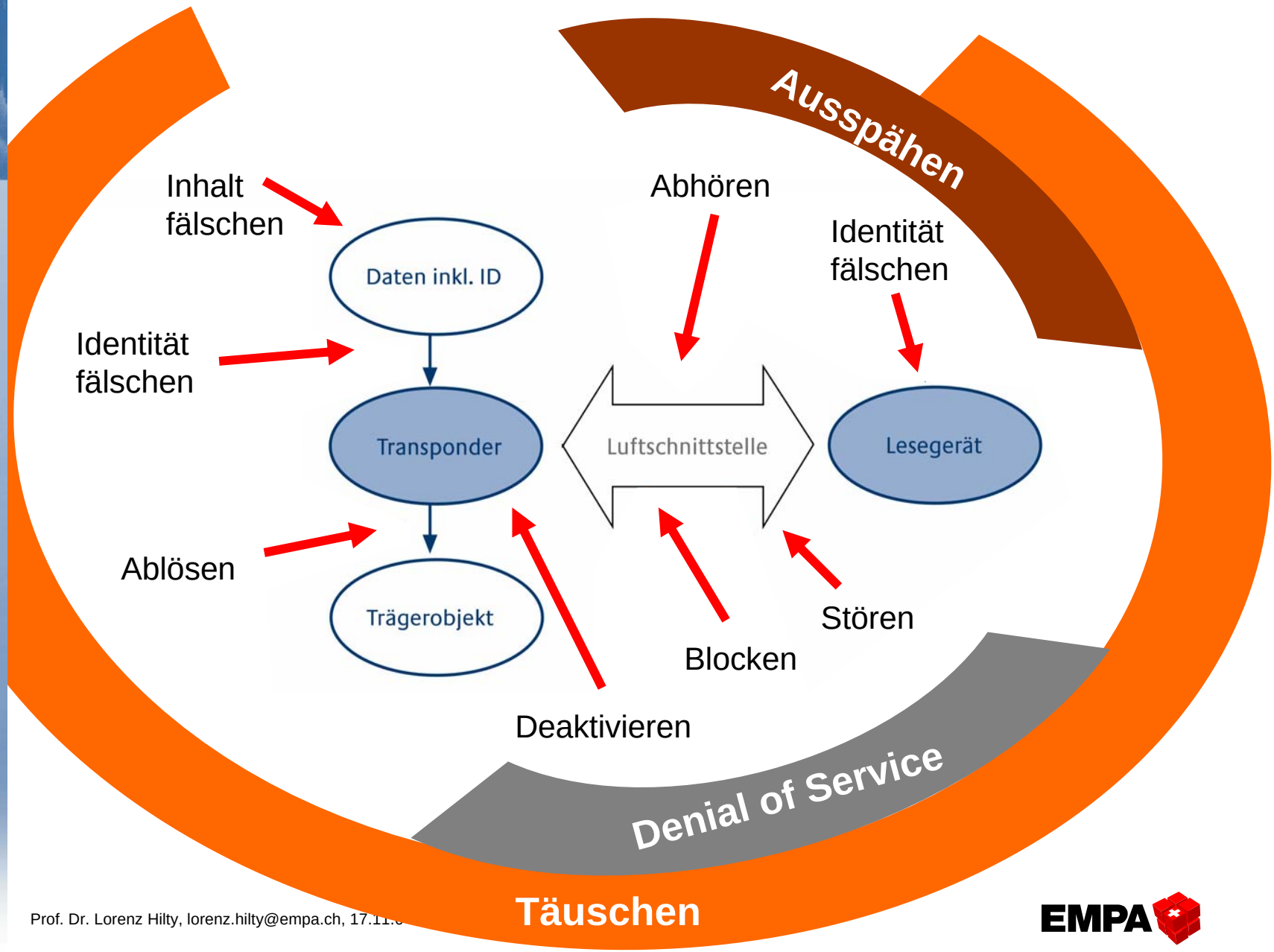
EMPA

Bedrohungslage

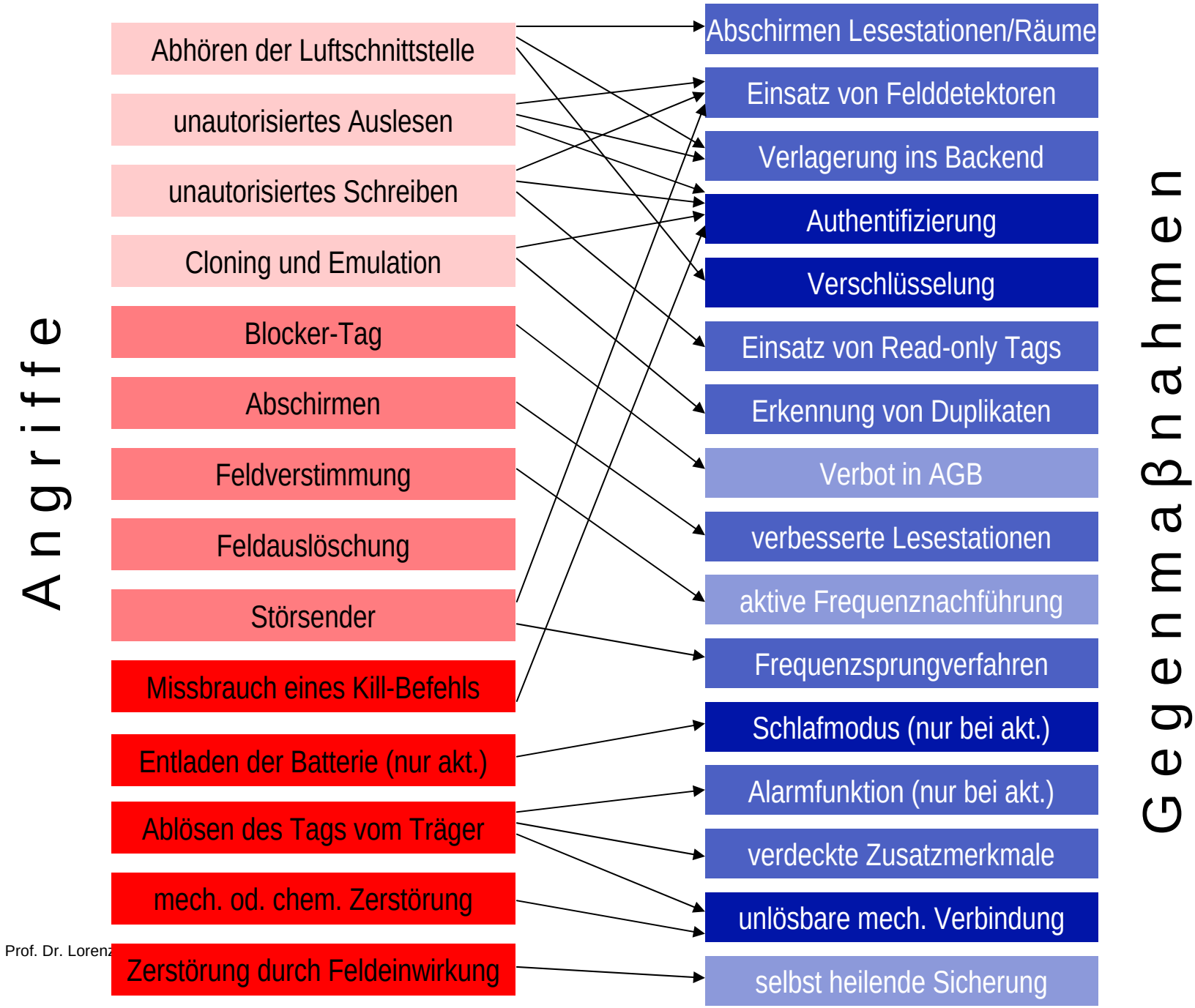
- **Angriffsarten:** Wie kann man ein RFID-System angreifen? (Angriffe, Gegenmaßnahmen)
- **Akteure:** Die Bedrohungslage aus Sicht verschiedener Akteure (aktive Partei, passive Partei)


Inhalt fälschen
Daten inkl. ID
Identität fälschen
Transponder
Deaktivieren
Ablösen
Trägerobjekt
Abhören
Identität fälschen
Luftschnittstelle
Lesegerät
Blocken
Stören


Inhalt fälschen
Abhören
Identität fälschen
Daten inkl. ID
Identität fälschen
Transponder
Luftschnittstelle
Lesegerät
Ablösen
Trägerobjekt
Stören
Blocken
Deaktivieren


Ausspähen
Inhalt fälschen
Abhören
Identität fälschen
Daten inkl. ID
Identität fälschen
Transponder
Luftschnittstelle
Lesegerät
Ablösen
Trägerobjekt
Stören
Blocken
Deaktivieren
Denial of Service
Täuschen

EMPA


Angriffe
Abhören der Luftschnittstelle
unautorisiertes Auslesen
unautorisiertes Schreiben
Cloning und Emulation
Blocker-Tag
Abschirmen
Feldverstimmung
Feldauslöschung
Störsender
Missbrauch eines Kill-Befehls
Entladen der Batterie (nur akt.)
Ablösen des Tags vom Träger
mech. od. chem. Zerstörung
Zerstörung durch Feldeinwirkung
Gegenmaßnahmen
Abschirmen Lesestationen/Räume
Einsatz von Felddetektoren
Verlagerung ins Backend
Authentifizierung
Verschlüsselung
Einsatz von Read-only Tags
Erkennung von Duplikaten
Verbot in AGB
verbesserte Lesestationen
aktive Frequenznachführung
Frequenzsprungverfahren
Schlafmodus (nur bei akt.)
Alarmfunktion (nur bei akt.)
verdeckte Zusatzmerkmale
unlösbare mech. Verbindung
selbst heilende Sicherung

Akteure

- **aktive Partei** = Betreiber des RFID-Systems, bedroht durch
  - Angriffe durch die passive Partei
  - Angriffe durch eine Drittpartei (Konkurrenten, Wirtschaftsspione, Cyberterroristen…)
- **passive Partei** = Träger von Tags oder getaggten Objekten, bedroht durch
  - Angriffe durch eine Drittpartei
  - Nutzung oder Weitergabe der Daten durch die aktive Partei zum Nachteil der passiven Partei

Einschätzung der Bedrohungslage für die aktive Partei

- Die Bedrohung durch **Angriffe** auf RFID-Systeme ist im Vergleich zu den heute festzustellenden **technischen Schwierigkeiten** ihres Betriebs gering.
- Mit der Massenanwendung von RFID könnte das Bedrohungspotenzial zunehmen, da sowohl die **Anreize** als auch die **Gelegenheiten** für Angriffe sich vervielfachen.
- Allerdings werden auch die **Stückkosten für Sicherheitsmaßnahmen** mit deren Massen-anwendung sinken.

Einschätzung der Bedrohungslage für die passive Partei

- Aus Sicht der passiven Partei können **Data Privacy** und **Location Privacy** bedroht sein.
- Die Privatsphäre ist insgesamt weniger durch **Angriffe** auf RFID-Systeme als durch ihren **Normalbetrieb** bedroht.
- Durch die zeitnahe Abbildung der realen in der virtuellen Welt werden Datenbestände aufgebaut, die nachträglich **zweckfremde** Auswertungen zulassen.
- Es ist **umstritten**, ob dies im Vergleich zu akzeptierten Systemen wie Kreditkarten, Kundenkarten, Mobiltelefonie relevant ist.

Sicherheitsmaßnahmen 1/6: Kill-Befehl

- einfach zu realisieren
- ohne Passwortschutz leicht zu missbrauchen
- mit Passwortschutz kompliziert zu gebrauchen
- passive Partei hat keine definitive Gewissheit

Sicherheitsmaßnahmen 2/6: Verlagerung der Daten ins Backend

- Ist aus Sicht der aktiven Partei ohnehin vorteilhaft, falls keine Offline-Verarbeitung erforderlich ist.
- Sicherheit der im Backend gespeicherten Daten ist so gut wie IT-Sicherheit allgemein → nicht spezifisch für RFID.
- IT-Sicherheitsmaßnahmen im Backend lassen sich leichter neuen Anforderungen anpassen.
- Transparenz für die passive Partei kann abnehmen.
- Kein Beitrag zur Location Privacy.

Sicherheitsmaßnahmen 3/6: Abhörsichere Antikollisionsprotokolle

- Sollen speziell das Abhören der ID-Nummern aus Distanz verhindern und dadurch einen Beitrag zur Location Privacy leisten.
- Nutzen die Tatsache aus, dass das Lesegerät ein stärkeres Signal sendet als das Tag: Abhördistanz für Downlink kann daher größer sein als für Uplink.
- Untersuchungen des BSI haben diese Voraussetzung in Frage gestellt (zumindest für induktiv gekoppelte Transponder bei 13,56 MHz; Finke/Kelter, 2004).

Sicherheitsmaßnahmen 4/6: Starke kryptographische Verfahren

- Stark abweichende Schätzungen zu den Auswirkungen auf die Kosten pro Chip, in Zukunft möglicherweise sehr günstig zu realisieren.
- Ausreichende, wenn auch nicht absolute Sicherheit gegen unautorisierten Zugriff.
- Identität des Tags kann durch Dritte nicht festgestellt werden (Beitrag zur Location Privacy).
- Bringt für die passive Partei keine Transparenz.

Sicherheitsmaßnahmen 5/6: Verfahren mit wechselnden IDs

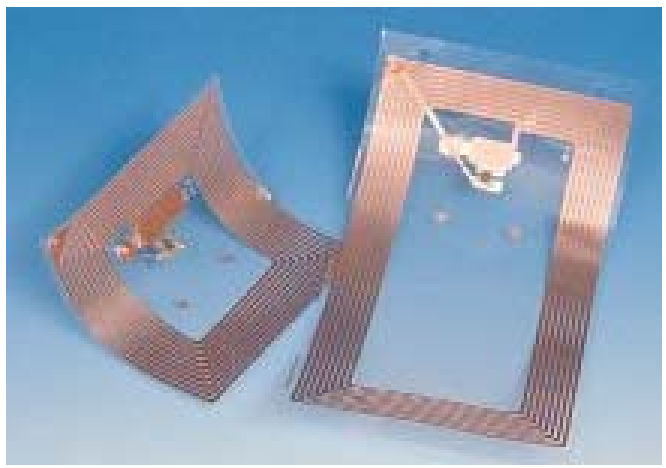
- geringe Anforderungen an den Chip, für 0,5 Cent pro Tag zu realisieren (Hash-Funktionen)
- Identität des Tags kann durch Dritte nicht festgestellt werden.
- Technisch einfachere Alternative zu starken kryptographischen Verfahren (low end).
- Bringt für die passive Partei keine Transparenz.

Sicherheitsmaßnahmen 6/6: Faire Informationspraxis implementieren

- Grundsätze der FIP (Zweckbestimmung, limitierte Nutzung, Transparenz, Verantwortbarkeit) in RFID-Protokolle integrieren (Flörkemeier, ETHZ)
- Anfragen des Lesegeräts bleiben nicht anonym, es sendet eine eindeutige Kennung und deklariert den Zweck des Auslesens durch einen Code.
- Die passive Partei kann hierfür ein Anzeigegerät verwenden und ggf. Missbräuche ahnden.
- Tags können so programmiert werden, dass sie nur bei erwünschter Zweck-Deklaration antworten.

Risiken und Chancen des Einsatzes von RFID-Systemen

RFID – alles sicher?



Prof. Dr. Lorenz Hilty
Abteilung Technologie und Gesellschaft
EMPA, St. Gallen

EMPA