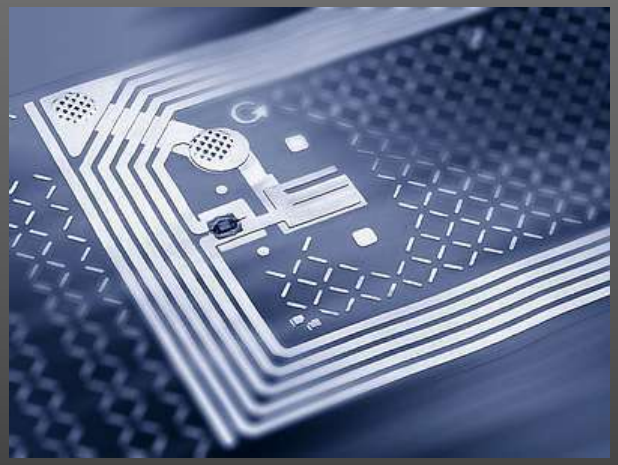
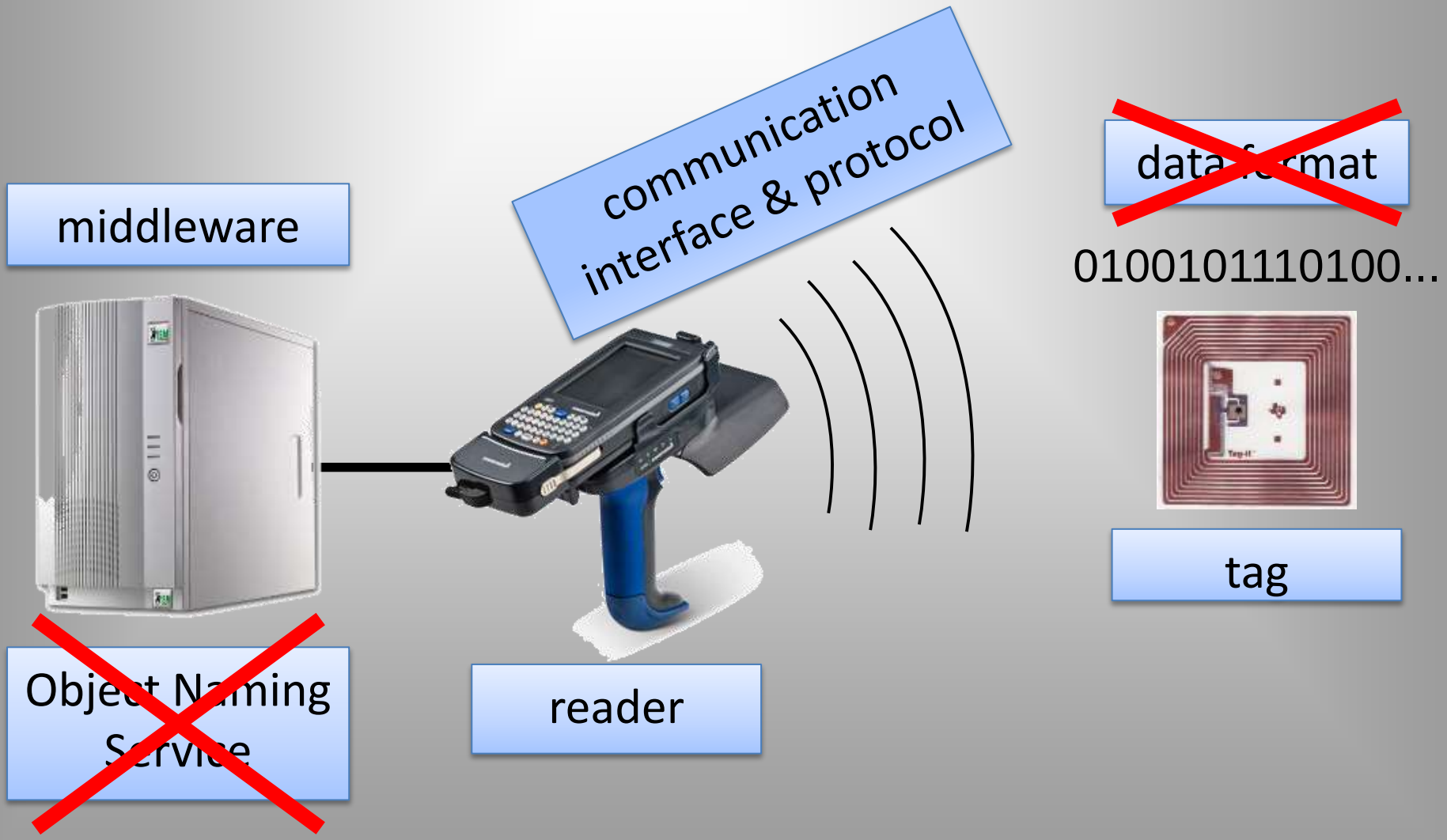
RFID Security



Materials from the FIRB SAT lecture slides by Massimo Rimondini included with permission.

Architecture



Who

- Supply chain management
  - Benetton
  - Wal-Mart
  - Procter & Gamble
  - Gillette
- U.S. Department of Defense
- Tires
  - Michelin (truck tires)
  - Goodyear (racing tires)
- Volkswagen

Why

- Unique identification and tracking of goods
  - Manufacturing
  - Supply chain
  - Inventory
  - Retail
- Unique identification and tracking of people and animals
  - Access control & Authorization
  - Medical applications (drugs, blood banks, mother-baby pairing, etc.)
  - Tracking of livestock, endangered species, and pets
- Anti-theft systems
- Toll systems
- Passports
- Sports event timing

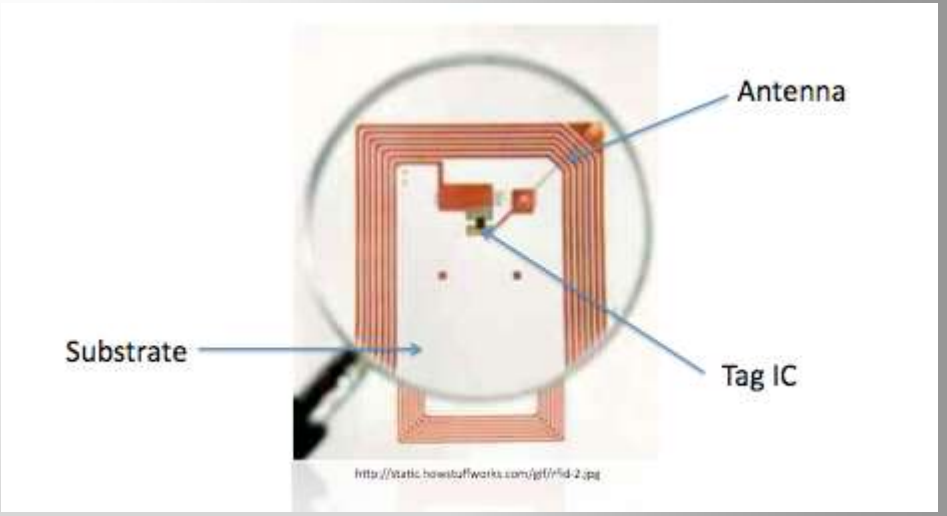
Sam Polniak. *The RFID Case Study Book: RFID Application Stories from Around the Globe*. Abhisam Software.

Operating Frequency

- The operating frequency of an RFID tag affects several parameters
- Range
  - LF (9-135KHz): a few cms
  - HF (13.56MHz): up to 1m
  - UHF (0.3-1.2GHz): >1m
  - MW (2.45-5.8GHz)
- Data exchange speed
- Signal attenuation through materials
- (Cross-country) Interoperability
  - FCC
    - ETSI

Types of Tags

- **Passive**
  - Operational power scavenged from reader radiated power



- **Semi-passive**
  - Operational power provided by battery

- **Active**
  - Operational power provided by battery - transmitter built into tag

Threats & Countermeasures

- Eavesdropping
  - Passive monitoring of the air interface
  - Encryption, shielding, range reduction
- Relaying
  - Man-in-the-middle (allows legitimate authentication)
  - Shielding, range reduction, distance bounding protocols
- Unauthorized tag reading
  - Fake reader with extended range
  - Reader authentication, on-demand tag enabling, sensitive data in the backend, tag killing

Pawel Rotter. *A Framework for Assessing RFID System Security and Privacy Risks*. IEEE Pervasive Computing, 7(2):70–77, June 2008.

Threats & Countermeasures

- Cloning
  - Duplication of tag contents and functionality
  - Authentication, manufacturing-stage countermeasures against reverse engineering
- Tracking
  - Rogue readers in doors or near legitimate ones
  - Authentication, range reduction, shielding tags, tag disabling, pseudonyms
- Replaying
  - Repeated authentication sequences
  - Authentication [see eavesdropping]

Pawel Rotter. *A Framework for Assessing RFID System Security and Privacy Risks*. IEEE Pervasive Computing, 7(2):70–77, June 2008.

Threats & Countermeasures

- Tag content changes
  - Insertion or modification of data in the tag's memory
  - Lock, permalock, smarter malware-proof readers
- Tag destruction
  - Burn in a microwave oven, slam with a hammer, etc.
  - ...?
- Blocking
  - Reader awaits response from several non-existent tags
  - Detection is possible
- Jamming
  - Radio noise
  - Detection is possible

Pawel Rotter. *A Framework for Assessing RFID System Security and Privacy Risks*. IEEE Pervasive Computing, 7(2):70–77, June 2008.

Threats (reprise)

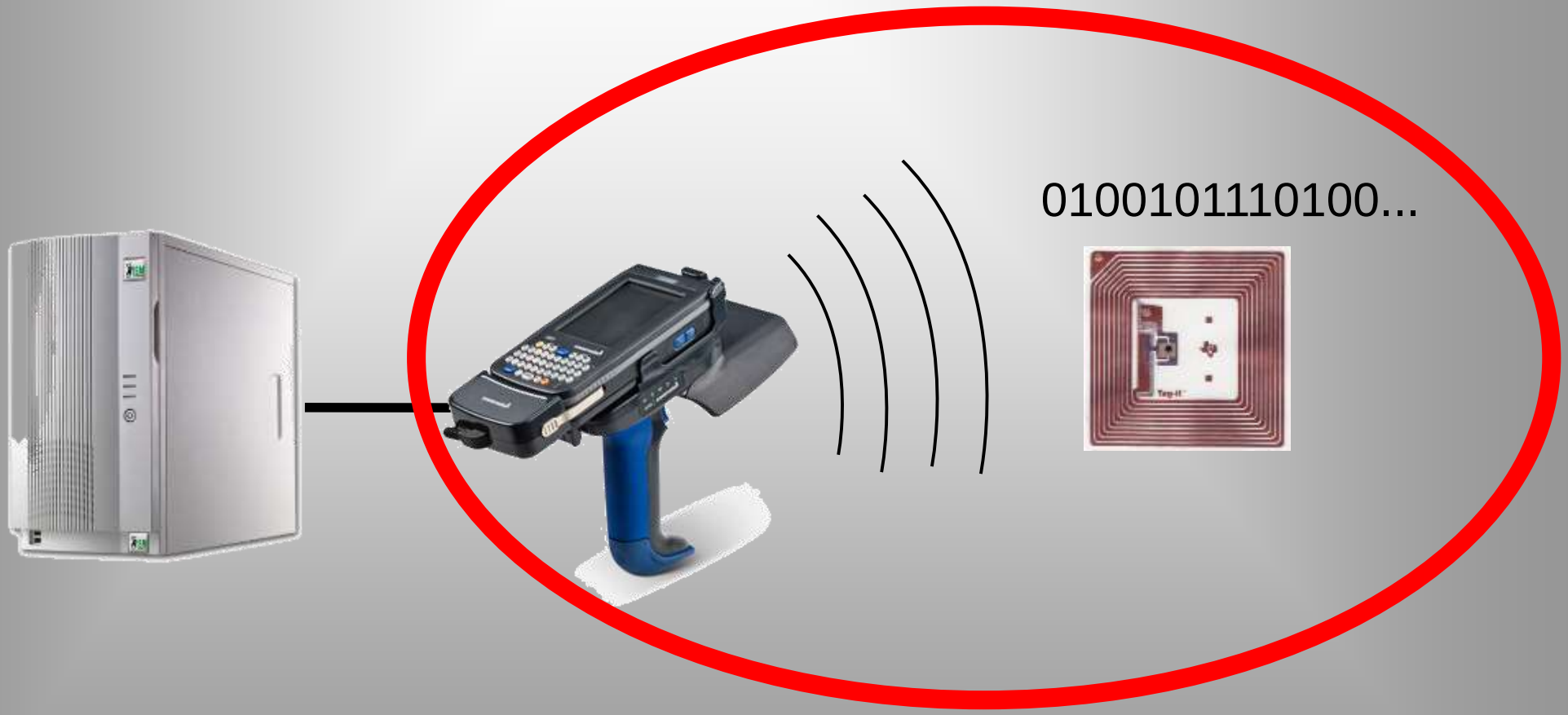
- Breakdown of business processes
- Handling of crucial and strategical information
- Privacy violations
- External risks
  - e.g., exposure to RF radiation, middleware hacking

Tom Karygiannis, Bernard Eydt, Greg Barber, Lynn Bunn, and Ted Phillips. *Guidelines for securing radio frequency identification (RFID) systems*. Recommendations of the National Institute of Standards and Technology, NIST 800-98, 2007.

Security coordinates

- Service availability
- Cloning
- Security of read operations
- Security of write operations
- Security of information

Focus



Denial of Service

Denial of Service

- Impair communication with valid tag
  - Jamming
    - oscillator+audio amplifier
  - Faraday cage
    - aluminium leaf
- Fool the reader with counterfeit tags
- Confuse the singulation tree walking
  - Blocker tag
- Interposing metals
- Detaching tag antennas
- Physical destruction (of anti-shoplifting tags)
    - camera's flash circuit

Cloning

Cloning

- Violates information integrity
  - Breaks stock availability (rather than money gain)
  - Allows spoofing & theft
- Made possible by writable memories
- Possible even just with a PDA+PC card
- Countermeasures:
  - Killing
  - Read-only memories
  - (Mutual) Authentication protocols
  - PUFs

Ranges

- Depend on the frequency

traffic analysis
(without interpreting
transmission)

rogue command

nominal

back channel
eavesdropping

forward channel
eavesdropping

rogue
skimming/scanning

Information Security

Security of Write Operations

Security of write operations

Recycle solutions for read operations

Timings

- Writes may take longer than reads
  - Some skimming-like scenarios vanish

Faulty writes

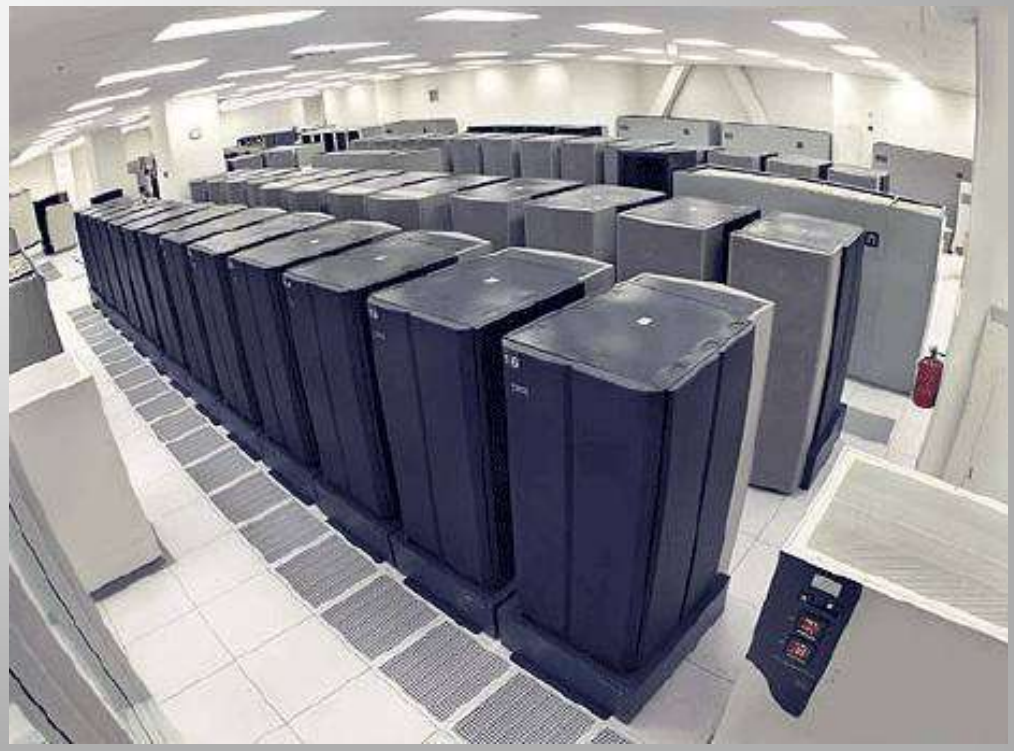
- Tags may confirm faulty writes
  - Wrong data has been written
  - Data has not been written at all
- Caused by
  - Temporary antenna failure
  - Radio interference
  - Laser radiation

Michael Hutter, Jörn-Marc Schmidt, and Thomas Plos. *RFID and Its Vulnerability to Faults*. Proceedings of the 10th International Workshop Cryptographic Hardware and Embedded Systems, CHES 2008, August 2008. Springer.

Focus

0100101110100...

Information Security



Security of Data (and Infrastructure)

Backend vulnerabilities

- Each component of an RFID systems may be vulnerable
- Compromising a component reflects on others
- Compromising tags may affect the backend!

Backend vulnerabilities

Malware

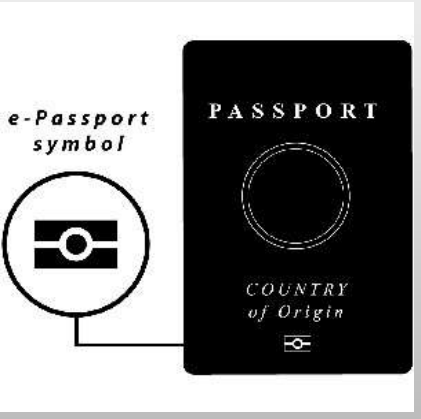
- The world's First RFID chip infected with a virus

Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum. *Is your cat infected with a computer virus?* In Proc. IEEE PerCom 2006, 2006.

Security of existing applications

Security of existing applications

- e-Passports
  - ICAO (International Civil Aviation Organization) requires:
    - compulsory authentication of passport data, signed by the issuer
    - (optionally) access control based on cryptographic keys
    - (optionally) public key authentication of the passport
  - Vulnerabilities still exist
    - Transferability (verifier becomes prover)
    - Reset attacks (same coin toss by resetting internal state of one party)



Carlo Blundo, Giuseppe Persiano, Ahmad-Reza Sadeghi, and Ivan Visconti. *Resettable and Non-Transferable Chip Authentication for ePassports*. In Conference on RFID Security, Budaperst, Hongria, July 2008.

Security of existing applications

- Car ignition: Keeloq
  - Manufacturer has master secret
  - Cars have unique ID
  - MASTER $\oplus$ ID = car's secret key
  - Finding **1** key leads to the master secret!!
  - ~2 days on a cluster of 50 Dual-Cores
  - "Soon, cryptographers will all drive expensive cars" :-)

Sebastian Indesteege, Nathan Keller, Orr Dunkelman, Eli Biham, and Bart Preneel. *A practical attack on keeloq*. In Proc. Eurocrypt 2008, 2008.