Security for RFID Tags

M. Tehranipoor

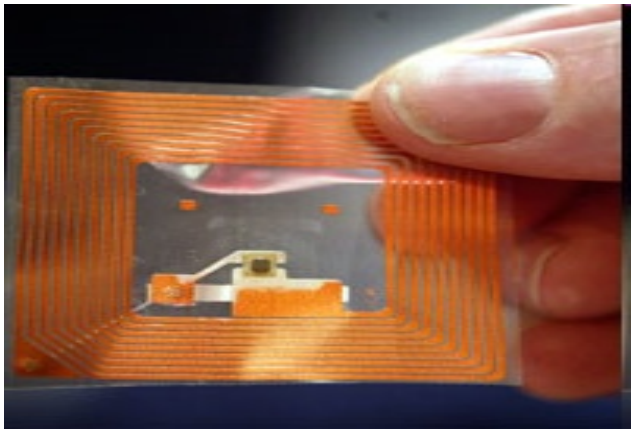
Introduction to Hardware Security & Trust
University of Florida

Overview

- Introduction to RFID and its applications
- Types of security attacks to Passive RFID Tags
  - Impersonation
  - Information Leakage
  - Physical Manipulation
- Types of Protection Methods for RFID Tags
  - PUFs and Unclonable RFID Tags
  - Other means of security
- Fingerprinting RFID Tags
- References

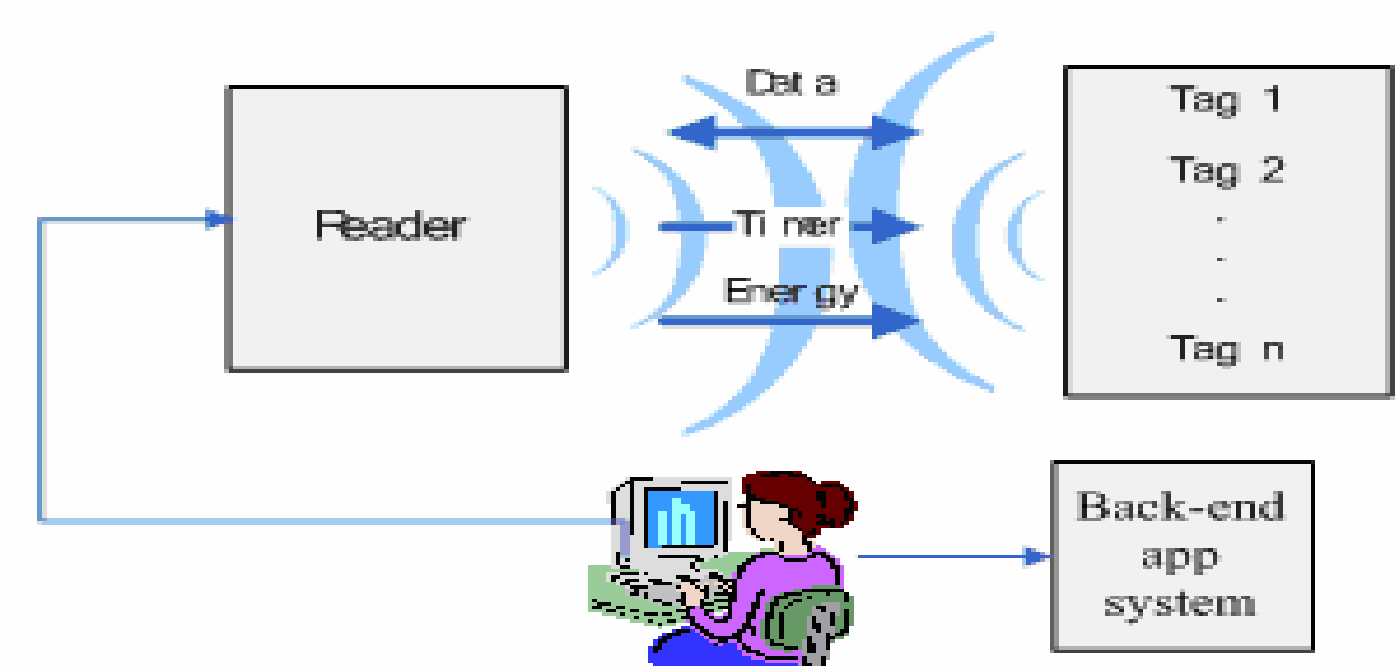
RFID

- Radio frequency identification (RFID) is an automatic identification method
  - Retrieve and access data using RFID tags
  - RFID tags are intelligent bar codes that can talk to a networked system which can track and identify every product using radio waves
- RFID system includes:
  - Tags, readers, database system



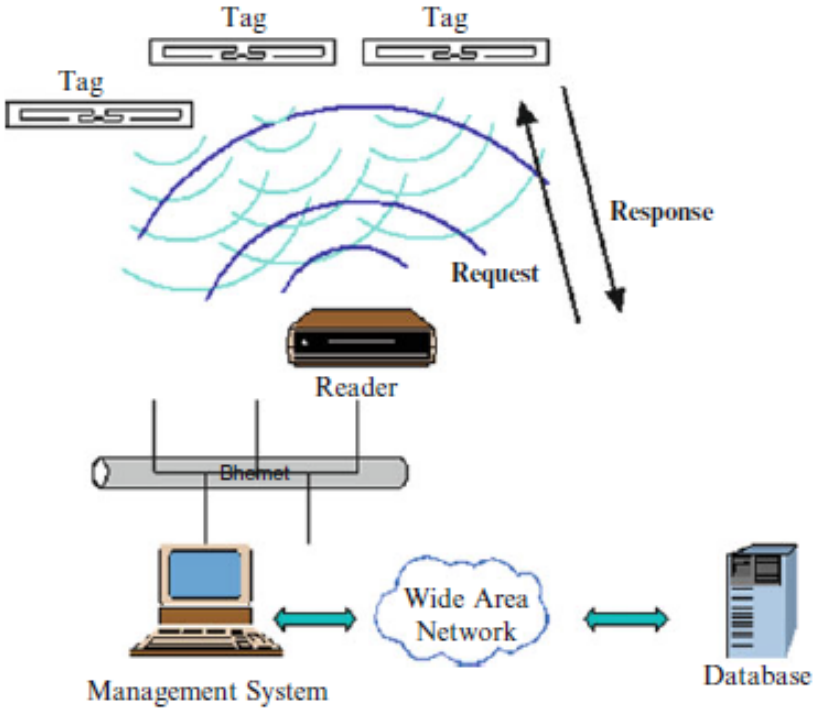
RFID System

- RFID system includes:
  - Tags, readers, database system



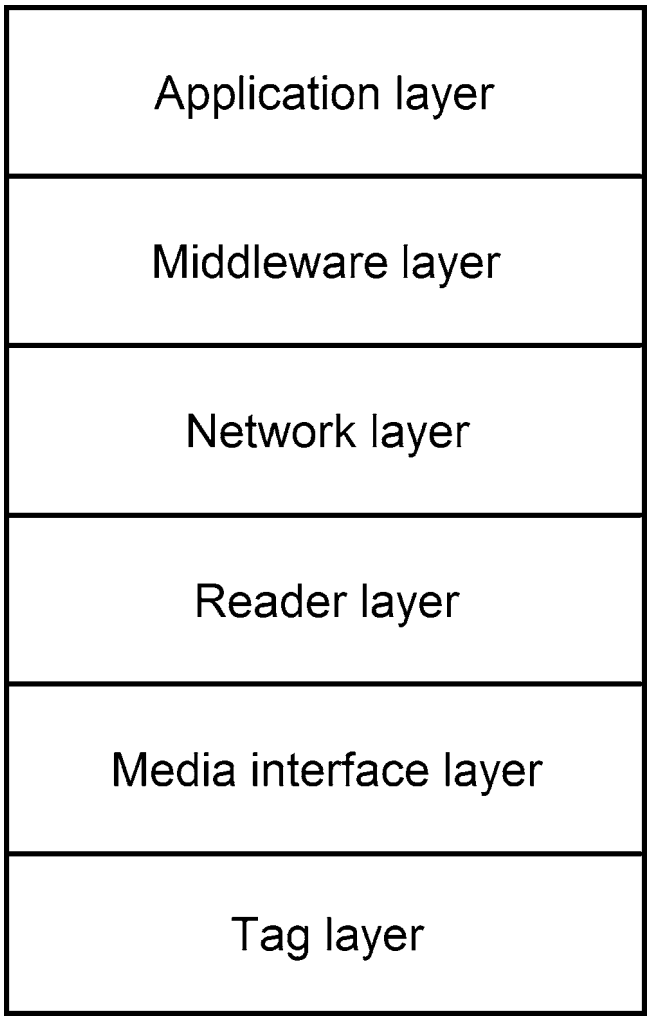
RFID System cont'd

- Reader emits continuous RF signals and keeps observing the received RF signals for data
- The tag harvests direct energy from RF signal
- Tag reflects a modified version of the RF signal back to the reader to convey information
- The reader demodulates the signals received from the tag and decodes it for further processing



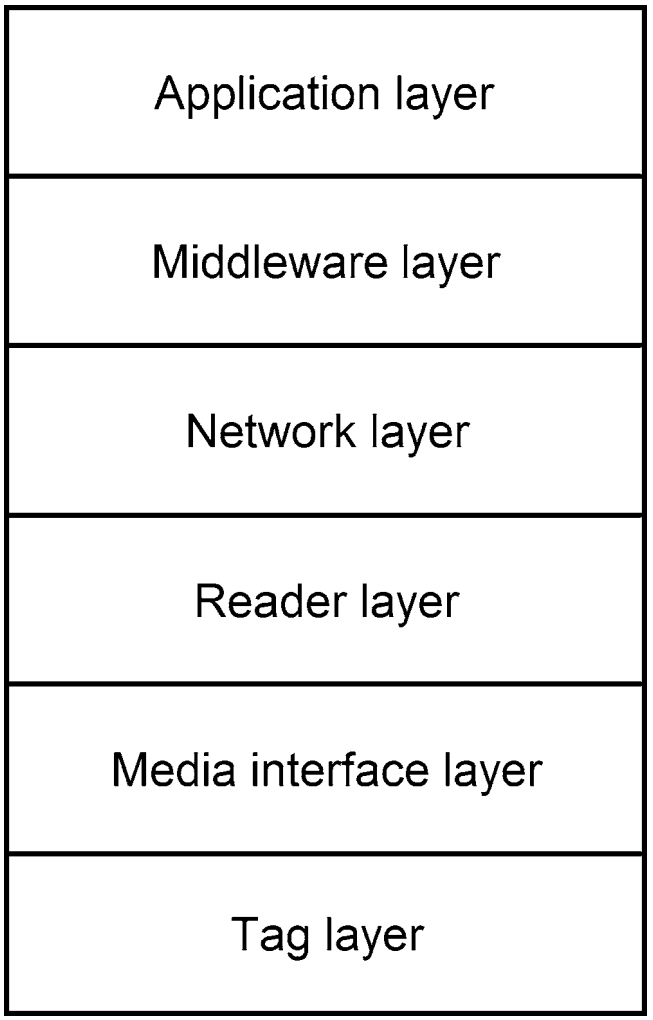
RFID Reference Model

- Standard six-layer grouping of different functions for an RFID system
  - **Application layer**: refers to different RFID uses (i.e. item management)
  - **Middleware layer**: refers to software that translates/filters data from reader to application
  - **Network layer**: refers to the communication pathway between reader and application residing on a server



RFID Reference Model cont'd

- **Reader layer**: refers to the architecture of a reader – a computer and receiver in one package connected to antennas
- **Media interface layer:** refers to the way the reader controls access to the media (generally wireless)
- **Tag layer:** refers to the architecture of the tag including power harvesting circuit, modulator, demodulator, logic, and memory layout



Types of RFID Tags

- Active tags : Should have power source, longer ranges, larger memories to store additional information sent by the transceiver.
- Passive tags : They are cheaper, because of less hardware, do not have their own power supply. Electrical current induced in the antenna by the incoming radio-frequency scan provides enough power to the tag to send a response
- Based off radio frequency :

  A. Low frequency tags (125-134Khz)

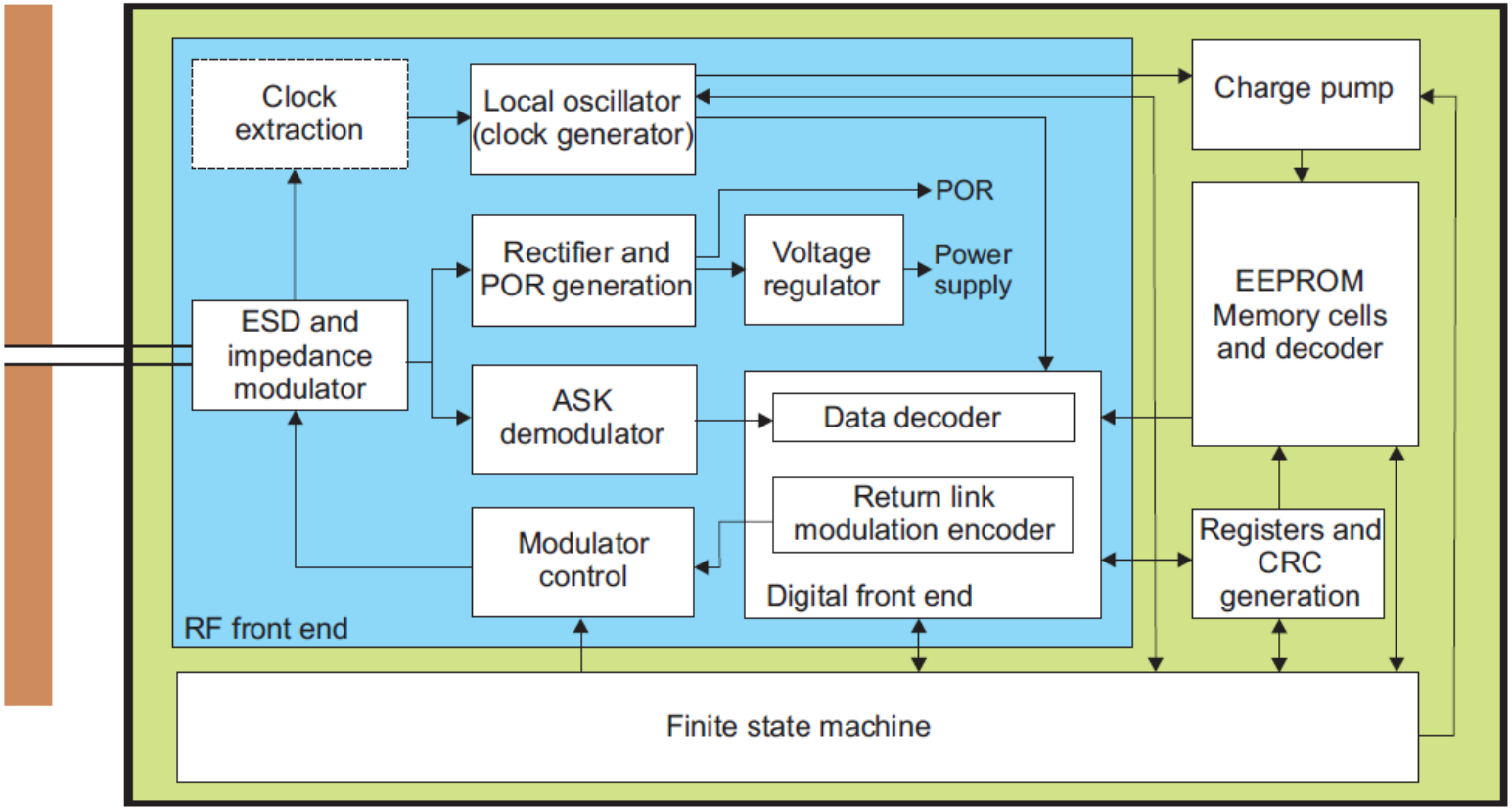
  B. High frequency tags (13.56 MHz)

  C. UHF tags (868-956 MHz)

  D. Microwave tags (2.45 GHz)

Passive RFID Block Diagram

- Mainly consists of RF front end, memory circuitry, and FSM for logic circuitry



Passive RFID Description

A. **RF Front End:** Antenna inputs passes through circuits for ESD protection. ASK (Amplitude Shift Keying) demodulation circuits extracts the modulation dips from the received signal and Rectifier will rectify the received signal to generate power, regulated using voltage regulator to avoid voltage surges due to variations in the RF field

B. **Memory Circuitry:** EEPROM will store the EPC tag and charge Pump consists of series of capacitors to achieve voltage of 17 Volts for writing to the tags memory

C. **Finite State Machine (Logic Circuitry):** Chip Logic circuitry will execute reader commands and implement an anti-collision scheme that allows the reading of multiple labels by the reader. It also controls read and write access to the EEPROM memory circuits

Application of RFID Tags

- Item management
  - Includes supply chain, logistics, inventory control, and equipment management
  - Provides visibility to the supply chain
    - Businesses can identify bottlenecks in the system and correct them
- Smart cards (e-passports)
  - Low-cost alternative to passports
  - Contains UHF RFID tag (ultra-high frequency)
  - US Citizens can enter US from Mexico, Canada, Caribbean, and Bermuda with e-passport
  - Similarly, future driver licenses will contain RFID tags

Application of RFID Tags cont'd

- Finance and banking industries
  - Major credit cards offering embedded RFID tags
  - User can wave card near reader in front of cash register to pay for items – faster payment method than magnetic strip
- Sensor tags using RFID
  - Tag programmed to log data into nonvolatile memory
  - Data retrievable after battery is drained (passive tag)
- Livestock tracking, human-implantable RFID tags
  - Cows, pets, human healthcare information
- Mitigate counterfeiting
  - ~$600 billion per year problem

Security Attacks to Passive RFID Tags

- Due to relatively simple on-tag circuits and wireless communication nature, RFID systems have numerous vulnerabilities
- The target of these attacks can be:
  - Tag, reader, communication protocol, middleware, or the database

Attacks for Impersonation

1. Tag Cloning

- Duplicating or manipulating RFID tag data to make similar copies that can be accepted by an RFID application as valid
- In simple passive RFID systems, cloned tags are indistinguishable from authentic ones

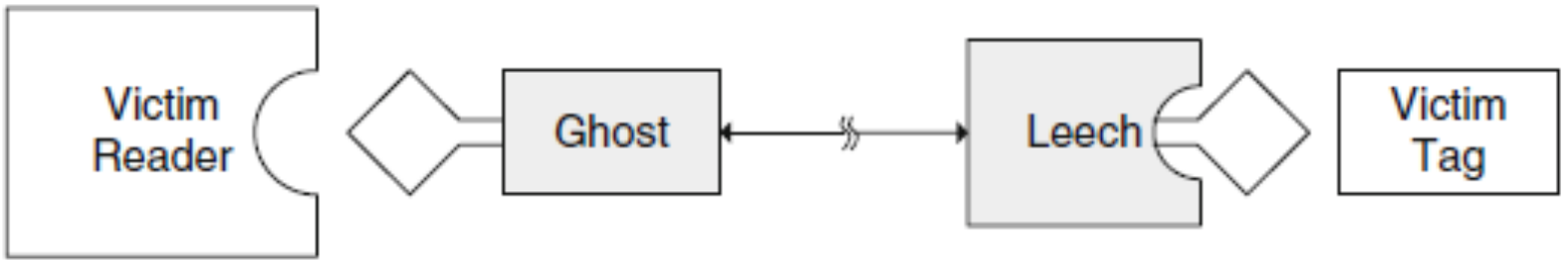
2. Tag Spoofing (emulation)

- May use custom designed electronic device to imitate, or emulate, the authentic tag
- Can fool automated checkout system into thinking product is still on shelf
- Adversary must have full access to legitimate communication channels and knowledge of protocols

Attacks for Impersonation

3. Relay Attacks

- Need two devices acting as a tag and a reader
  - Leech device as reader to legitimate tag
  - Ghost device as tag to legitimate reader
- The illegitimate devices can modify the data during relay
- Can be carried out over considerable distances



Attacks for Impersonation

4. Replay Attacks

- Similar to relay attack
- May use captured valid reader-tag communication data at a later time
  - Use for other readers or tags for impersonation
- Data can be captured via relay attacks or eavesdropping
- Typical scenario involved breaking FRID-based access control systems

Attacks for Information Leakage

1. Eavesdropping

- Attacker uses special reader and antennas to collect an RFID data.
- Records the messages in either direction
  - Forward channel → reader-to-tag
  - Backward channel → tag-to-reader

2. Code Injection Attacks (Tag Modification)

- Data contained in the RFID tag can be modified so that it contains malicious code which can change the course of execution of backend systems or databases processing the RFID data
- i.e. adversary may wipe out price stored on tags for expensive products in a store – write a cheaper price to it

Attacks for Denial-of-Service (DoS)

1. KILL Command Abuse

- Protected by password stored on tag
- Set of tags often share same KILL password
- Can be obtained through more sophisticated attacks and then used to issue unauthorized KILL commands

2. Passive Interference (generally unintentional)

- Water and metal cause interference to the comm. link
- Radio waves may collide and cancel each other out

3. Active Jamming

- Send out radio signals to disrupt reader-tag communication
  - Radio noise generators

Attacks through Physical Manipulation

1. Physical Tampering

- Microprobing, fault injection, laser cutter microscopes

2. Tag Swapping, Removal, Destruction

- Tag swapping removes tag from associated object and attaching it to another one
- Tag removal is removing a tag from the associated object
- Tag destruction is to physically disable the tag
  - Chemicals, excess pressure or tension, or taking off antenna

3. Tag Reprogramming

- Attacks tags that are reprogrammable either through RF or wired interface
  - Program a tag to create a clone or cause data inconsistency

Protection Mechanisms

- Ever since the threats and attacks to RFID tags were identified, researchers from industry and academia have been working on various protection mechanisms.
- In this section a variety of existing protections for RFID tags are introduced and organized by the corresponding attack categories as in the previous section

Attacks for Impersonation

1. Tag Cloning and Spoofing

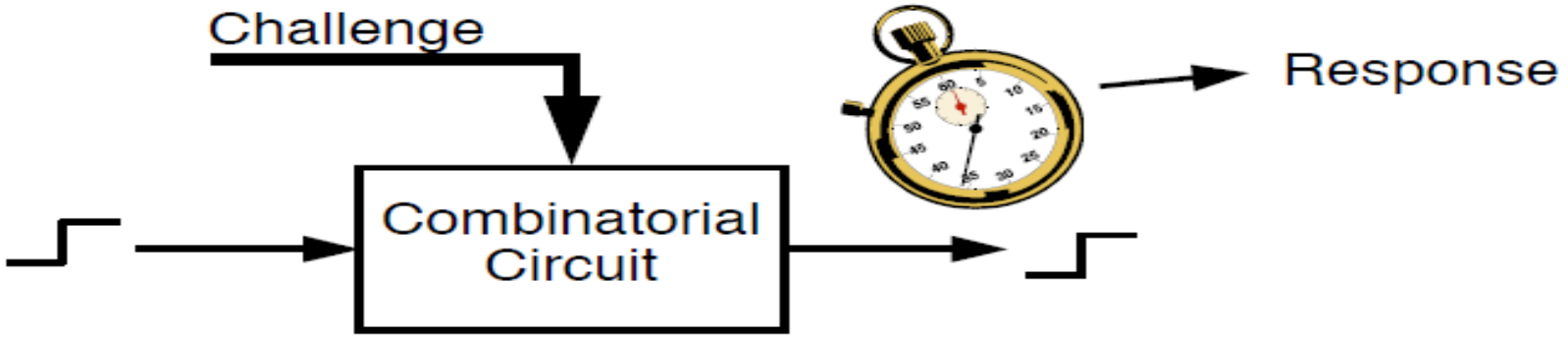
- The limited on-tag hardware resources leads to weak authentication protocols
- **PUFs** – can be mitigated via challenge-response authentication protocols with additional circuitry
  - Challenge-Response pairs initially created and stored in database
- **Watermarking** – generate a watermark using pseudo random number generator based on data stored in tag
  - Watermark embedded in reader-tag communication protocol

PUFs

- A Physical Unclonable Function (PUF) is:
  - Based on the physical system and easy to evaluate (using the physical system).
    - Its output looks like random function
  - Unpredictable for an attacker with physical access
  - Due to process variations no two identical circuits are the same

PUFs cont'd

- Identical circuits with the same layouts placed on different FPGAs shows that path delays will vary enough across ICs to use them for identification
  - Process Variation



PUFs and Security

- PUF Security is based on:
  - Wire delays
  - Gate delays
  - Quantum mechanical fluctuations
- PUF characteristics:
  - Uniqueness
  - Reliability
  - Unpredictability
- PUF Assumptions:
  - Infeasible to accurately model PUF
  - Physical tampering will modify PUF

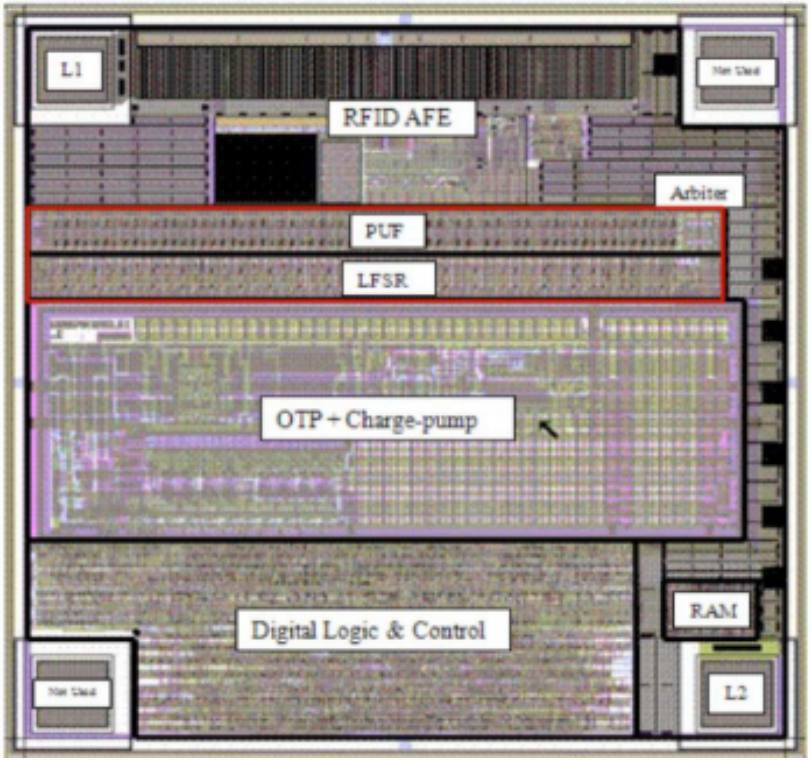
Unclonable RFID Tags

- RFID Tag equipped with a PUF
  - Delay PUF, Coating PUF, Optical PUF, etc.

- Secure because:
  - Removing the PUF leads to destruction.
  - PUF output is inaccessible to attacker
  - Attacker cannot tamper with the communication between the PUF and RFID Tag
  - PUFs provide a secure, robust, low cost mechanism to authenticate silicon chips

Example Unclonable RFID Tag

- Majority of silicon area is consumed by standard RFID components
  - RF front-end, OTP memory, digital logic for commands
- PUF circuit and Linear Feedback Shift Register (LFSR) uses small portion
  - PUF component ~0.02mm^2 in chip using .18u fab technology



Floorplan of PUF enabled RFID Tag

Attacks for Impersonation cont'd

2. Relay Attack and Replay Attack

- Relay attacks can be prevented by measuring the distance between the reader and the tag
  - Shorter the distance, the harder it is for relay attacks
  - Methods include:
    - Round trip delay of RF signal or signal strength
    - Ultra-wide band pulse communication-based distance protocol
- Replay attacks can be prevented using distance between tag and reader to distinguish authorized tags/readers
- Other methods include:
  - Timestamps, one-time passwords, RF shielding (limit direction of radio signals), etc.

Attacks for Information Leakage

1. Unauthorized Tag Reading / Eavesdropping

- Two categories
  - Break reader-tag communication link when tag is not being accessed
    - Tag shielding (aluminum-line wallets to protect the tag)
    - Blocker tag (simulates many RFID tags to reader, masking existence of actual tag)
  - Apply access control mechanisms to the tag
    - Adding cryptographic transactions to the reader-tag communication protocol → permanently deactivate tag using KILL command
    - Reduce availability of memory resource on the tag → clear unused memory every few seconds or randomize data locations

Attacks for Information Leakage

2. Side-Channel Attacks

- Power-based side-channel attacks can be mitigated through power balancing or power randomization
  - New CMOS logic gates (full charge/discharge cycle for each data processed)
  - Asynchronous circuits using dual-rail encoded logic
    - First rail is asserted to transmit a 0 value, or the second rail is asserted to transmit a 1 value. The asserted rail is then reset to zero before the next data value is transmitted, thereby indicating 'no data' or a 'spacer' state

Attacks for Information Leakage

3. Side-Channel Attacks

- Fault-injection side-channel attacks can be prevented using temporal and spatial redundancy
  - Concurrent Error Detection, Error detection/correction code, Modular redundancy, BIST – Built-In Self-Test, Algorithm modification

4. Tag Modification and Reprogramming

- Read-only tags provides a simple solution
  - However, degrades flexibility of RFID systems and limits its applications
- Adopt cryptographic algorithms to secure the on-tag data
  - Reader authentication methods also prevent unauthorized access

Attacks for DoS

1. KILL Command Abuse, Passive Interference, Active Jamming

- Improve physical security of authorized reader-tag communication channel
  - Use walls opaque to relevant radio frequencies
- Secure password management mechanisms
  - Avoid use of master password

Attacks through Physical Manipulation

1. Physical Tampering

- Anti-tampering technologies
  - Memory protection, chip coating, self-destruction

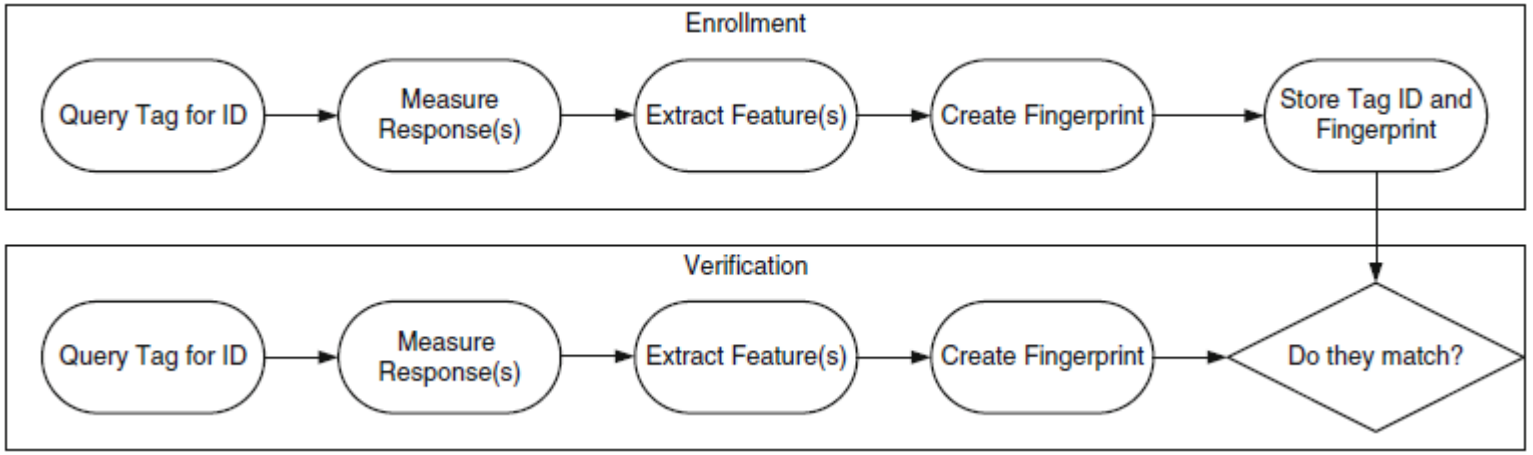
2. Tag Swapping, Removal, and Destruction

- Improve physical resilience of RFID tags
  - Strong mechanical bond or glue
  - Embedding tags inside the item package
    - Issues → RF signals can be absorbed by materials like water and metal, rendering tabs inaccessible

Fingerprinting RFID Tags

- Use electronic characteristics of RFID tags caused by manufacturing differences
  - Clock skews, transient timing responses, frequency responses, and other RF characteristics
- Creates fingerprint unique to individual tag
- Prevents counterfeiting
- Can be used by itself or in conjunction with other authentication protocols
- Involves an “enrolling and verifying” process

Fingerprinting RFID Tags



- Enrollment Phase
  - Features are measured to create the fingerprint
- Verification Phase
  - Features of presumed authentic tag are measured
- Enrolled and Measured fingerprints are compared
  - If they match, then high probability of authentic tag

Challenges of Fingerprinting

- Fingerprinting passive RFID Tags modifies the signal sent from the reader
- A study was conducted on passive HF RFID tags used in E-Passports
  - Only able to distinguish different models of tags
  - NOT different tags of the same model
  - Passive RFID tags have a strong influence on the signal from the reader due to inductive coupling
    - Change in current flow through one wire induces voltage across ends of the other wire

References

- M. Tehranipoor and C. Wang, Introduction to Hardware Security and Trust, Springer, 2011
- http://people.csail.mit.edu/devadas/pubs/rfid_puf_08.pdf
- Romero HP, Remley KA, Williams DF, Wang C (2009) Electromagnetic measurements for counterfeit detection of radio frequency identification cards. IEEE Trans Microwave Theory Tech 57(5): 1383–1387
- Niranjan Presentation Slides