RFID
Radio Frequency Identification

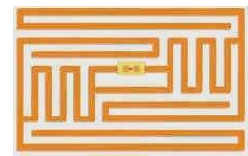
Ibéria Medeiros

Departamento de Informática
Faculdade de Ciências da Universidade de Lisboa

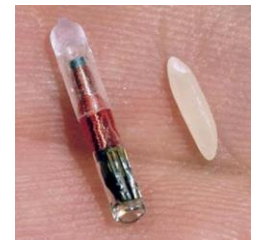
Overview

RFID is an *automatic identification method*, relying on radio signals for the retrieval of identification data stored on remote devices

- Typically, there is a small *tag* or *label* associated with a specific object, and
  - a ***reader*** sends an identification request through a radio signal
  - the ***tag*** receives the request, interprets it, and returns a response with identification information
- The message exchange can be protected cryptographically depending on the application and the tag capabilities (more security ⇒ more sophistication at the tag ⇒ higher costs)



RFID tag used by Wal-Mart



RFID tag together with a grain of rice

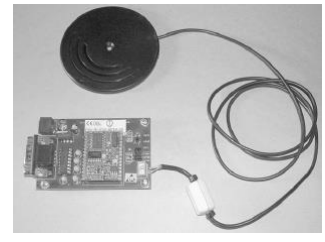
Example of Early Application

- *Identification Friend or Foe (IFF)* was developed in England during the second world war to distinguish friendly aircraft from the enemy
- In principle, it operates in a similar manner as the RFID
  - each airplane carries a transponder (short for *Trans*mitter-res*ponder*), which has associated a unique identifier
  - when an airplane approaches another one, it sends an interrogation signal, which usually contains data about the sender
  - the transponder receives and decodes the request, and generates an encrypted response with identification information (sometimes also containing some data manually set by the pilot)
- Nowadays, this method continues to be utilized, both for the civilian and military aviation; the exchanged data can include, besides the identification, the altitude of the plane and other relevant information

Tags (or Labels or Chips)

- Most RFID tags contain at least two parts:
  - an integrated circuit for storing and processing information, and modulating and demodulating a RF signal
  - an antenna for receiving and transmitting the signal.
- Chipless RFID allows for discrete identification of tags without an integrated circuit, thereby allowing tags to be printed directly onto assets at a lower cost than traditional tags

Example tags



RFID reader

Physical Form Factor

- Tag design can be adapted to the function it performs, and can be influenced by other factors such the type of antenna (which is influenced by the frequency of transmission)

  Rule: larger tags can be read at more distance
- They can be standalone or embedded in some other device (e.g., car key)
- Some of the most common designs are
  - *cards*: up to 3 times as thick as a credit card
    - » building/room access
    - » contactless credit cards
  - *key fobs*: placed in container designed to use in a key ring
  - *attached to vehicles* or *retail packages*

Example Tags

Radio-frequency identification tags measuring up to 3mm in length were attached to the backs of rock ants and then monitored by scientists

A sheep with an ear tag

Just after the operation to insert the RFID tag

Disney uses EPC passive UHF tags to track $100 million worth of costumes at its parks and on its cruise ships

Tags

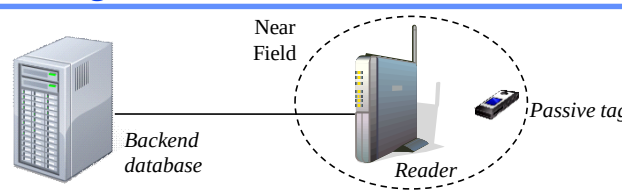
- Depending on the application, RFID systems use different **radio frequency (RF) bands**, since they influence the distance of signal propagation, the physical size of antennas and the required power transmission levels
  - *Low frequency*: 30 to 300 kHz
  - *High frequency*: around 13.56 MHz
  - *Ultra high frequency*: 860 to 930 MHz

Higher Distance

NOTE: there have been attacks that show that standard distances can not be trusted from a security perspective

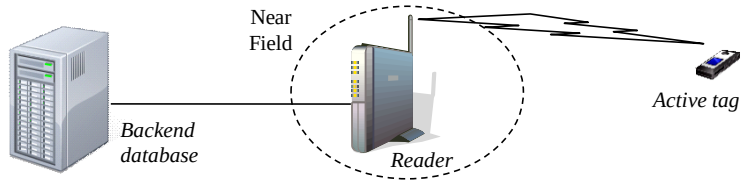
- The **tag data** depends on the application but
  - can be from a few bytes up to several megabytes
  - can be read-only or read-write
  - can have a proprietary format or use a standard such as *Electronic Product Code (EPC)* (which is the RFID replacement for the UPC barcode)
    - » EPC General ID-96 = 8bit header + 28bit General Manager Number + 24bit Object Class + 36bit Serial Number

Types of Tags



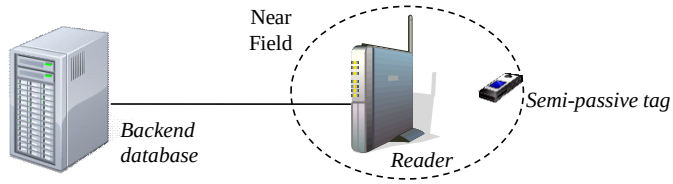
- ***Passive tags*** do **not have** a battery or other power source, but
  - can contain a resonant circuit capable of absorbing power from the reader´s antenna (using an electromagnetic property called **Near Field**)
  - need to be in vicinity of the reader´s antenna (from 10 cm to a few meters) to get enough power to generate and transmit a response
  - the response is not necessarily just an ID number, since the tag can contain non-volatile data possibly stored in an EEPROM
  - they can be quite small and are suitable for manufacture with a printing process for the antennas

Types of Tags (cont.)



- ***Active tags*** have their **own power source**, and therefore they can actively transmit and receive (and be further away from the reader)
  - communication is typically much more reliable (i.e. fewer errors) than from passive tags – can create a session with the reader
  - generate strong responses an therefore they are more robust in "RF challenged" environments (humidity)
  - generally bigger (due to battery size) and more expensive to manufacture
  - may include larger memories and the ability to store additional information received from the reader
  - may include specialized sensors (temperature, humidity, etc)

Types of Tags (cont.)



- ***Battery assisted passive tags*** have a battery for the memory and microchip, but rely on proximity to get energy to power the radio circuits for data reception/transmission
  - need power levels 100 times weaker than passive tags, and since a reduced time is needed for collecting energy, the response has a shorter latency time
  - greater sensitivity than passive tags which can be leveraged to increased range (by one order magnitude) and/or as enhanced read reliability (by reducing bit error rate at least one order magnitude)
  - longer battery powered life cycle than active tags
  - can perform active functions (temperature logging) under their own power

Readers and Middleware

- Readers are basically transceivers (i.e., transmitters and receivers) and may have
  - an integrated or separated antenna
  - a system interface (e.g., Ethernet or RS-232) for backend communication
  - cryptographic encoding and decoding circuitry
  - power supply or battery
- If a reader intends to work with a collection of tags, it needs to either discover all devices within an area to iterate over them afterwards, or use collision avoidance protocols
- Middleware software manages the readers and the data coming from the tags, and passes it to the backend database systems

> *NOTE: the communications between the reader and database servers, and the actual nodes running the reader and servers, can be compromised using the same sort attacks that have been studied in the course!!!*

Protocols

- Currently, the RFID technology is becoming more standardized. Examples:
  - *ISO 14223: Radio frequency identification of animals*
  - *ISO/IEC 14443:* a high-frequency standard *(13.56 MHz),* which is being used as the basis of *RFID-enabled passports*
  - *ISO/IEC 15693:* another high-frequency standard, which is used for *non-contact smart payment and credit cards*
  - *ISO/IEC 18000: radio frequency identification for item management*
  - *ISO 18185*: the industry standard for *electronic seals for tracking cargo containers* (433 MHz and 2.4 GHz)

EXAMPLE APPLICATIONS AND SOME PROBLEMS

Identification of Products (in Stores & Warehouses)

- Products are shipped from factories to retailers and stores with RFID tags
- Products in stores are identified with unique RFID tags, which in some cases are read-only to decrease cost or contain a small amount of read-write memory
  - stores can add a type identifier to specify a class of products

- Some advantages
  - finding out how much to pay can be done much more efficiently (e.g., no need to turn the product to get bar code) and ideally one could have a solution where products stay in the carts and are only read as a whole
  - readers placed in the shelves can determine if products need to be replenished from the warehouse
  - managing inventories becomes simpler and more accurate (e.g., by reading all selves or by maintaining information about what leaves the store)
  - robbery and fraud could potentially be easier to detect

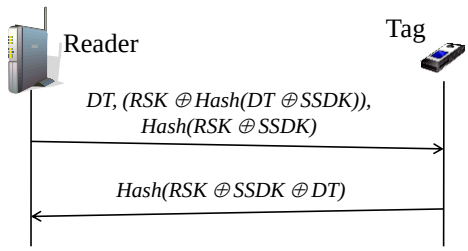
Identification of Products (cont.)

- **Privacy concerns** are a major problem, as the example shows
  - a tag is placed in a sweater and at the checkout one pays with the credit card
  - the tag is still operating when the person returns to the store
    - » P1: the reader at the entrance matches the tag with the credit card info
    - » P2: the reader at the entrance reads all clothes tags and creates a profile and ranking of the person based on the value of what is being dressed
    - » P3: a thieve can carry a RFID reader to scan for potential targets …
- To address this problem one can
  - disable the tag as the product leaves the store, but one has to be careful that
    - » the whole identification information cleared (and not just part)
    - » but with the downside, the tag can no longer be used for after sales support
  - encrypt the tag content, but this
    - » generates in practice a new identifier which can be used for tracking users

Identification of Products (cont.)

- Having a read-write memory to store some identification information causes some extra problems such as
  - the tags from various products with different prices can be read, and then a high priced item can be re-written with the identifier of a cheaper one
  - items on a shelve are written with another identification, causing the shelve reader to ask for more items, which creates a major problem in the supply chain
  - all tags could be zeroed, preventing products from being checked out
- To address this problem one can
  - use authentication protocols and (shared) secrets to identify the good readers

Example Protocol: Zero-knowledge Auth. Protocol



- *SSDK – Shared Secret Device Key*
- *DT – is a increasing nonce (e.g., timestamp), and the last value is memorized by the tag*
- *RSK – Random Session Key*

- *accept request only if DT > DT_last*
- *use DT & SSDK to obtain RSK*
- *use RSK & SSDK to authenticate*
- *only respond if correctly authenticated*

- Notes
  - the tag does not need to be tamper resistant and might not even know the "real secret" – EPC id
  - other parameters can be added to the request message by XOR/Hash() combinations with RSK
  - backward secrecy can be guaranteed by updating SSDK with RSK in each iteration and if the attacker is unable to listen to all future communications, forward secrecy is also ensured
  - different keys can be used by adding an extra parameter ("key type X"), supporting for instance *group keys for classes of products* and *keys with special privileges* (e.g., update info in the tag)

Passports

- RFID tags can be included in passports, following standards determined by the International Civil Aviation Organization (ICAO), where ISO 14443 RFID chips in e-passports are referred as "contactless integrated circuits"
- Passports would normally have
  - passive tags that operate in the 13.56 MHz range of frequencies
  - have a small amount of memory (64 KBytes) to store the same information of the passport (including the photograph); it might also include biometric data (e.g., fingerprint)
  - should only be read from small distances (10 cm)

- Some of the advantages
  - more difficult to **forge** because it is necessary to include a RFID tag
  - harder to **alter** stolen passports because the RFID also has to be updated

Passports (cont.)

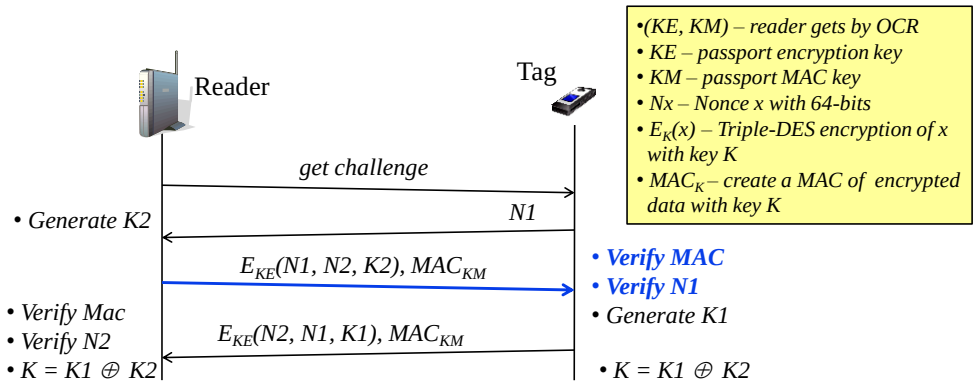
- Some problems
  - it is possible to covertly read a person´s data (called ***skimming***) **and** this can be performed from several meters way with a high powered antenna
  - nationals of a certain country can be identified through the presence of their passport (for robbery, kidnapping or terrorism)
- To address these issues,
  - *[OPTIONAL]* ***add a metallic layer*** to the front, back and spine of the passport, so that the tag can only be read if the passport is open
  - *[OPTIONAL]* ***random tag numbers*** where the tag generates a different ID for every interaction to prevent tracing
  - *[OPTIONAL]* ***Basic Access Control (BAC)***
    - » the passport RFID tag sends the data encrypted with a session key
    - » the session key is derived from an authentication with a passport key
    - » the passport key is printed in one of the pages of the passport and is scanned with a optical character recognition (OCR)

OCR Key

Key

• NOTE: the passport key is often based on the *passport number, date of birth and expiration data*, which can allow brute force attacks

Basic Access Control protocol



- Example attacks
  - **Identify country:** take advantage that different countries return distinct error codes
  - **Track a person:** msg blue is replayed; if error comes faster, then there was a MAC problem; otherwise, the problem is the wrong N1, and therefore, this passport matches the one we are tracking

Passports (cont.)

[OPTIONAL/MANDATORY in EU] ***Extended Access Control (EAC)***

– used to protect more sensitive data, such as the biometric data (fingerprint); run after BAC to check the authenticity of both the chip and the reader, using the country signing key; the reader receives a *card verifiable certificate* (CVC), with short lifetime and issued by the passport country, that gives permission to read card data

*[**MANDATORY**]* ***Passive Authentication (PA)*** to **detect changes** of passport data

– the chip contains a file (SOD) that stores hash values of all files stored in the chip (e.g., fingerprint) and a digital signature of these hashes

– the digital signature is made using a document signing key, whose public key is signed by a country signing key

[OPTIONAL] ***Active Authentication (AA)*** to prevent **cloning** of passport chips

– the chip contains a private key that **cannot** be read or copied, but its existence can easily be proven by signing a challenge sent by the reader

– the reader can get the public key from the passport, which is signed by the country signing key

Physical Access Control

- RFID tag can be inserted in *proximity cards*, which return identification information when interrogated by a door reader
- These cards vary widely in costs and technology but
  - normally have the size of a credit card, and can have a photo
  - either are read-only (preset from factory), write-once (the security staff writes to them), or read-write (for dynamic access control)
- Some advantages
  - no longer needed to have guards at the doors (which can have universal keys)
  - readers connected to a backend database support finer access control
  - an audit trail can be kept
  - less wear and tear when compared with magnetic cards, and therefore lower maintenance costs

Man-in-the-Middle Attack

- Basic attack: the adversary wants to **clone the card** by reading the ID in the tag
- Scenario 1: Tag simply **provides the identifier** when interrogated
  - the adversary gets near the victim´s tag, as long as it uses the right frequency and interrogation message he can get the tag ID information; then he clones the victims tag
- Scenario 2: Tag **runs a authentication protocol** with the reader
  - the adversary has an accomplice which is near the victim
  - the adversary approaches the door and uses a transceiver to listen to the request of the door reader
  - forwards the info to the accomplice, which transmits it to the victim´s tag
  - … and then the way around for the response …

Dealing with MIM Attacks

- Using the audit trail kept in the system it is possible to understand if a card was used to enter a room when it was not supposed to … but this is *done à posteriori*!

- Other solutions
  - create a profile for each user, monitor logs in real-time, and raise an alarm if
    - » the card assigned to the user is being employed to open a door outside the expected working hours
    - » a card is used to enter twice in a building without leaving
  - shield the card inside a metallic case to prevent remote readings
  - associate with the card other protection mechanism (e.g., a PIN)
  - have at the entrance gate a guard that compares the photograph associated with the owner of a card with the face of the person using it
  - resort to *distance-binding authentication protocols* that use physical factors

Contactless Payment System

- In contactless payment systems, users simply waive their credit card or payment tag near the reader at the POS
- Some examples are Mastercard PayPass, American Express ExpressPay
- Exxon-Mobile SpeedPass: more than 7 million users, and serves to pay gas and other products in the gas station

1. the user puts the tag near the reader associated with the gas pump
2. the reader handshakes with the tag and obtains the encrypted serial number
3. the info goes through a cable to the gas station satellite transceiver, which then sends it by satellite to the ExxonMobile data center
4. the center verifies the serial number and checks an authorization on the credit card associated to the account;
5. at the end, the authorization is returned through the reverse path

Technical Details

- Like the majority of these payments systems, most information is confidential, but nevertheless the tag
  - Texas Instruments Radio Identification System (TIRIS) 134.2 kHz Digital Signal Transponder (DST), which is an hermetically sealed glass transponder with 23 mm
  - the **authentication protocol**
    - » a tag has a unique 24-bit ID and 40-bit key embedded at manufacture that is never sent
    - » the reader starts by sending a 40-bit *challenge* to the tag
    - » the tag responds with the 24-bit ID plus a 24-bit value calculated by encrypting the challenge with the key
    - » the reader (i.e., the ExxonMobile) data center based on the ID gets the corresponding key, and the verifies the 24-bit value
  - the **encryption algorithm** is proprietary and not publicly available

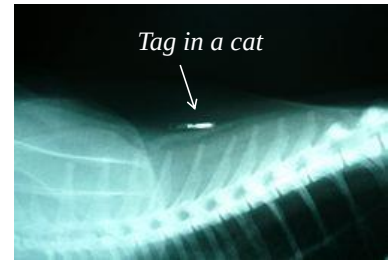
Attack on SpeedPass

- Presented by people from Johns Hopkins university and RSA Labs
- Steps for the attack
  - reverse engineer the encryption algorithm by trial and error experiments with real tags + presentation slides with some details discovered in the web
  - brute force a key search by capturing a challenge / response pair
  - improve key search performance by implementing the encryption algorithm in Field Programmable Arrays (FPGAs) - 16 boards, each testing 32 keys in parallel, took around 1 hour to find a key

NOTE: Current steps used to improve security
- *Monitoring transactions looking for unexpected behaviors*
- *Sometimes requiring the ZIP code when the payment is done*

Pets/Livestock Identification

- A chip with the size of a gain of rice in implanted via injection into the skin between the shoulders of a cat or dog; also ear RFID tags are possible
- The chip is designed to contain the typical data printed in traditional tags, and possibly some extra information related with the date of birth, breeders, vaccination …



- Some advantages
  - even if the traditional identifier is lost, it is still possible to obtain information about the animal
  - track cattle that is moved across a region
- Some problems that occur in practice
  - performance in the field of the RFID tags and readers varies greatly
  - there are multiple standards for these tags and therefore it is necessary readers that can read tags from multiple brands

Bibliography

- F. Thornton, et al., RFID Security, Syngress 2006 – chapters 1, 2, 4 and 5
- K. Mayes et al, Smart Cards, Tokens, Security and Applications, Springer, 2008 – chapter 13