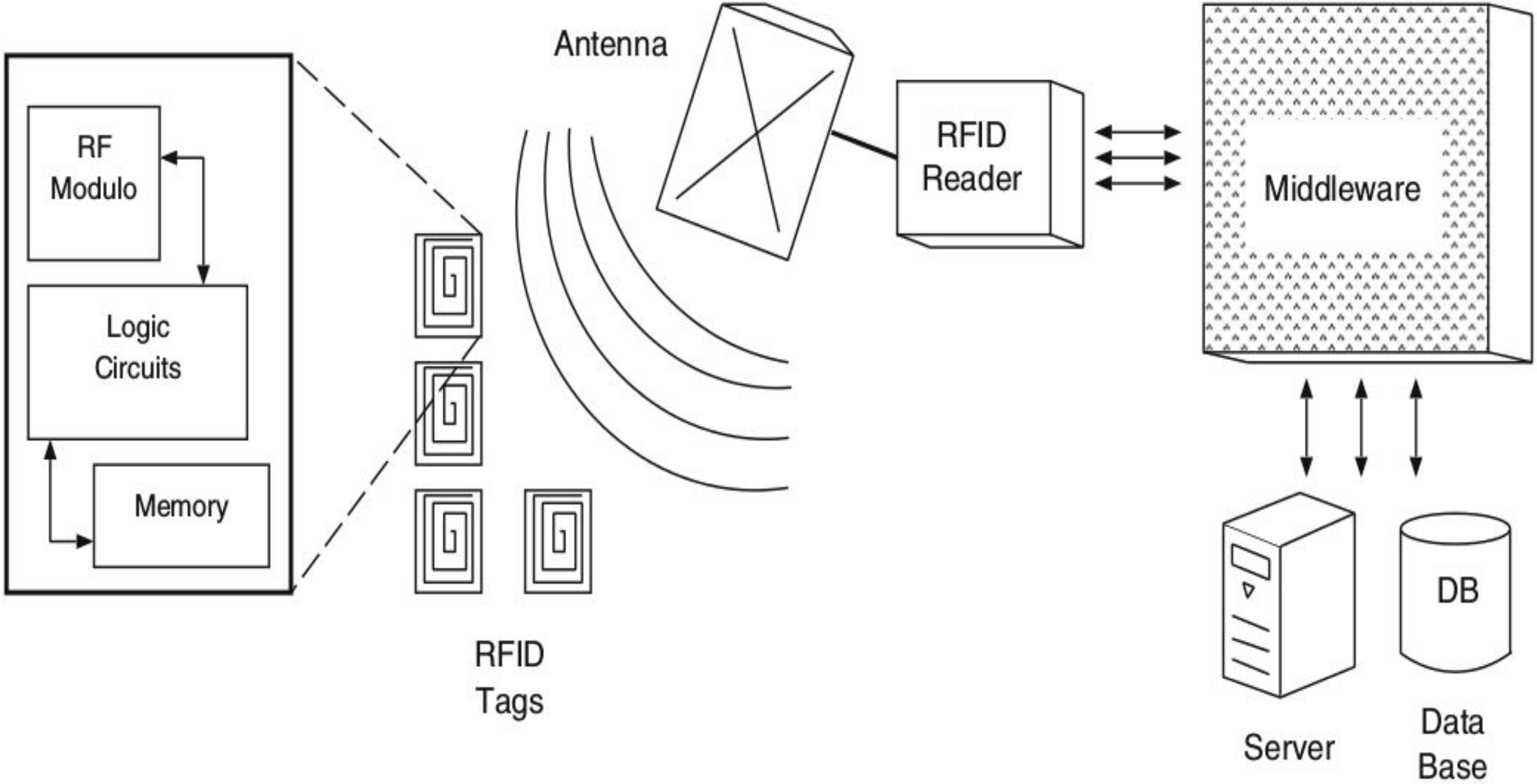
RFID Security

1

What is RFID ?

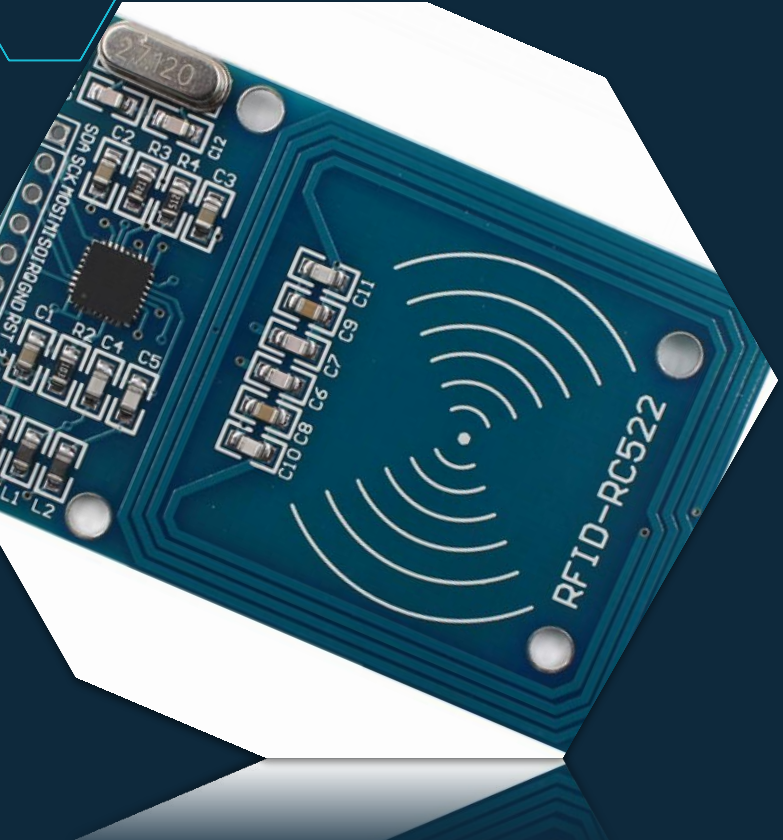
Radio Frequency Identification Device (RFID)

Automatic identification and data capture technology that uses radio frequency (RF) to identify objects.


RF
Modulo
Logic
Circuits
Memory
RFID
Tags
Antenna
RFID
Reader
Middleware
Server
DB
Data
Base

RFID Tag

- An integrated circuit (**IC**) that stores data and it is attached to an **antenna** used to transmit them to a reader.
- **Passive** or **Active Tags**
- Data can be read-only, read/write or a combination of these.



RFID Reader

- Radio frequency transmitter/receiver, controlled by microprocessor or digital signal processor.

- Accessing tags' data by wireless communication, then the reader communicates the collected data to a middleware.

2 Security Problems

Security Problems

Two kinds of possible accesses:

- **Physical access**

- **RF communication access**, by tag communication protocol, potentially without knowledge of the owner of the tag.

Elements affecting RFID security techniques

The main elements that affect RFID security techniques for tags are:

- low computational effort;
- limited memory;
- exposure to RF access by hidden readers.

Those elements don’t affect the *reader* and the *middleware* .

Tampering

A malicious action that alters something causing to different kind of effects:

- **Damage**
- **Alteration**

Two kind of protection:

- **Tamper-evidence:** detecting the existence of tampering.
- **Tamper-resistance**: resisting to tampering.

Tamper-Evident Approaches

- Fragile Watermarking
- Write Activity Record
- Symmetric Cryptography
- Public Key Cryptography

Tamper-Resistant Approaches

- Steganography
- Unwritable Memory
- Password
- Challenge-Response Protocols

Other security threats

- Data security threats
- Personal privacy threats
- Cloning threats

3

RFID authentication scheme

Serverless Authentication Protocol

$R_i \rightarrow T_j$: request

$R_i \leftarrow T_j$: $\mathbf{n_j}$

$R_i \rightarrow T_j$: $\mathbf{n_i, n_j}$

$R_i \leftarrow T_j$: $\mathbf{h(f(r_i,t_j))_m, h(f(r_i,t_j) \,||\, n_i \,||\, n_j) \oplus id}$

R_i : checks $\mathbf{L_i}$ for matching $\mathbf{h(f(r_i,t_j))_m}$ and
evaluates $\mathbf{(h(f(r_i,t_j)) \,||\, n_i \,||\, n_j)}$ to derive $\mathbf{id}$

Protocol phases

setup

Server-less authent.

Server mounted authent.

Tag searching

Setup Phase

Setting up connection between tags and readers.

Storing the information in a central database.

Tag

t : secret key

Id

$h(f(r_{cd},t_j))_m$: tag ref. Label

$f(X,Y) : h(X \,||\, Y)$

h() : hash function

Reader

r : identifier

$TS : h(TSP \,||\, r)$

$L=\{f(r_{cd},t_n)_m ,f(r_i,t_n), id_n\}$: access list

Central DB

r_{cd} : central DB identifier

Tag id

Tag secret keys

Reader identifiers

Access lists

TSP

Serverless Authentication Phase

$R_i \rightarrow T_j$: $\boldsymbol{r_i , n_i}$

$R_i \leftarrow T_j$: $\boldsymbol{n_j , h(f(r_{cd},t_j))_m, (h(f(r_i,t_j)) \,||\, n_i \,||\, n_j) \oplus id}$

The reader check its access list and compares the first part of each entry with the received $\boldsymbol{h(f(r_{cd},t_j))_m}$ *listing them.*

It calculates $\boldsymbol{(h(f(r_i,t_j)) \,||\, n_i \,||\, n_j) \oplus id}$ of the matching entries and compares the results with the received ones.

Get the correct one and take its ***id*** as $\boldsymbol{id_j}$

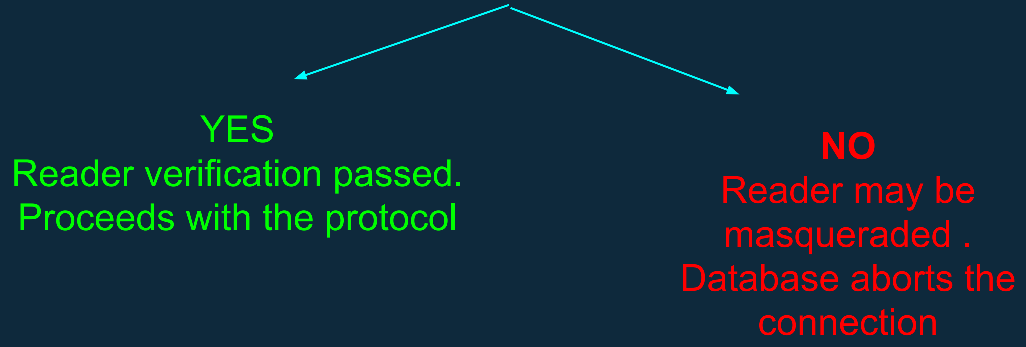
Server-Mounted Authentication Phase

Connection between the central database and readers.

$R_i \rightarrow CD$: $r_i\ ,\ n_i\ ,\ n_j\ ,\ h(f(r_{cd},t_j))_m,\ (h(f(r_i,t_j))\ ||\ n_i\ ||\ n_j) \oplus id\ ,$

$V{=}h(TS\ ||\ n_i\ ||\ n_j)$

The database calculates $h(h(TSP\ ||\ r_i)\ ||\ n_i\ ||\ n_j) = V$?



YES
Reader verification passed.
Proceeds with the protocol

NO
Reader may be masqueraded .
Database aborts the connection

Server-Mounted Authentication Phase

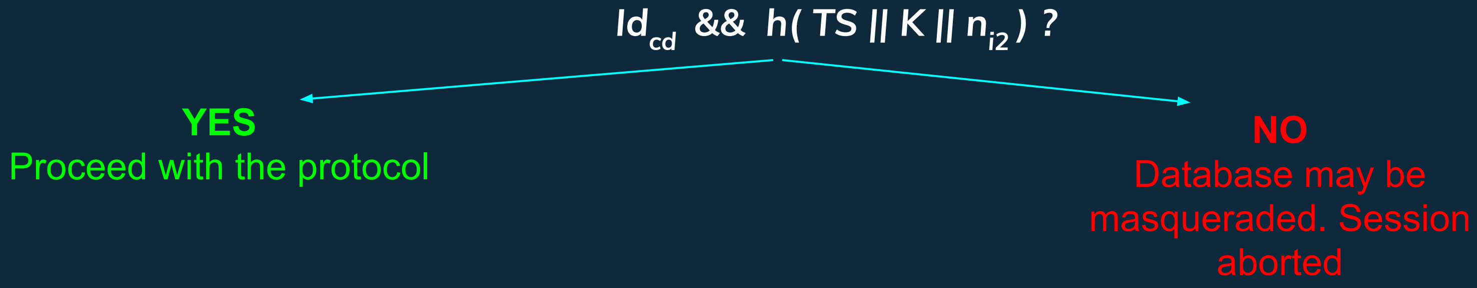
The Central Database choose from the access list of the requesting reader (r_i)a random tag *id* as *id*$_{cd}$ and the corresponding t_{cd}.

It prepares a random K and n_{i2}.

$R_i \leftarrow CD$: $\boldsymbol{n_{i2}\, ,\, h(f(r_{cd},t_{cd}))_m,\, h(f(r_i,t_{cd})||\, n_i\, ||\, n_j) \oplus id_{cd},\, h(\, id_{cd}||\, n_i\, ||\, n_j) \oplus K}$

$\boldsymbol{h(\, id_j\, ||\, n_{i2}\, ,\, r_i\,),\, h(\, TS\, ||\, K\, ||\, n_{i2}\,)}$

The reader checks $\boldsymbol{h(\, id_j\, ||\, n_i\, ,\, r_i\,)}$; gets id $_{cd}$ like server-less phase; gets K; checks $\boldsymbol{h(\, TS\, ||\, K\, ||\, n_{i2}\,)}$.



$\boldsymbol{Id_{cd}\ \&\&\ h(\, TS\, ||\, K\, ||\, n_{i2}\,)\ ?}$

YES
Proceed with the protocol

NO
Database may be masqueraded. Session aborted

Server-Mounted Authentication Phase

$R_i \rightarrow T_j$: $\boldsymbol{K, n_{i2}}$

$R_i \leftarrow T_j$: $\boldsymbol{n_{j2}, h(f(r_{cd},t_j))_m, (h(f(K,t_j)) \mathbin{||} n_{i2} \mathbin{||} n_{j2}) \oplus id_i}$

$R_i \rightarrow CD$: $\boldsymbol{n_{i2}, n_{j2}, h(f(r_{cd},t_j))_m, h(f(K,t_j) \mathbin{||} n_{i2} \mathbin{||} n_{j2}) \oplus id_i}$

The Database calculates $\boldsymbol{h(f(r_{cd},t_j))_m}$ and $\boldsymbol{h(f(K,t_j) \mathbin{||} n_{i2} \mathbin{||} n_{j2}) \oplus id_i}$ comparing id_j from the previous session with the received one. If they are consistent the reader is authenticated and further information may be transferred to it.

Tag Searching Phase

With desired tag id, the server-less authentication scheme can be used as tag searching scheme.

Security analysis

- Protection from replay
- Protection from DoS Attacks
- Protection from Spoofing Attacks

Thanks!

Any questions?

You can find me at:

- nife1600@student.miun.se