

Privacy issues in RFID systems

Myrto Arapinis

University of Birmingham

Outline

Context

Linking attacks

Analysing the French e-passport

Outline

Context

Linking attacks

Analysing the French e-passport

RFID definition and architecture

Definition

Radio Frequency Identification (**RFID**) is a method of remotely identifying objects or subjects using transponders (**tags** or **smartcards**) queried through a radio frequency channel.

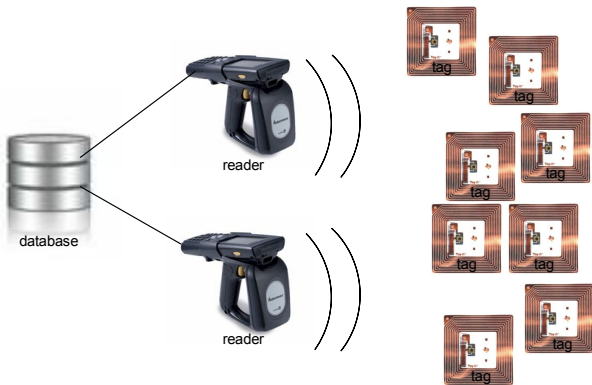
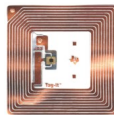


Figure: RFID architecture

Some examples

- ▶ Management of stocks



- ▶ Access control



- ▶ Electronic toll collection



- ▶ Electronic documents



- ▶ e-ticketing for public transport services



RFID technology specificities

- ▶ Wireless communication
- ▶ Tags/smartcards cannot be switched-off
- ▶ Tags/smartcards answer without the agreement of their bearers
- ▶ Communication range can be increased

Outline

Context

Linking attacks

Analysing the French e-passport

Tracking attacks

Identification protocol



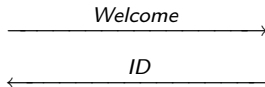
database



reader



tag



if $ID \in DB$ then open door

But!!

The tag can be traced

Tracking attacks

Identification protocol



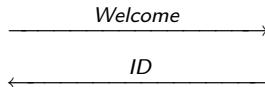
database



reader



tag



if $ID \in DB$ then open door

But!!

The tag can be traced

Unlinkability informally

Definition (ISO 15408)

Unlinkability ensures that a user may make multiple uses of a resource or service without other users being able to link these uses together.

A face is exposed for AOL searcher n° 4417749

Amongst AOL users, searcher n° 4417749 with Web search queries concerning

1. 60 single men,
2. dog that urinates on everything
3. landscapers in Lilburn, Ga,
4. several people with the last name Arnold
5. ...

⇒ No. 4417749 = Thelma Arnold, a 62-year-old from Lilburn, Ga, who loves her three dogs.

A face is exposed for AOL searcher n° 4417749

Amongst AOL users, searcher n° 4417749 with Web search queries concerning

1. 60 single men,
2. dog that urinates on everything
3. landscapers in Lilburn, Ga,
4. several people with the last name Arnold
5. ...

⇒ No. 4417749 = Thelma Arnold, a 62-year-old from Lilburn, Ga, who loves her three dogs.



Outline

Context

Linking attacks

Analysing the French e-passport

Basic Access Control (BAC)

Passport

(KE, KM)

$N_T, K_T \in_R \{0,1\}^{64}$

Reader

(KE, KM)

$N_R, K_R \in_R \{0,1\}^{64}$

← get_challenge

N_T →

← $\{N_R, N_T, K_R\}_{KE}, \text{MAC}_{KM}(\{N_R, N_T, K_R\}_{KE})$

→ $\{N_T, N_R, K_T\}_{KE}, \text{MAC}_{KM}(\{N_T, N_R, K_T\}_{KE})$

$K_{seed} = K_T \oplus K_R$

$K_{seed} = K_T \oplus K_R$

The French implementation of BAC

Passport

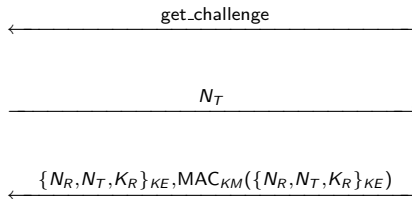
(KE, KM)

$N_T, K_T \in_R \{0,1\}^{64}$

Reader

(KE, KM)

$N_R, K_R \in_R \{0,1\}^{64}$



$$K_{seed} = K_T \oplus K_R$$

$$K_{seed} = K_T \oplus K_R$$

The French implementation of BAC

Passport

(KE, KM)

$N_T, K_T \in_R \{0,1\}^{64}$

Reader

(KE, KM)

$N_R, K_R \in_R \{0,1\}^{64}$

← get_challenge

N_T →

← $\{N_R, N_T, K_R\}_{KE}, \text{MAC}_{KM}(\{N_R, N_T, K_R\}_{KE})$

if MAC check fails → mac_err

$K_{seed} = K_T \oplus K_R$

$K_{seed} = K_T \oplus K_R$

The French implementation of BAC

Passport

(KE, KM)

$N_T, K_T \in_R \{0,1\}^{64}$

Reader

(KE, KM)

$N_R, K_R \in_R \{0,1\}^{64}$

← get_challenge

N_T →

← $\{N_R, N_T, K_R\}_{KE}, \text{MAC}_{KM}(\{N_R, N_T, K_R\}_{KE})$

if nonce check fail → nce_err

$K_{seed} = K_T \oplus K_R$

$K_{seed} = K_T \oplus K_R$

The French implementation of BAC

Passport

(KE, KM)

$N_T, K_T \in_R \{0,1\}^{64}$

Reader

(KE, KM)

$N_R, K_R \in_R \{0,1\}^{64}$

← get_challenge

N_T →

← $\{N_R, N_T, K_R\}_{KE}, \text{MAC}_{KM}(\{N_R, N_T, K_R\}_{KE})$

else

→ $\{N_T, N_R, K_T\}_{KE}, \text{MAC}_{KM}(\{N_T, N_R, K_T\}_{KE})$

$K_{seed} = K_T \oplus K_R$

$K_{seed} = K_T \oplus K_R$

An attack on the French e-passport (part1)

The attacker eavesdrop on Alice using her passport

Alice's passport

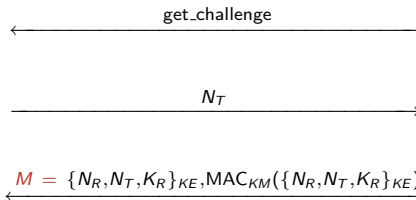
(KE, KM)

$N_T, K_T \in_R \{0,1\}^{64}$

Reader

(KE, KM)

$N_R, K_R \in_R \{0,1\}^{64}$



and records message M

An attack on the French e-passport (part2)

????

(KE', KM')

$N'_T, K'_T \in_R \{0,1\}^{64}$

Attacker

← get_challenge

N'_T →

← $M = \{N_R, N_T, K_R\}_{KE}, \text{MAC}_{KM}(\{N_R, N_T, K_R\}_{KE})$

An attack on the French e-passport (part2)

????

Attacker

(KE', KM')

$N'_T, K'_T \in_R \{0,1\}^{64}$

← get_challenge

N'_T →

← $M = \{N_R, N_T, K_R\}_{KE}, \text{MAC}_{KM}(\{N_R, N_T, K_R\}_{KE})$

MAC check fails

→ mac_err

MAC check failed $\Rightarrow KM \neq KM' \Rightarrow KM'$ is not Alice's key \Rightarrow
???? is not Alice

An attack on the French e-passport (part2)

????

Attacker

(KE', KM')

$N'_T, K'_T \in_R \{0,1\}^{64}$

← get_challenge

N'_T →

← $M = \{N_R, N_T, K_R\}_{KE}, \text{MAC}_{KM}(\{N_R, N_T, K_R\}_{KE})$

nonce check fails

→ nce_err

MAC check passed $\Rightarrow KM = KM' \Rightarrow KM'$ is Alice's key \Rightarrow ????
is Alice