Mécanismes de Restauration de Privacy pour les Systèmes RFID Offlines

Gildas AVOINE, **Iwen COISEL**, Tania MARTIN

Journées C2 – Octobre 2012

Goal of our Paper

Authentication protocol that

- restores privacy
- in case of compromised readers
- in offline RFID systems

Offline RFID Systems

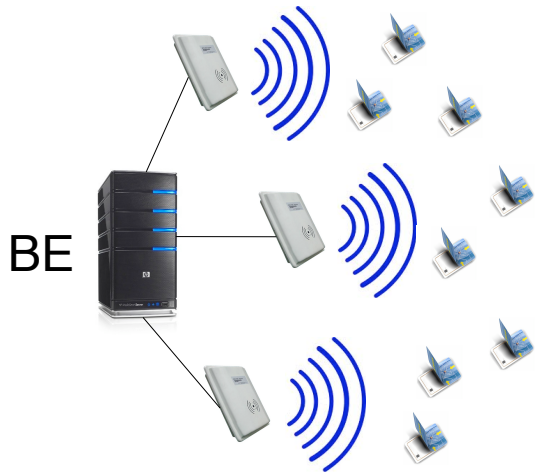
Online system

- Fixed readers
- Always connected to BE
- Readers do not store data to authenticate tags

Offline system

- Handheld readers
- Operate without BE
- Readers **must store** all data to authenticate tags

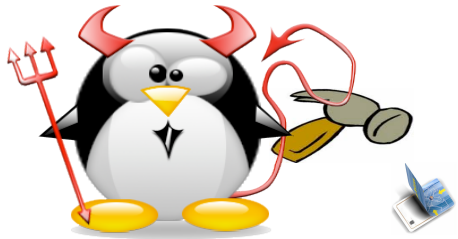
  i.e. **all tags' secrets**



Compromised Readers in Offline RFID Systems

Tag corruption

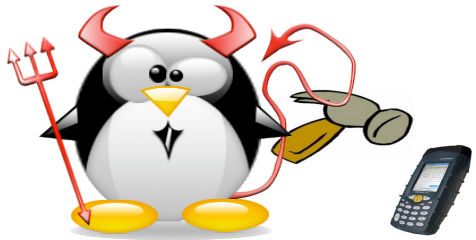
- $\mathcal{A}$ steals secrets of the corrupted tag



vs.

Compromised reader in offline RFID systems

- $\mathcal{A}$ steals **all tags' secrets** stored by reader



Privacy in RFID

Malicious traceability

An adversary $\mathcal{A}$ can distinguish two (challenge) tags over their different protocol executions

Privacy in RFID

Malicious traceability

An adversary $\mathcal{A}$ can distinguish two (challenge) tags over their different protocol executions

Tag corruption

- We consider that tags *do not* share secrets
- $\mathcal{A}$ can trace this corrupted tag

Privacy in RFID

Malicious traceability

An adversary $\mathcal{A}$ can distinguish two (challenge) tags over their different protocol executions

Tag corruption

- We consider that tags *do not* share secrets
- $\mathcal{A}$ can trace this corrupted tag

Compromised readers in offline RFID systems

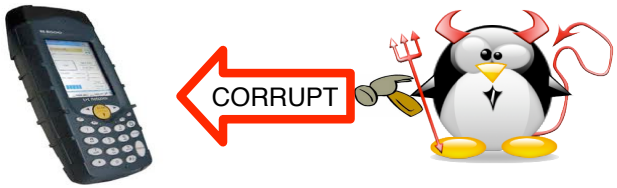
- $\mathcal{A}$ can trace **all tags**

$\Rightarrow$ **More powerful** attack than tag corruption

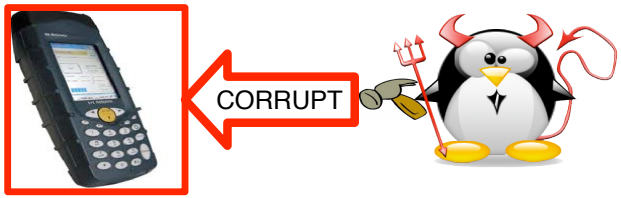
Outline

Our Protocol : Principle

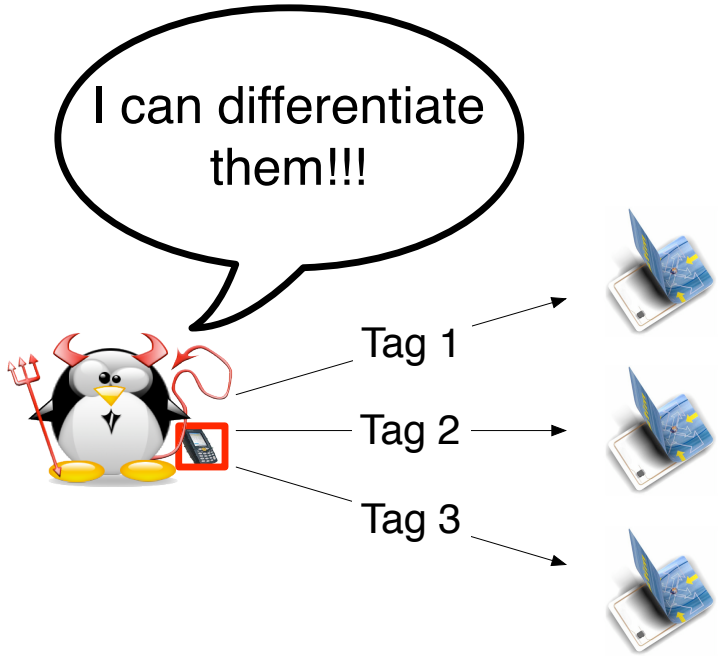
Our Protocol : Principle



Our Protocol : Principle



Our Protocol : Principle



Our Protocol : Principle

What can we do against this problem of traceability ?

Solution

- Repair the compromised reader
- Spread this info of repaired reader via tags' mobility

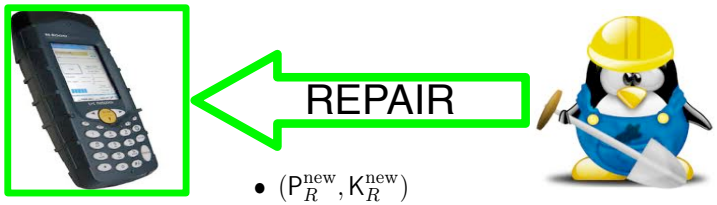
Our Protocol : Design Choices

- Challenge/response authentication protocol
  - Based on Needham-Schroeder [ACM-Comm-1978]
- Public-key crypto
  - For authentication
    - Cryptosystem (Enc/Dec) for T's answer
    - Signature scheme (Sign/Verif) for R's identity
      $\Rightarrow$ via C_R certificate
  - For privacy-restoring mechanism
    - Signature scheme (Sign/Verif) for info about repaired readers
      $\Rightarrow$ via $NewC_R$/$NewC_T$ certificates
- Secret-key crypto to personalize tags' secrets
  - Unique secret key s_{TR} by pair (T, R)

Our Protocol : Principle

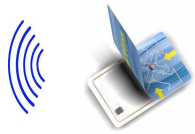
- $(\mathsf{P}_R^{\text{new}}, \mathsf{K}_R^{\text{new}})$
- $\mathsf{C}_R^{\text{new}}, \mathsf{v}_R^{\text{new}}$
- $\mathsf{Tab}_R^{\text{new}} = \{\forall T : (\mathsf{ID}_T, \mathsf{s}_{TR}^{\text{new}})\}$
- $\mathsf{NewC}_R^{\text{new}}$

Our Protocol : Principle



- $(\mathsf{P}_R^{\text{new}}, \mathsf{K}_R^{\text{new}})$
- $\mathsf{C}_R^{\text{new}}, \mathsf{v}_R^{\text{new}}$
- $\mathsf{Tab}_R^{\text{new}} = \{\forall T : (\mathsf{ID}_T, \mathsf{s}_{TR}^{\text{new}})\}$
- $\mathsf{NewC}_R^{\text{new}}$

Our Protocol : Principle



- Picks a nonce n_R

$\xrightarrow{\mathsf{C}_R,\ n_R}$

- Checks C_R
- $\mathsf{s}_{TR} = \mathrm{MAC}(\mathsf{k}_T||\mathsf{ID}_R||\mathsf{v}_R)$
- $E = \mathrm{Enc}_{\mathsf{P}_R}(\mathsf{ID}_R||n_R||\mathsf{s}_{TR})$

$\xleftarrow{E}$

- $\mathsf{ID}_R||n_R||\mathsf{s}_{TR} = \mathrm{Dec}_{\mathsf{K}_R}(E)$
- Authenticates T if $\mathsf{s}_{TR} \in \mathsf{Tab}_R$

Our Protocol : Principle

- Picks a nonce n_R

$\xrightarrow{\mathsf{C}_R,\ n_R}$

- Checks C_R
- $\mathsf{s}_{TR} = \mathrm{MAC}(\mathsf{k}_T||\mathsf{ID}_R||\mathsf{v}_R)$
- $E = \mathrm{Enc}_{\mathsf{P}_R}(\mathsf{ID}_R||n_R||\mathsf{s}_{TR})$
- Sends NewC_T

$\xleftarrow[\mathsf{NewC}_T]{E}$

- $\mathsf{ID}_R||n_R||\mathsf{s}_{TR} = \mathrm{Dec}_{\mathsf{K}_R}(E)$
- Authenticates T if $\mathsf{s}_{TR} \in \mathsf{Tab}_R$
- Checks NewC_T
  - → Updates its values
- Sends NewC_R if newer than NewC_T

$\xrightarrow{\mathsf{NewC}_R}$

- Checks NewC_R
  - → Updates its values

Our Protocol : Principle

- Picks a nonce n_R

$\xrightarrow{\mathsf{C}_R,\ n_R}$

- Checks C_R
- $\mathsf{s}_{TR} = \mathrm{MAC}(\mathsf{k}_T||\mathsf{ID}_R||\mathsf{v}_R)$
- $E = \mathrm{Enc}_{\mathsf{P}_R}(\mathsf{ID}_R||n_R||\mathsf{s}_{TR})$
- Sends NewC_T

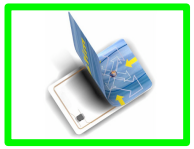
$\xleftarrow[\mathsf{NewC}_T]{E}$

- $\mathsf{ID}_R||n_R||\mathsf{s}_{TR} = \mathrm{Dec}_{\mathsf{K}_R}(E)$
- Authenticates T if $\mathsf{s}_{TR} \in \mathsf{Tab}_R$
- Checks NewC_T
  - → Updates its values
- Sends NewC_R if newer than NewC_T

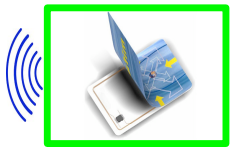
$\xrightarrow{\mathsf{NewC}_R}$

- Checks NewC_R
  - → Updates its values

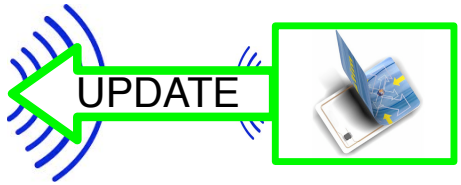
Our Protocol : Principle



Our Protocol : Principle

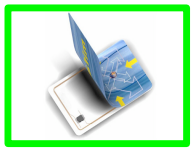


Our Protocol : Principle

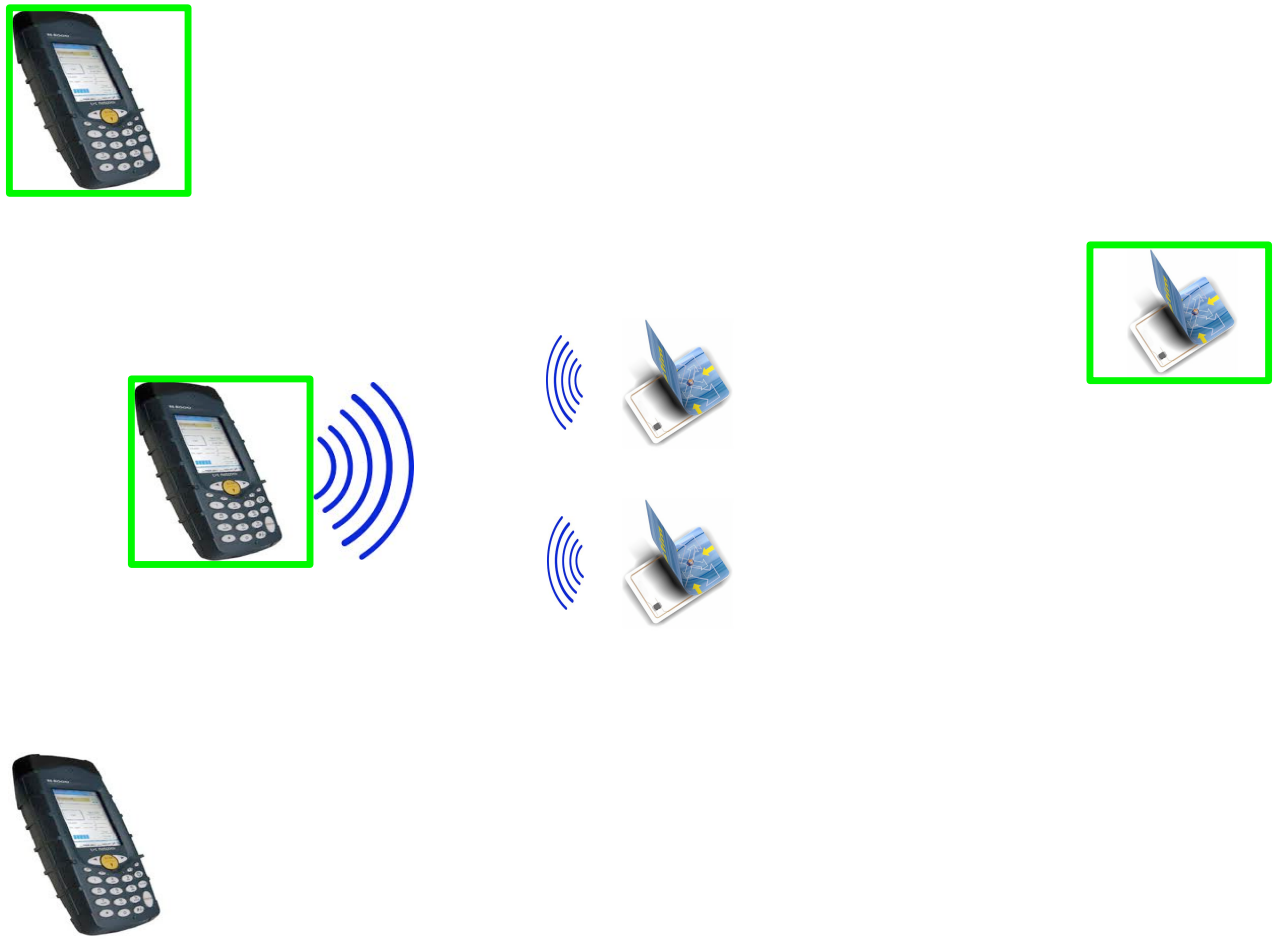


Our Protocol : Principle

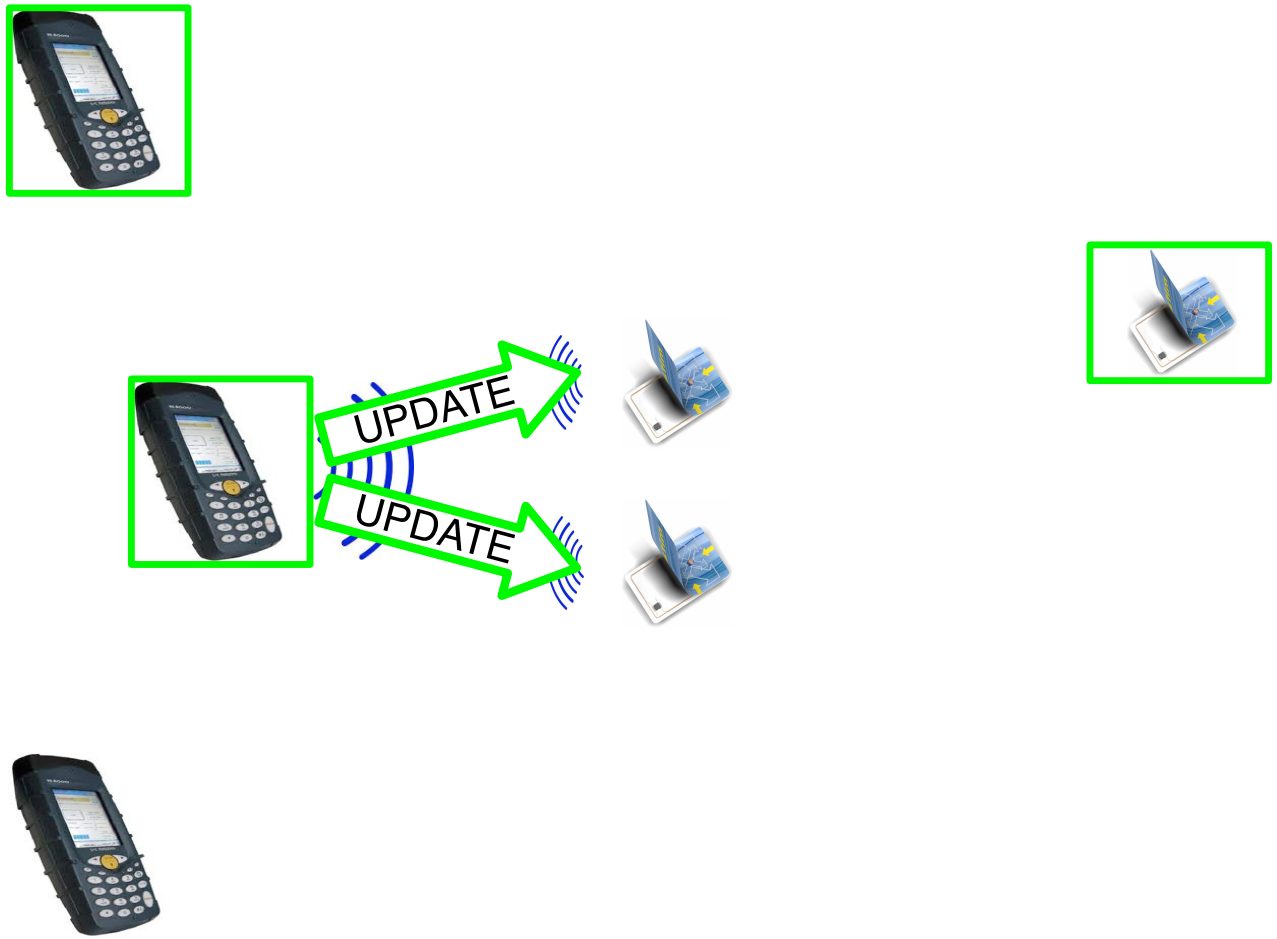
Our Protocol : Principle



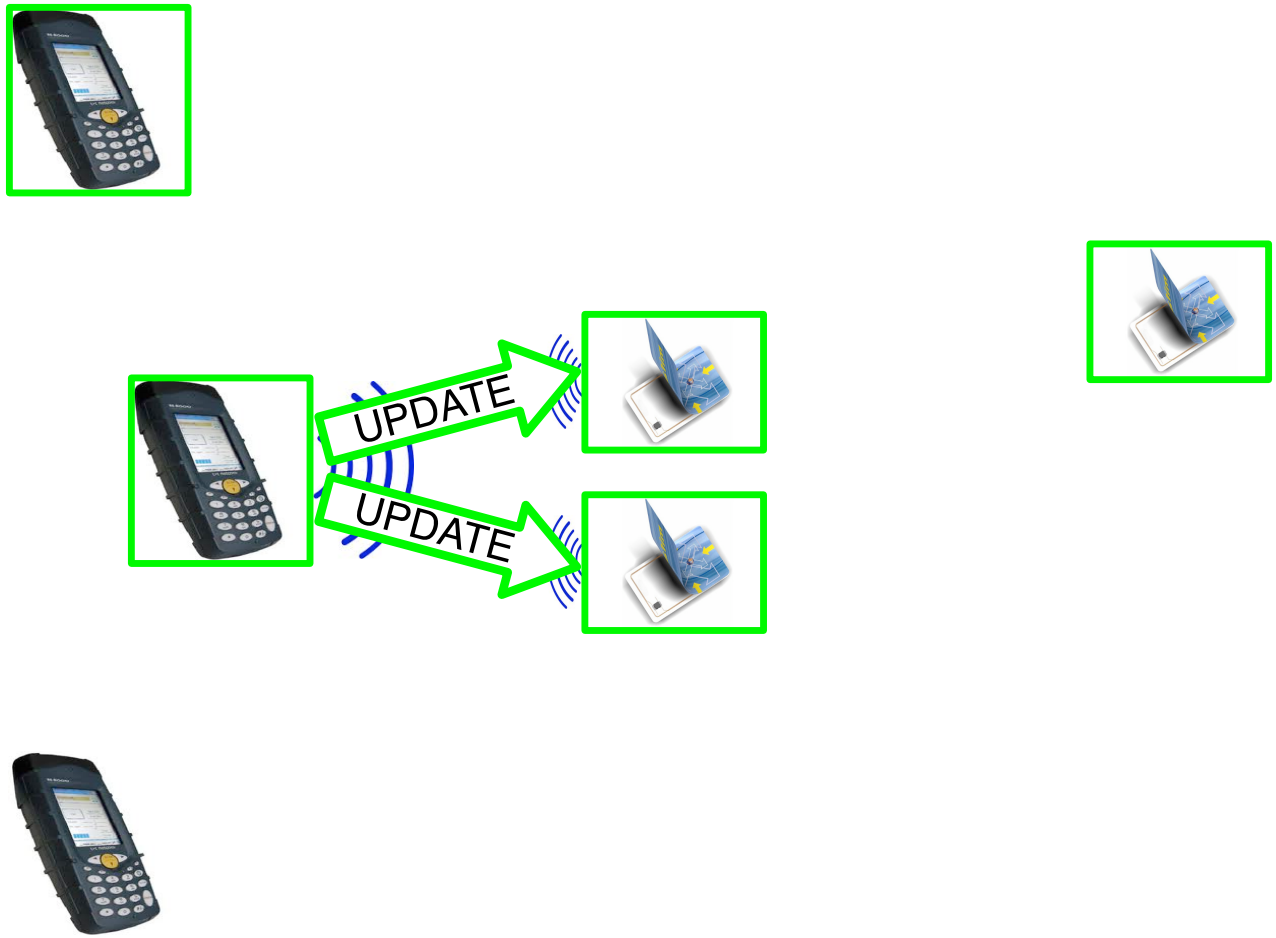
Our Protocol : Principle



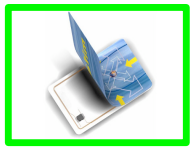
Our Protocol : Principle

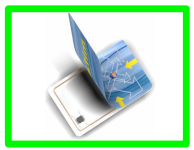


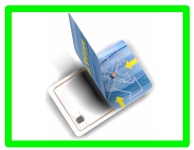
Our Protocol : Principle



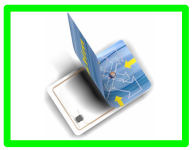
Our Protocol : Principle

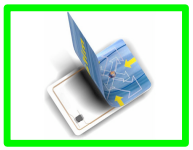


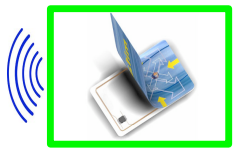




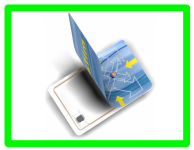
Our Protocol : Principle

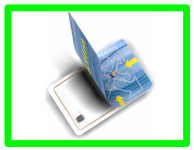




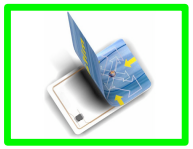


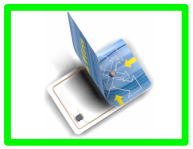
Our Protocol : Principle



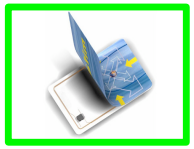


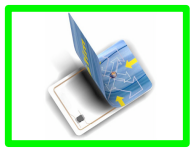
Our Protocol : Principle

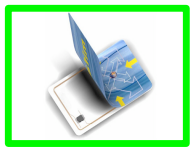




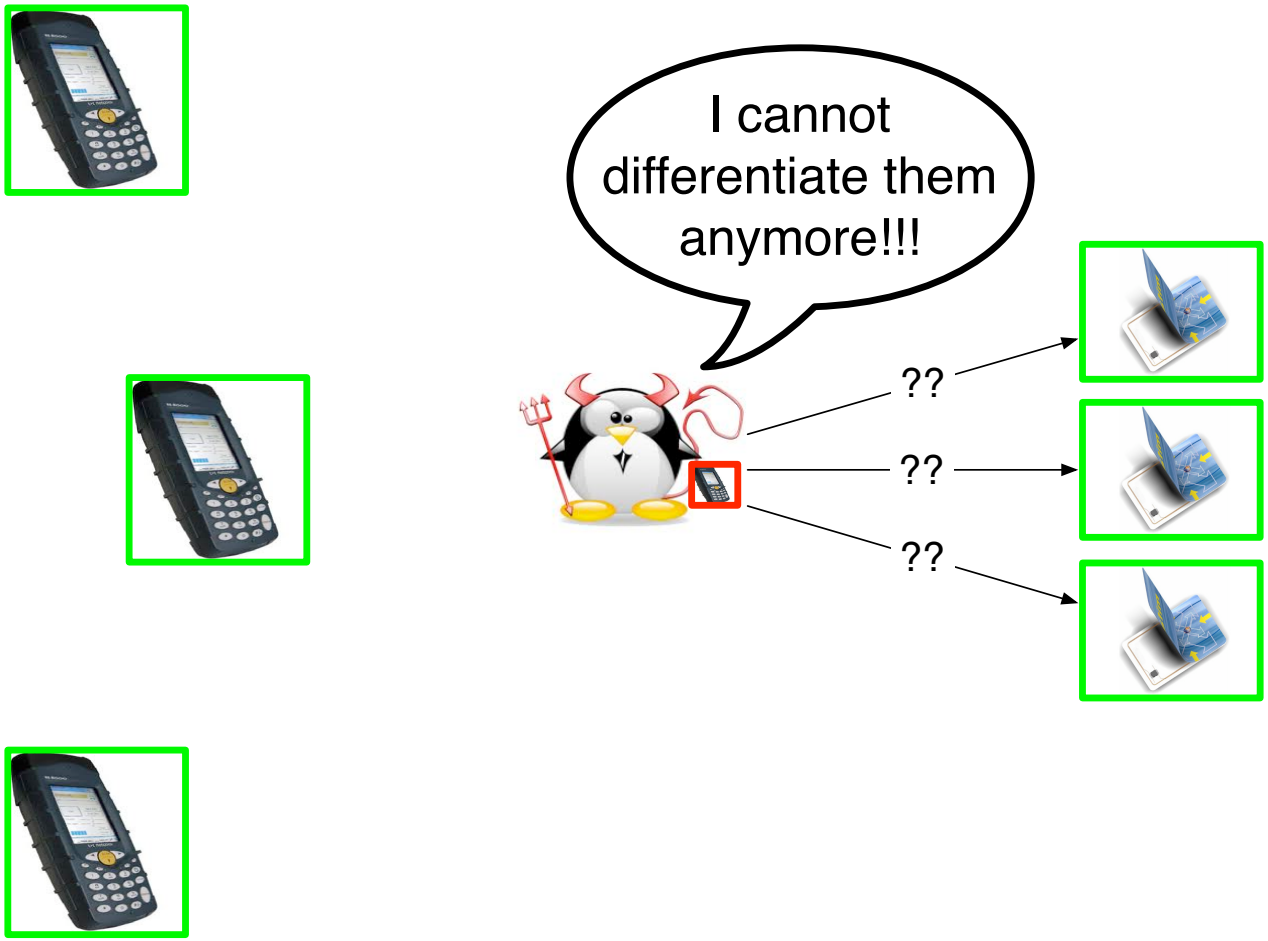
Our Protocol : Principle







Our Protocol : Principle



Outline

Our Protocol

Privacy Analysis

Efficiency Analysis

Implementation

Privacy Analysis

Privacy experiment (from Juels and Weis' model)

1. The challenger $\mathcal{C}$ initializes the RFID system $\mathcal{S}$.
2. $\mathcal{A}$ interacts with the whole system.
3. $\mathcal{A}$ chooses two challenge tags T and T', and gives them to $\mathcal{C}$.
4. $\mathcal{C}$ chooses a random bit b, and assigns $T_b = T$ and $T_{b\oplus 1} = T'$. Then $\mathcal{C}$ gives back T_b and $T_{b\oplus 1}$ to $\mathcal{A}$.
5. $\mathcal{A}$ interacts with the whole system.
6. $\mathcal{A}$ outputs a guess bit b'.

$\mathcal{A}$ wins if $b = b'$.

Adversary classes

- STANDARD [$\mathcal{A}$ can corrupt any tag (except challenge tags)]
- FORWARD [$\mathcal{A}$ can corrupt any tag]
- CORRUPT [$\mathcal{A}$ can corrupt any reader]
  - CORRUPT is composable with previous classes

  $\Rightarrow$ **4 possible adversaries**

Privacy Analysis

When the system is stable

- FORWARD-privacy
- CORRUPT-STANDARD-privacy

During the system update

- We define the average probability $\tau(t)$ to trace 1 tag
- When $t \nearrow$ then $\tau(t) \searrow$

$$\begin{aligned}\tau(t) &= \left(\frac{1}{2}+\epsilon(s)\right)\left(\frac{u(t)}{n}\right)\left(\frac{u(t)-1}{n-1}\right) \\ &\quad +\left(1-\frac{u(t)}{n}\right)\left(1-\frac{u(t)}{n-1}\right)+2\left(\frac{u(t)}{n-1}\right)\left(1-\frac{u(t)}{n}\right)\end{aligned}$$

where $u(t)$ = number of updated tags at time t

Outline

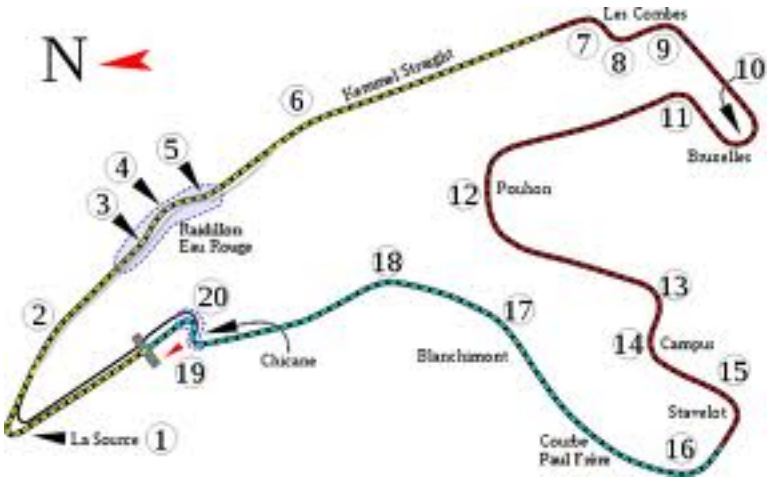
Case Study : 3-Day F1 Grand Prix

Goal

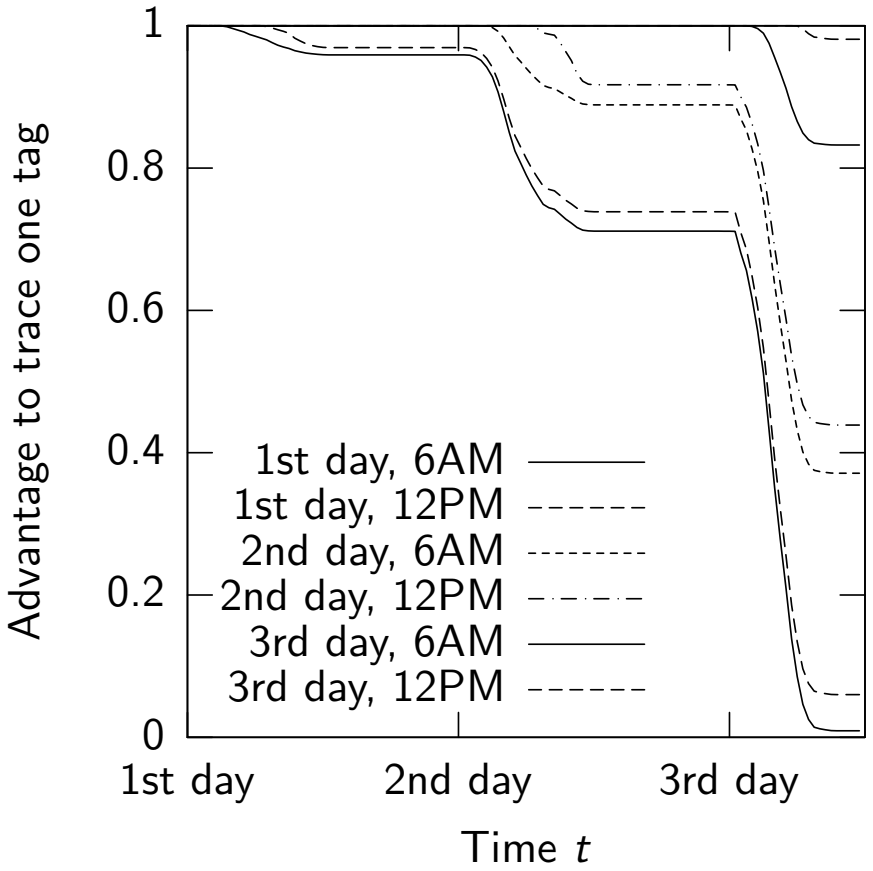
Analyze in practice our privacy-restoring mechanism

Experimental conditions

- 55 readers spread all over the area
- 102 110 tags
- 1 reader has been compromised and repaired



Case Study : Tracing 1 Tag During the Event



- Advantage $= |2\,\tau(t) - 1|$
- Curves depend on the update start time
- Influenced by the 1-day tickets

Outline

Implementation

- Consider the 3-day sport event data with
  - 55 readers
  - 10 compromised readers (at most)

	Our Protocol	$\Rightarrow$	JavaCard	
EEPROM	0.8 KB	$\Rightarrow$	72 KB	
Transmission	5953 bits	$\Rightarrow$	68.04ms	TOTAL
Tag computation	1 PK encryption + 2 certif verifs	$\Rightarrow$	331.7ms	$\approx$ 400ms

Conclusion

- Privacy-restoring mechanism
  - Can face the problem of compromised readers in offline systems
  - Via tags' mobility
- Efficient protocol in a real case study
  - When attack detected at the beginning of the event
    $\Rightarrow$ 99.5% of tags with a restored privacy
- Protocol deployable in practice
  - Tested and operable on JavaCard

Conclusion

- Privacy-restoring mechanism
  - Can face the problem of compromised readers in offline systems
  - Via tags' mobility
- Efficient protocol in a real case study
  - When attack detected at the beginning of the event
    $\Rightarrow$ 99.5% of tags with a restored privacy
- Protocol deployable in practice
  - Tested and operable on JavaCard

Thank You !