

# When Compromised Readers Meet RFID

Gildas Avoine   Cédric Lauradoux   Tania Martin

Université catholique de Louvain

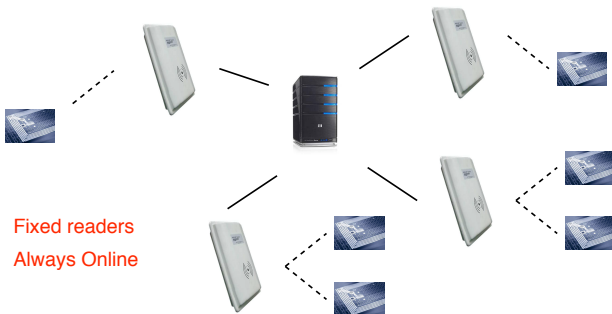
Belgium

July 1, 2009



# The context: Compromised readers in RFID

## Scenario 1



### Scenario 1

- Back-end trusted
- No compromised readers

# The context: Compromised readers in RFID

## Scenario 2

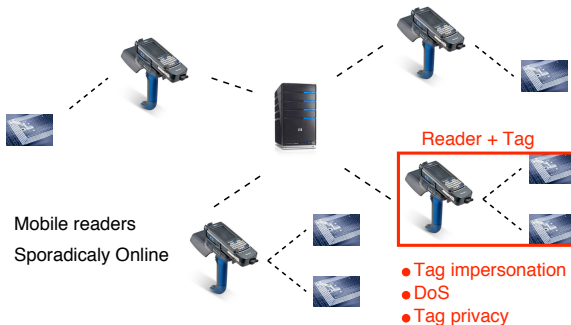


## Scenario 2

- Back-end trusted
- Compromised readers

# The context: Compromised readers in RFID

## Scenario 2



## Scenario 2

- Back-end trusted
- Compromised readers

# Outline

- 1 Available authentication protocols
- 2 Privacy with compromised readers
- 3 Conclusion

# Available authentication protocols

## Our selection

- ISO/IEC 9798 standard:
  - Symmetric-Key (SK) encryption
  - Signature
  - Hash function
  - Zero-Knowledge (ZK)
- GPS: zero-knowledge protocol with coupons [NESSIE]
- WIPR: challenge/response based on PKC [RFIDSec08]
- TanSL: hash-based challenge/response with secret computed on-the-fly [PerCom07]

# Available authentication protocols

Sum up: a first sort

	Scenario 1		Scenario 2		Area	Speed
	Impers.	DoS	Impers.	DoS		
SK Chall./Resp.	+	+	-	+	+	+
Signature - ZK	+	+	+	+	-	-
GPS	+	-	+	-	+	+
WIPR	+	+	-	+	+	-
TanSL	+	+	+	+	+	+

Our best candidates: TanSL and GPS

# Privacy with compromised readers

## Tag Privacy

### Information leakage

An adversary can extract useful side information related to the environment

### Malicious traceability

An adversary can correlate messages from a given tag over different protocol executions

### The Big Problem

- **Scenario 1:** 1 attack = privacy of 1 tag threatened
- **Scenario 2:** 1 attack = privacy of ALL the tags threatened

# Privacy with compromised readers

Privacy analysis of our candidates

Privacy	Scenario 1	Scenario 2
SK Chall./Resp.		
Signature - ZK		
GPS	-	-
WIPR		
TanSL	+	-

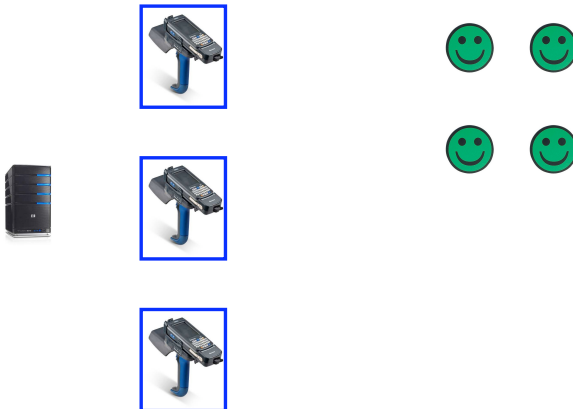
**NO TAG PRIVACY IN SCENARIO 2**

# Privacy with compromised readers

Our protocol: Principle

## Goal

Restore the security of the system without changing physically all the tags

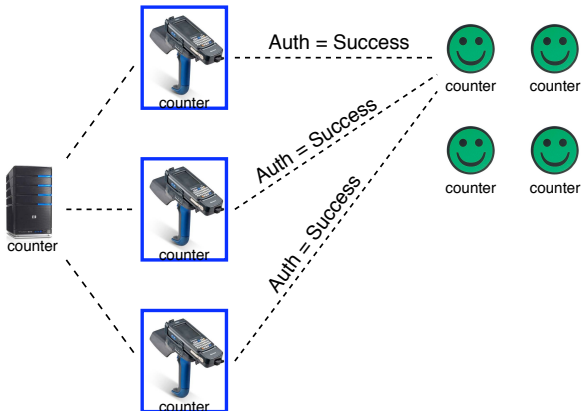


# Privacy with compromised readers

Our protocol: Principle

## Goal

Restore the security of the system without changing physically all the tags

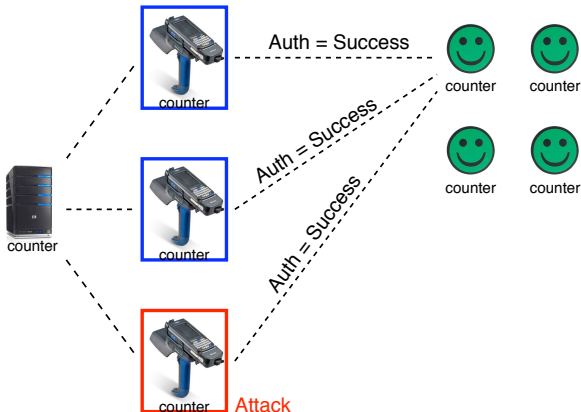


# Privacy with compromised readers

Our protocol: Principle

## Goal

Restore the security of the system without changing physically all the tags

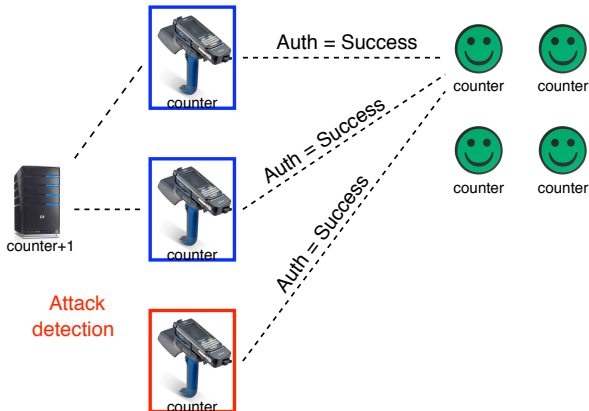


# Privacy with compromised readers

Our protocol: Principle

## Goal

Restore the security of the system without changing physically all the tags



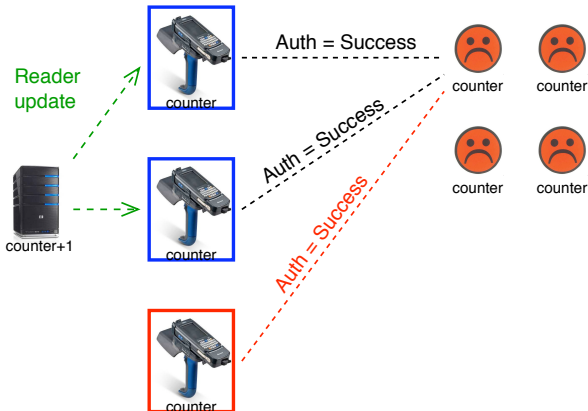


# Privacy with compromised readers

Our protocol: Principle

## Goal

Restore the security of the system without changing physically all the tags

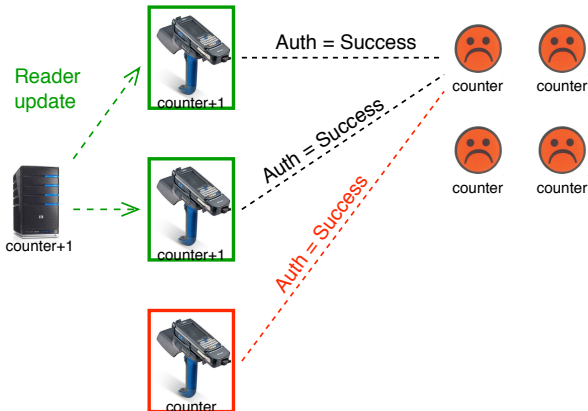


# Privacy with compromised readers

Our protocol: Principle

## Goal

Restore the security of the system without changing physically all the tags

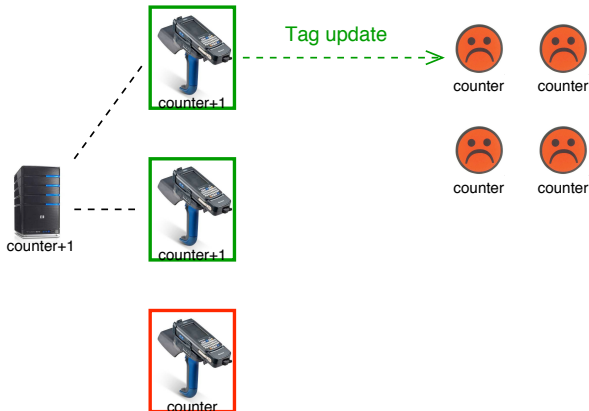


# Privacy with compromised readers

Our protocol: Principle

## Goal

Restore the security of the system without changing physically all the tags

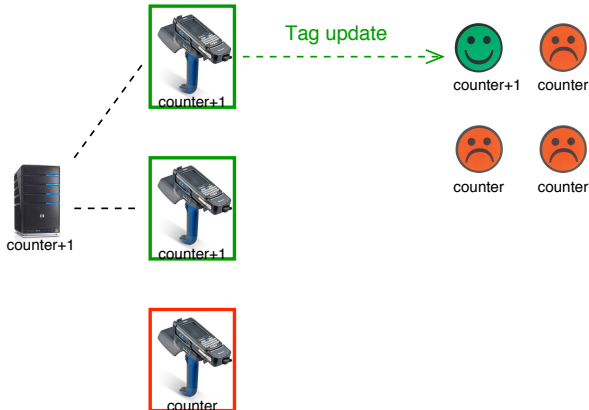


# Privacy with compromised readers

Our protocol: Principle

## Goal

Restore the security of the system without changing physically all the tags

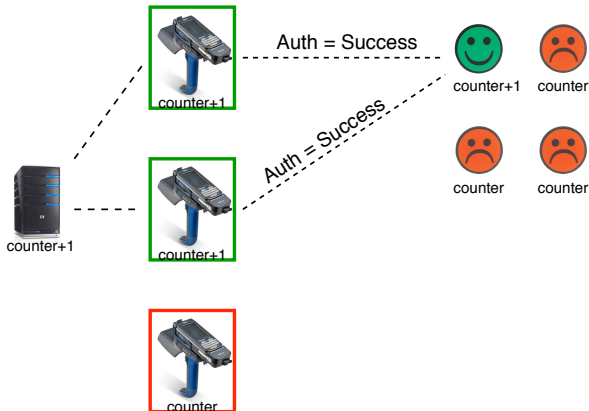


# Privacy with compromised readers

Our protocol: Principle

## Goal

Restore the security of the system without changing physically all the tags

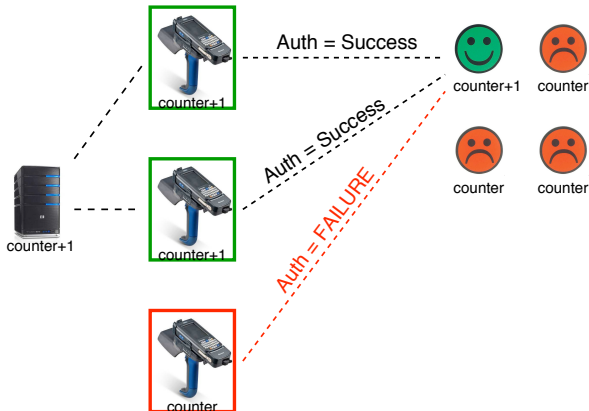


# Privacy with compromised readers

Our protocol: Principle

## Goal

Restore the security of the system without changing physically all the tags



# Privacy with compromised readers

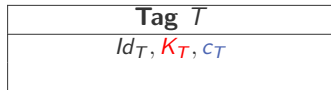
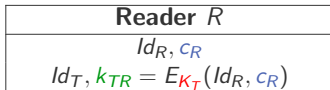
Our protocol: Initialization

Back-End $B$	Reader $R$	Tag $T$
$Id_R, Id_T, K_T, C_B$	$Id_R, C_R$ $Id_T, k_{TR}$	$Id_T, K_T, C_T$

- SK-based encryption
- $R$  sporadically connected to  $B$  through a secure channel
- Update counters:  $C_B, C_R, C_T$  initially synchronized
- $T$ 's unique long-term key  $K_T$
- $T$ 's authentication key  $k_{TR} = E_{K_T}(Id_R, C_R)$

# Privacy with compromised readers

Our protocol: Authentication



Picks  $n_R$

$\xrightarrow{Id_R, c_R, n_R}$

# Privacy with compromised readers

Our protocol: Authentication

Reader $R$
$Id_R, c_R$ $Id_T, k_{TR} = E_{K_T}(Id_R, c_R)$

Picks  $n_R$

$\xrightarrow{Id_R, c_R, n_R}$

Tag $T$
$Id_T, K_T, c_T$

Checks  $c_R$

- If  $c_R \geq c_T$ :
  - Computes the key  
 $k_{TR} = E_{K_T}(Id_R, c_R)$
  - Picks  $n_T$
  - Encrypts  $(n_R, n_T)$   
with  $k_{TR}$
- If  $c_R < c_T$ : aborts

# Privacy with compromised readers

Our protocol: Authentication

Reader $R$
$Id_R, c_R$ $Id_T, k_{TR} = E_{K_T}(Id_R, c_R)$

Tag $T$
$Id_T, K_T, c_T$

Picks  $n_R$

$\xrightarrow{Id_R, c_R, n_R}$

Checks  $c_R$

- If  $c_R \geq c_T$ :
  - Computes the key  
 $k_{TR} = E_{K_T}(Id_R, c_R)$
  - Picks  $n_T$
  - Encrypts  $(n_R, n_T)$   
with  $k_{TR}$

- Decrypts  $E_{k_{TR}}(n_R, n_T)$
- Verifies  $n_R$
- Recovers  $n_T$

$\xleftarrow{E_{k_{TR}}(n_R, n_T)}$

- If  $c_R < c_T$ : aborts

# Privacy with compromised readers

Our protocol: Authentication

Reader $R$
$Id_R, C_R$ $Id_T, k_{TR} = E_{K_T}(Id_R, C_R)$

Tag $T$
$Id_T, K_T, C_T$

Picks  $n_R$

$\xrightarrow{Id_R, C_R, n_R}$

Checks  $C_R$

- If  $C_R \geq C_T$ :
  - Computes the key  $k_{TR} = E_{K_T}(Id_R, C_R)$
  - Picks  $n_T$
  - Encrypts  $(n_R, n_T)$  with  $k_{TR}$

- Decrypts  $E_{k_{TR}}(n_R, n_T)$
- Verifies  $n_R$
- Recovers  $n_T$

$\xleftarrow{E_{k_{TR}}(n_R, n_T)}$

- If  $C_R < C_T$ : aborts

$\xrightarrow{n_T}$

Checks  $n_T$  and if  $C_R > C_T$ :  
 $C_T \leftarrow C_R$

# Privacy with compromised readers

Our protocol: Key update

Back-End $B$
$Id_R, Id_T, K_T, C_B$

Reader $R$
$Id_R, C_R$ $Id_T, k_{TR} = E_{K_T}(Id_R, C_R)$

- Increments  $C_B$ :  
 $C_B \leftarrow C_B + 1$
- $\forall R \forall T$ , computes the new key:  
 $k_{TR,up} = E_{K_T}(Id_R, C_B)$

# Privacy with compromised readers

Our protocol: Key update

Back-End $B$
$Id_R, Id_T, K_T, C_B$

Reader $R$
$Id_R, C_R$ $Id_T, k_{TR} = E_{K_T}(Id_R, C_R)$

- Increments  $C_B$ :  
 $C_B \leftarrow C_B + 1$
- $\forall R \forall T$ , computes the new key:  
 $k_{TR_{up}} = E_{K_T}(Id_R, C_B)$

$\xrightarrow{Id_T, C_B, k_{TR_{up}}}$

- $C_R \leftarrow C_B$
- $k_{TR} \leftarrow k_{TR_{up}}, \forall T.$

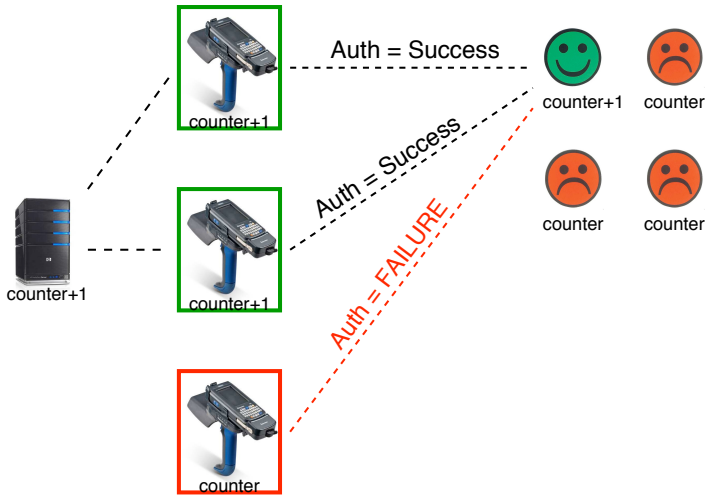
# Privacy with compromised readers

## Our comparison

	Scenario 1			Scenario 2		
	Impers.	DoS	Privacy	Impers.	DoS	Privacy
GPS	+	-	-	+	-	-
mGPS	+	-	+	+	-	-
TanSL	+	+	+	+	+	-
Our protocol	+	+	+	+	+	+

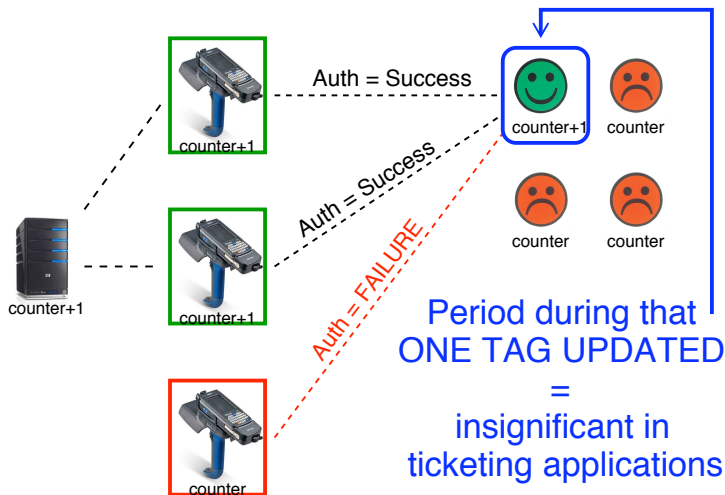
# Privacy with compromised readers

Our protocol: an open problem



# Privacy with compromised readers

Our protocol: an open problem



# Conclusion

- Problem of **compromised readers**
- Analysis of existing authentication protocols
- Presentation of **privacy issues** in such context
- Proposition of an **authentication protocol** resistant to:
  - Tag impersonation
  - DoS
  - Tag privacy

in an RFID system w/o compromised readers