School of
Information Systems

SMU
SINGAPORE MANAGEMENT UNIVERSITY

Some Recent Development in RFID Privacy Models

Robert H. Deng
School of Information Systems
Singapore Management University

Introduction

- RFID tags are low-cost electronic devices, from which stored info can be collected by an RFID reader efficiently and at a distance without line of sight

- RFID has found numerous applications, from warehouse inventory control, supermarket checkout counters, e-ticket, to e-passport

RFID Triggered Significant Concerns on Security & Privacy

- **Perfect working condition for attackers**
  - Tags can be read or traced by malicious readers from a distance w/o its owner's awareness
- **Security**
  - Tag authentication: ensure data collected not from fake tag & prevent database pollution
  - Reader authentication: prevent unauthorized access to/or tampering with tag data
- **Privacy**
  - Anonymity: Confidentiality of the tag identity
  - Untraceability: Unlinkability of the tag's transactions

Cryptographic Protocols for RFID Privacy

- Numerous lightweight RFID protocols for low-cost tags have been proposed
  - Use simple operations (XOR, bit inner product, CRC, etc)

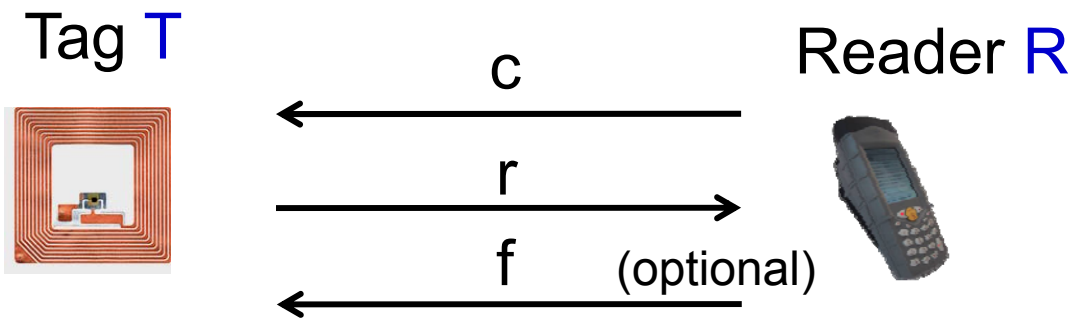
- Most of them have been broken
  - T. van Deursen and S. Radomirovic: Attacks on RFID Protocols, *ePrint Archive: Report 2008/310*

- Need to investigate formal RFID security and privacy models which are fundamental to the design and analysis of robust RFID systems

Assumptions

- **S** = $\{T_1,\ldots,T_n\}$ - polynomial-size group of tags
- **R/D** - Reader/Database have secure connection
- Adversary **A** has complete control over communications between reader and tags

Canonical RFID Protocol π



- Shorthand notation: $(c, r, f) \leftarrow \pi(R, T)$

Adversary

- **Interactions between A and protocol parties R and T occur through 4 oracles**
  - **O_1 - Launch():** return a session id sid and the 1st message c
  - **O_2 - SendTag(sid, c, T):** return r, the response of tag T
  - **O_3 - SendReader(sid, r):** return f, the response of Reader
  - **O_4 - Corrupt(T):** return the secret information and state of tag T

Ind-Privacy: Indistinguishability of two tags

JW06 (Jules & Weis, PerCom 2007)

Experiment:

- $\{T_i, T_j\} \leftarrow \boldsymbol{A_1}^{O1,O2,O3,O4}(R, \mathbf{S})$;
- $b \in \{0, 1\}$;
- If $b = 0$ then $T_c = T_i$, else $T_c = T_j$;
- $\mathbf{S'} = \mathbf{S} - \{T_i, T_j\}$;
- $b' \leftarrow \boldsymbol{A_2}^{O1,O2,O3,O4}(R, \mathbf{S'}, T_c)$.

$\boldsymbol{A_1}$ not allowed to query O_4 on T_i and T_j

$\boldsymbol{A_2}$ not allowed to query O_4 on T_c

- The advantage of adversary A = $|Pr[b'=b]-1/2|$
- **No protocol has been directly proven to satisfy Ind-Privacy**

Unp*-Privacy (Ha, Moon, Zhou & Ha, *ESORICS 2008;* Lai, Deng, Li, ACNS 2010)

Experiment:

- $T_c \leftarrow \boldsymbol{A_1}^{O1,O2,O3,O4}(R, \boldsymbol{S})$;
- $b \in \{0, 1\}$;
- ***When*** $\boldsymbol{A_2}$ makes queries to O_1, O_2, O_3 on T_c
  - If b = 0, return oracles' responses
  - Else (b = 1)
    - return $c \in_R \mathbb{C}$ if query O_1
    - return $r \in_R \mathbb{R}$ if query O_2
    - Return $f \in_R \mathbb{F}$ if query O_3
- $b' \leftarrow \boldsymbol{A_3}$

A_1 & A_2 not allowed to query O_4 on T_c

- The advantage of adversary *A* = |Pr[b'=b]-1/2|
- **Some protocols have been proven to satisfy Unp*-privacy**

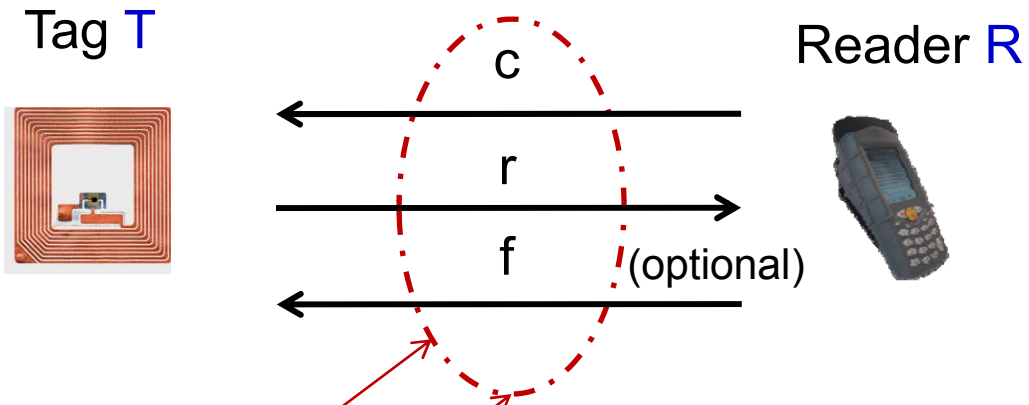
School of Information Systems

SMU SINGAPORE MANAGEMENT UNIVERSITY

Relationships (Ma, Li, Deng, Li, CCS09)

- **Ind-privacy $\Rightarrow!$ Unp*-privacy**
  - Assume that (c, r, f)$\leftarrow \pi$(R, T) satisfies Ind-privacy
  - Let (c, r|r, f) $\leftarrow \pi$'(R,T)
  - π'(R,T) also satisfies Ind-privacy, but it does not satisfy Unp*-privacy
- **Ind-privacy $\Leftarrow$ Unp*-privacy**
- **Minimal requirement for RFID systems to achieve RFID system privacy**
  - Unp*-privacy $\Leftarrow\Rightarrow$ PRF

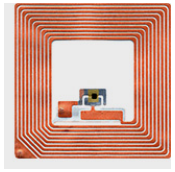
RFID Privacy Preserving Authentication Protocol Design



- **Privacy requirements**
  - **Anonymity:** Confidentiality of the tag identity
  - **Untraceability:** Unlinkability of the tag's transactions

Symmetric Key Crypto Based Solution

Tag T (ID_T, K_T)



Reader R

Database D	
Tag ID	Tag Secret
ID_{T1}	K_{T1}
ID_{T2}	K_{T2}
.....	
ID_{Tn}	K_{Tn}

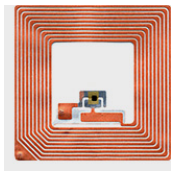
c ←

$r = prf(K_T \mid c \ldots)$, ~~$ID_T$~~ →

Exhaustive research to find a matching K_T and then ID_T

f (optional) ←

Symmetric Key Crypto & Counter Based Solution



Tag T (K_T, Ctr)

Reader R

Database D			
ID'	**ID**	**Secret**	**Ctr**
ID'_{T1}	ID_{T1}	K_{T1}	Ctr_{T1}
ID'_{T2}	ID_{T2}	K_{T2}	
	.....		
ID_{Tn}	ID'_{Tn}	K_{Tn}	Ctr_{Tn}

c

$ID'_T = h(K_T, Ctr)$
$Ctr \leftarrow Ctr + 1$

ID'_T, ...

Use ID'_T as index to the database

f (optional)

Must be able to recover from disynchronization attack

Public Key Crypto Based Solution

Tag T (ID_T, K_T, P_R)

Reader R (S_R)

Database D	
Tag ID	Tag Secret
ID_{T1}	K_{T1}
ID_{T2}	K_{T2}
.....	
ID_{Tn}	K_{Tn}

c

$r = PK_R(K_T \mid ID_T \mid c \ ...)$ **Use ID_T as index to look for K_T**

f (optional)

PKC based protocols do not satisfy Unp*-privacy!

Summary

- Ind-Privacy and Unp*-Privacy models
- No protocol has been directly proven to satisfy Ind-Privacy
- Symmetric key based protocols can be designed to satisfy Unp*-privacy, but not public key based protocols
- ZK-privacy model **(Deng, Li, Yung, Zhao, ESORICS 2010)**
  - Output of real world experiment and output of simulated world experiment are indistinguishable
  - Both symmetric key and public key protocols can be designed to satisfy zk-privacy

Acknowledgement

Junzuo LAI[1]

Tieyan LI[2]

Yingjiu LI[1]

Changshe MA[3]

Yunlei Zhao[4]

1. Singapore Management University
2. Institute for Infocomm Research, Singapore
3. South China Normal University
4. Fudan University

Thank You!