Vulnerability Analysis of a Mutual Authentication Scheme under the EPC Class-1 Generation-2 Standard

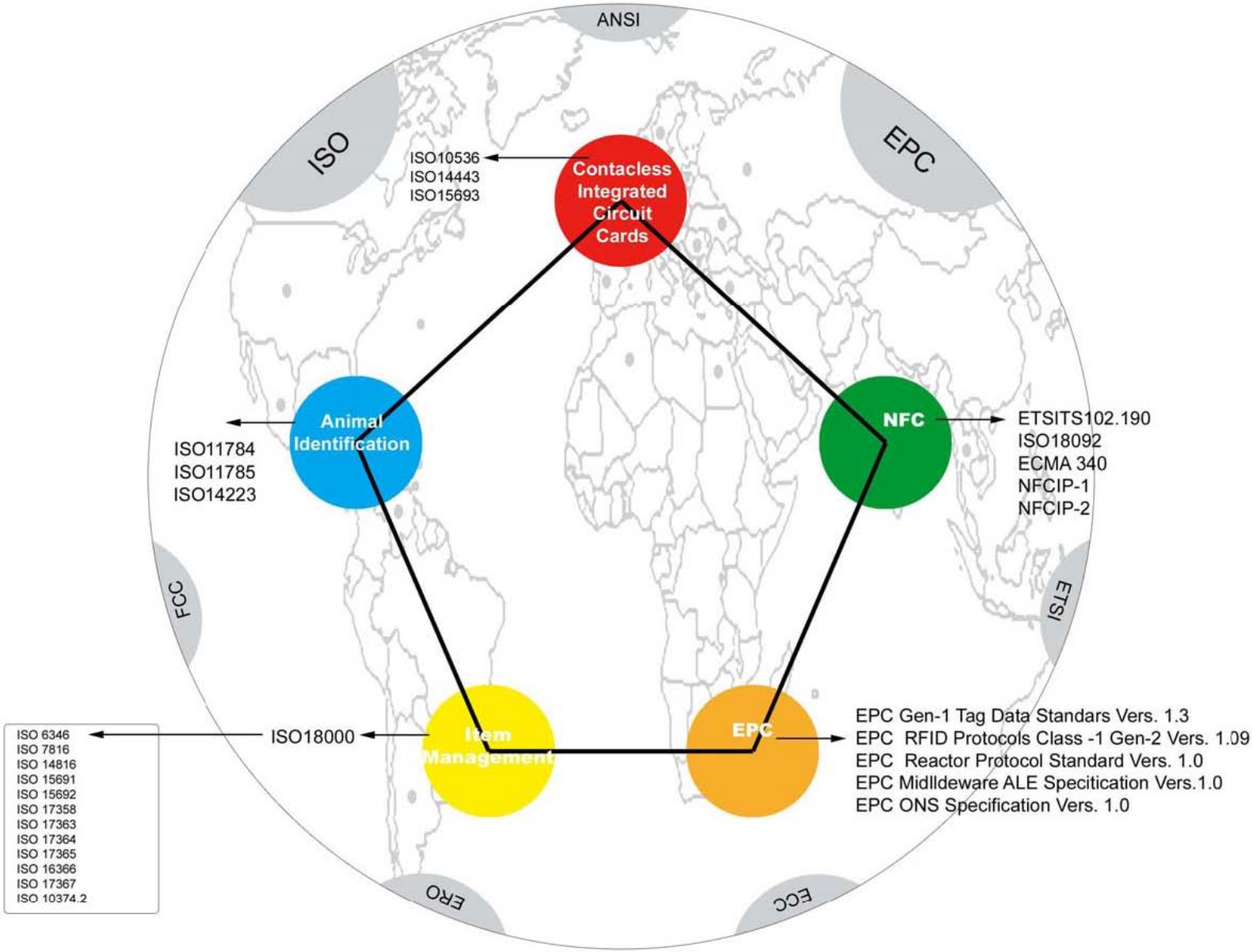
Pedro Peris-Lopez[1] Tieyan Li[2] Tong-Lee Lim[2]
Julio C. Hernandez-Castro[1] Juan M. Estevez-Tapiador[1]

[1]Computer Science Department, Carlos III University of Madrid
[2]Institute for Infocomm Research, A*STAR Singapore

Workshop on RFID Security
9-11 July, 2008, Budapest

Outline

RFID Standards



EPC-C1G2 and ISO 18000-6C

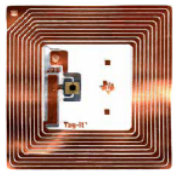
Tags specifications

- Tags are passive
- Tags have very constrained computing and storage capabilities
- Tags have on chip a 16-bit Pseudo-Random Number Generator and 16-bit Cyclic Redundancy Code (CRC) checksum
- Tags have two 32-bit PINs: Kill and Access

Tags Operations

- **Select:** select a subset of the tag population
- **Inventory:** identify a tag
- **Access:** interact with individual tags

Select Command



[1] Reader issues a Query

Query Request

[2] Generates RN16
while (RN16 <> 0)
RN16 - -
Tag backscatters RN16

RN16

[3] Reader acknowledges Tag with an ACK including RN16

ACK(RN16)

PC, EPC, CRC16

[4] If valid RN16 :
Tag answers with PC, EPC, CRC16
If invalid RN16 : No reply

Select command: EPC is transmitted as plain text!

[1] Reader issues a Query

Query Request

[2] Generates RN16
while (RN16 <> 0)
RN16 - -
Tag backscatters RN16

RN16

[3] Reader acknowledges Tag with an ACK including RN16

ACK(RN16)

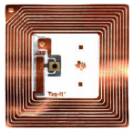
PC, EPC, CRC16

[4] If valid RN16 :
Tag answers with PC, EPC, CRC16
If invalid RN16 : No reply

Privacy **Tracking** **Spoofing**

Access Command



[5] Reader issues ReqRN using the same RN16

ReqRN(RN16) →

[6] If valid RN16 :
Tag responds with handle: RN16'
If invalid RN16 : No reply

← handle

[7.1] Reader issues ReqRN using the handle

ReqRN(handle) →

[7.2] Tag verifies the handle
Tag ignores command if the handle does not match.

← RN16'

PIN[31:16] ⊕ RN16'|| handle || CRC →

MSB

ReqRN(handle) →

← RN16''

PIN[15:10 ⊕ RN16''|| handle || CRC →

LSB

Access Command: PIN can be disclosed!

Tag-Reader Mutual Authentication Protocol

Divyan Konidala, Zeen Kim, and Kwangjo Kim.
A Simple and Cost-Effective RFID Tag-Reader Mutual Authentication Scheme (RFIDSec'07, July 2007) [2]

Objectives

- Tag-Reader mutual authentication:
  - Simple, lightweight, **secure?**
- A better cover-code or obscure tag Access Password
  - **Access and Kill password protection?**
- Under the EPCglobal framework
  - No cryptographic primitives (hash functions, ciphers, etc.)
- The proposed scheme utilizes tag's already existing:
  - 16-bit PRNG
  - Bitwise XOR
  - Access and Kill Password

Tag-Reader Mutual Authentication Protocol

Tag ⇒Reader: EPC, RN_1^{Tag}, RN_2^{Tag}

Reader ⇒ Tag: RN_1^{Rdr}, RN_2^{Rdr}, $CCPwd_{M1}$, $CCPwd_{L1}$, RN_3^{Rdr}, RN_4^{Rdr}

$CCPwd_{M1} = APWD_M \oplus PAD_1$

$CCPwd_{L1} = APWD_L \oplus PAD_2$

Tag: Verify $CCPwd_{M1}$ and $CCPwd_{L1}$

Tag ⇒ Reader: RN_3^{Tag}, RN_4^{Tag}, $CCPwd_{M2}$, $CCPwd_{L2}$

$CCPwd_{M2} = APWD_M \oplus PAD_3$

$CCPwd_{L2} = APWD_L \oplus PAD_4$

Reader: Verify $CCPwd_{M2}$ and $CCPwd_{L2}$

[1] $TRMA : PAD_i = PadGen(RN_i^{Tag}, RN_i^{Reader})[APWD]$

$TRMA^+ : PAD_i = PadGen(PadGen(RN_i^{Tag}, RN_i^{Reader})[APWD], RN_i^{Tag})[KPWD]$

Pad Generation Function - PadGen(.)

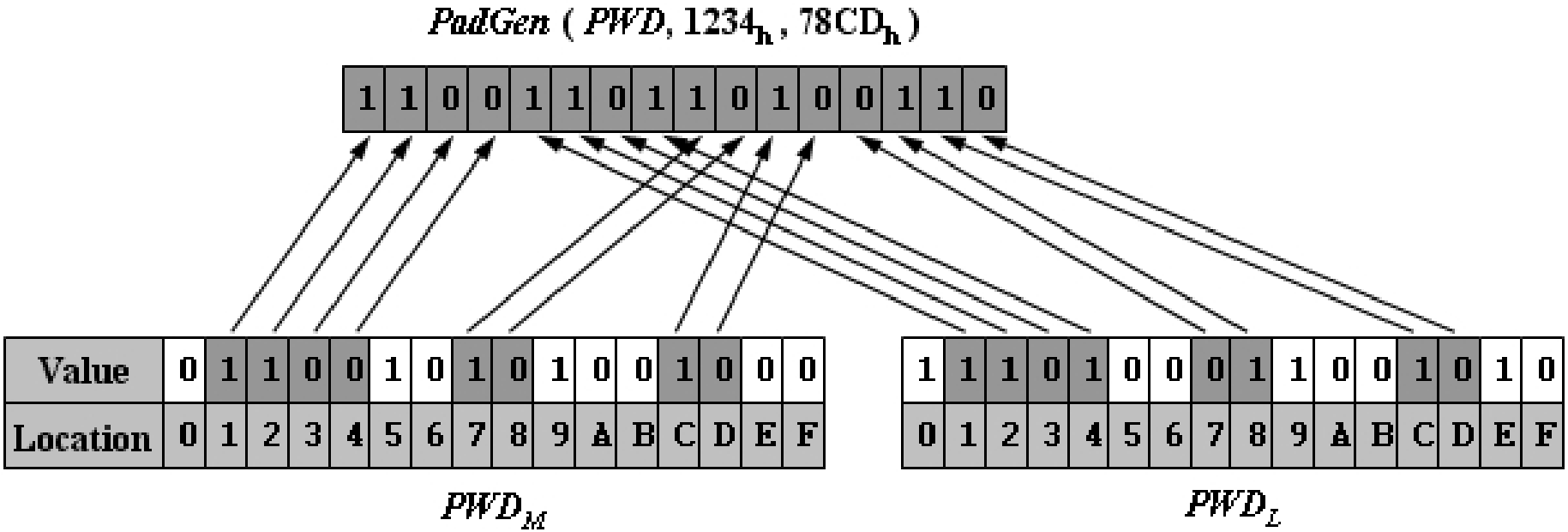
$$PAD_i = PadGen(PadGen(RN_i^{Tag}, RN_i^{Reader})[APWD], RN_i^{Tag})[KPWD] \quad (1)$$

$$\begin{aligned} XPWD &= XPWD_M \,||\, XPWD_L \\ XPWD_M &= b_0\, b_1\, b_2 \ldots\ldots b_{13}\, b_{14}\, b_{15} \\ XPWD_L &= b_{16}\, b_{17}\, b_{18} \ldots\ldots b_{29}\, b_{30}\, b_{31} \end{aligned}$$

$$\begin{aligned} RN_i^{Tag} &= H_{i,0}^{Tag}\, H_{i,1}^{Tag}\, H_{i,2}^{Tag}\, H_{i,3}^{Tag} \\ RN_i^{Rdr} &= H_{i,0}^{Rdr}\, H_{i,1}^{Rdr}\, H_{i,2}^{Rdr}\, H_{i,3}^{Rdr} \end{aligned}$$

$$\begin{aligned} & PadGen(RN_i^{Tag}, RN_i^{Rdr})[XPWD] \\ = \;& b_{H_{i,0}^{Tag}}\, b_{H_{i,1}^{Tag}}\, b_{H_{i,2}^{Tag}}\, b_{H_{i,3}^{Tag}} \,||\, b_{H_{i,0}^{Tag}+16}\, b_{H_{i,1}^{Tag}+16}\, b_{H_{i,2}^{Tag}+16}\, b_{H_{i,3}^{Tag}+16} \,|| \\ & b_{H_{i,0}^{Rdr}}\, b_{H_{i,1}^{Rdr}}\, b_{H_{i,2}^{Rdr}}\, b_{H_{i,3}^{Rdr}} \,||\, b_{H_{i,0}^{Rdr}+16}\, b_{H_{i,1}^{Rdr}+16}\, b_{H_{i,2}^{Rdr}+16}\, b_{H_{i,3}^{Rdr}+16} \quad [Base\ 2] \\ = \;& P_0 P_1 P_2 P_3 \quad [Base\ 16] \end{aligned}$$

Pad Generation Function - PadGen(.)



Attacks on TRMA$^+$

1. Access Password Attack (LSB)
2. Access Password Attack (MSB)
3. Kill Password Attack

Access Password Attack (LSB)

(1)	$T \rightarrow R$:	$\{EPC, RN_1^{Tag}, RN_2^{Tag}\}$
(2)	....	
(3)	$A \rightarrow R$:	$\{EPC, RN_1^{Tag'}, RN_2^{Tag'}\}$
(4)	$R \rightarrow A$:	$\{CCPwd_{M1}, CCPwd_{L1}, RN_1^{Rdr}, RN_2^{Rdr}, RN_3^{Rdr}, RN_4^{Rdr}\}$

Notation: T-Tag R-Reader A-Attacker

$$RN_i^{Tag'} = RRRR_h \quad [Base\ 16]$$
$$CCPwd_{M1} = APWD_M \oplus PAD_1$$
$$CCPwd_{L1} = APWD_L \oplus PAD_2$$

Access Password Attack (LSB)

For $i \in \{1, 2\}$,

$$PAD_i = PadGen(PadGen(RN_i^{Tag'}, RN_i^{Rdr})[APWD], RN_i^{Tag'})[KPWD] \quad (1)$$

$$\begin{aligned} PAD_i &= PadGen(V_0V_1V_2V_3, RRRR)[KPWD] \quad [Base\ 16] \\ &= k_{V_0}k_{V_1}k_{V_2}k_{V_3} \parallel k_{V_0+16}k_{V_1+16}k_{V_2+16}k_{V_3+16} \parallel k_Rk_Rk_Rk_R \parallel \\ &\quad k_{R+16}k_{R+16}k_{R+16}k_{R+16} \quad [Base\ 2] \\ &= P_0P_1P_2P_3 \quad [Base\ 16] \end{aligned}$$

P_2 and P_3 are the same, i.e. $P_2, P_3 \in \{0000_b = 0_h,\ 1111_b = \mathrm{F}_h\}$

$$P_2P_3 \in \{00_h, 0F_h, F0_h, FF_h\}$$

Access Password Attack (LSB)

$$APWD_M[8...15] = \begin{cases} CCPwd_{M1}[8...15] \oplus 0x00 & \text{with } p = 2^{-2} \\ CCPwd_{M1}[8...15] \oplus 0x0F & \text{with } p = 2^{-2} \\ CCPwd_{M1}[8...15] \oplus 0xF0 & \text{with } p = 2^{-2} \\ CCPwd_{M1}[8...15] \oplus 0xFF & \text{with } p = 2^{-2} \end{cases}$$

$$APWD_L[8...15] = \begin{cases} CCPwd_{L1}[8...15] \oplus 0x00 & \text{with } p = 2^{-2} \\ CCPwd_{L1}[8...15] \oplus 0x0F & \text{with } p = 2^{-2} \\ CCPwd_{L1}[8...15] \oplus 0xF0 & \text{with } p = 2^{-2} \\ CCPwd_{L1}[8...15] \oplus 0xFF & \text{with } p = 2^{-2} \end{cases}$$

Access Password Attack (LSB)

$$RN_1^{Tag'} = RN_2^{Tag'} = RRRR_h \quad [Base\ 16]$$

$$APWD_M[8...15] \,||\, APWD_L[8...15]$$

$$= \begin{cases} CCPwd_{M1}[8...15] \oplus 0x00 \,||\, CCPwd_{L1}[8...15] \oplus 0x00 & p = 2^{-2} \\ CCPwd_{M1}[8...15] \oplus 0x0F \,||\, CCPwd_{L1}[8...15] \oplus 0x0F & p = 2^{-2} \\ CCPwd_{M1}[8...15] \oplus 0xF0 \,||\, CCPwd_{L1}[8...15] \oplus 0xF0 & p = 2^{-2} \\ CCPwd_{M1}[8...15] \oplus 0xFF \,||\, CCPwd_{L1}[8...15] \oplus 0xFF & p = 2^{-2} \end{cases}$$

4 possible values for the LSB of $APWD_M$ and $APWD_L$!

Access Password Attack (MSB)

(1) $T \rightarrow A$:	$\{EPC, RN_1^{Tag}, RN_2^{Tag}\}$
(2a) $A \rightarrow R$:	$\{EPC, RN, RN\}$
(2b) $R \rightarrow A$:	$\{CCPwd_{M1}, CCPwd_{L1}, RN_1^{Rdr}, RN_2^{Rdr}, RN_3^{Rdr}, RN_4^{Rdr}\}$
(3a) $A \rightarrow R$:	$\{EPC, RN_1^{Tag}, RN_2^{Tag}\}$
(3b) $R \rightarrow A$:	$\{CCPwd_{M1}', CCPwd_{L1}', RN_1^{Rdr'}, RN_2^{Rdr'}, RN_3{}^{Rdr'}, RN_4{}^{Rdr'}\}$
(4) $A \rightarrow T$:	$\{CCPwd_{M1}', CCPwd_{L1}', RN_1^{Rdr'}, RN_2^{Rdr'}, RN, RN\}$
(5) $T \rightarrow A$:	$\{RN_3^{Tag}, RN_4^{Tag}, CCPwd_{M2}, CCPwd_{L2}\}$

$$RN = RRRR_h \quad [Base\ 16]$$

$$CCPwd_{M1} = APWD_M \oplus PAD_1$$

$$CCPwd_{L1} = APWD_L \oplus PAD_2$$

$$CCPwd_{M2} = APWD_M \oplus PAD_3$$

$$CCPwd_{L2} = APWD_L \oplus PAD_4$$

$APWD_M[0:1-4:5]$

$APWD_L[0:1-4:5]$

$APWD_M[2:3-6:7]$

$APWD_L[2:3-6:7]$

Access Password Attack (MSB)

For $i \in \{1, 2\}$,

$$
\begin{aligned}
& PadGen(RN, RN_i^{Rdr})[APWD] \\
= \;& PadGen(RRRR, H_{i,0}^{Rdr} H_{i,1}^{Rdr} H_{i,2}^{Rdr} H_{i,3}^{Rdr})[APWD] \quad [Base\ 16] \\
= \;& a_R a_R a_R a_R \;||\; a_{R+16} a_{R+16} a_{R+16} a_{R+16} \;||\; a_{H_{i,0}^{Rdr}} a_{H_{i,1}^{Rdr}} a_{H_{i,2}^{Rdr}} a_{H_{i,3}^{Rdr}} \;||\; \\
& a_{H_{i,0}^{Rdr}+16} a_{H_{i,1}^{Rdr}+16} a_{H_{i,2}^{Rdr}+16} a_{H_{i,3}^{Rdr}+16} \quad [Base\ 2] \\
= \;& V_0 V_1 V_2 V_3 \quad [Base\ 16] \qquad (1)
\end{aligned}
$$

$$V_0, V_1 \in \{0_h, F_h\} or\, V_0 V_1 \in \{00_h, 0F_h, F0_h, FF_h\}$$

$$
\begin{aligned}
& PAD_{i \in \{1,2\}} \\
= \;& PadGen(PadGen(RN, RN_1^{Rdr})[APWD], RN)[KPWD] \\
= \;& PadGen(V_0 V_1 V_2 V_3, RRRR)[KPWD] \quad [Base\ 16] \\
= \;& k_{V_0} k_{V_1} k_{V_2} k_{V_3} \;||\; k_{V_0+16} k_{V_1+16} k_{V_2+16} k_{V_3+16} \;||\; k_R k_R k_R k_R \;||\; \\
& k_{R+16} k_{R+16} k_{R+16} k_{R+16} \quad [Base\ 2]
\end{aligned}
$$

$$
\begin{aligned}
Prob(k_{V_0} = k_{V_1}) &= (0.5)(1) + (0.5)(0.5) = 0.75 \\
Prob(k_{V_0+16} &= k_{V_1+16}) = 0.75
\end{aligned}
$$

Access Password Attack (MSB)

For $i \in \{3,4\}$,

$$
\begin{aligned}
& PadGen(RN_i^{Tag}, RN)[APWD] \\
= \;& PadGen(H_{i,0}^{Tag} H_{i,1}^{Tag} H_{i,2}^{Tag} H_{i,3}^{Tag}, RRRR)[APWD] \quad [Base\ 16] \\
= \;& a_{H_{i,0}^{Tag}} a_{H_{i,1}^{Tag}} a_{H_{i,2}^{Tag}} a_{H_{i,3}^{Tag}} \;||\; a_{H_{i,0}^{Tag}+16} a_{H_{i,1}^{Tag}+16} a_{H_{i,2}^{Tag}+16} a_{H_{i,3}^{Tag}+16} \;||\; \\
& a_R a_R a_R a_R \;||\; a_{R+16} a_{R+16} a_{R+16} a_{R+16} [Base\ 2] \\
= \;& S_0 S_1 S_2 S_3 \quad [Base\ 16] \qquad (1) \\
& \qquad (2) \\
& S_2, S_3 \in \{0_h, F_h\} or S_2 S_3 \in \{00_h, 0F_h, F0_h, FF_h\} \qquad (3)
\end{aligned}
$$

$$
\begin{aligned}
& PAD_{i \in \{3,4\}} \\
= \;& PadGen(PadGen(RN_i^{Tag}, RN)[APWD], RN_i^{Tag})[KPWD] \\
= \;& PadGen(S_0 S_1 S_2 S_3, H_{i,0}^{Tag} H_{i,1}^{Tag} H_{i,2}^{Tag} H_{i,3}^{Tag})[KPWD] \quad [Base\ 16] \\
= \;& k_{S_0} k_{S_1} k_{S_2} k_{S_3} \;||\; k_{S_0+16} k_{S_1+16} k_{S_2+16} k_{S_3+16} \;||\; k_{H_{i,0}^{Tag}} k_{H_{i,1}^{Tag}} k_{H_{i,2}^{Tag}} k_{H_{i,3}^{Tag}} \;||\; \\
& k_{H_{i,0}^{Tag}+16} k_{H_{i,1}^{Tag}+16} k_{H_{i,2}^{Tag}+16} k_{H_{i,3}^{Tag}+16} \quad [Base\ 2] \qquad (4)
\end{aligned}
$$

$$Prob(k_{S_2} = k_{S_3}) = 0.75$$

$$Prob(k_{S_2+16} = k_{S_3+16}) = 0.75$$

Access Password Attack (MSB)

Since $V_0 = S_2$ and $V_1 = S_3$, we then have

$$\begin{aligned} k_{V_0} = k_{S_2} &= k_{V_1} = k_{S_3} \quad p = 0.75 \\ k_{V_0} = k_{S_2} &\neq k_{V_1} = k_{S_3} \quad p = 0.25 \\ k_{V_0+16} = k_{S_2+16} &= k_{V_1+16} = k_{S_3+16} \quad p = 0.75 \\ k_{V_0+16} = k_{S_2+16} &\neq k_{V_1+16} = k_{S_3+16} \quad p = 0.25 \end{aligned}$$

Combining both sets of information:

Case 1: $P(k_{V_0} = k_{S_2} = k_{V_1} = k_{S_3}$ and $k_{V_0+16} = k_{S_2+16} = k_{V_1+16} = k_{S_3+16}) = 0.625$

Case 2: $P(k_{V_0} = k_{S_2} = k_{V_1} = k_{S_3}$ and $k_{V_0+16} = k_{S_2+16} \neq k_{V_1+16} = k_{S_3+16}) = 0.125$

Case 3: $P(k_{V_0} = k_{S_2} \neq k_{V_1} = k_{S_3}$ and $k_{V_0+16} = k_{S_2+16} = k_{V_1+16} = k_{S_3+16}) = 0.125$

Case 4: $P(k_{V_0} = k_{S_2} \neq k_{V_1} = k_{S_3}$ and $k_{V_0+16} = k_{S_2+16} \neq k_{V_1+16} = k_{S_3+16}) = 0.125$

Access Password Attack (MSB)

$$APWD_M[0...7] \,||\, APWD_L[0...7] \;=\; A \oplus mask \,||\, B \oplus mask$$

$$A = (CCPwd_{M1}[0..7] \wedge 0\text{xCC}) \vee (CCPwd_{M2}[0..7] \wedge 0\text{x33})$$
$$B = (CCPwd_{L1}[0..7] \wedge 0\text{xCC}) \vee (CCPwd_{L2}[0..7] \wedge 0\text{x33})$$

Case 1 $mask \in \{0\text{x00}, 0\text{x0F}, 0\text{xF0}, 0\text{xFF}\}$ and the probability of a successful attack would be $0.625 \times 1/4 = 0.15625$

Case 2 $mask \in \{0\text{x05}, 0\text{x0A}, 0\text{xF5}, 0\text{xFA}\}$ and the probability of a successful attack would be $0.125 \times 1/4 = 0.03125$.

Case 3 $mask \in \{0\text{x50}, 0\text{x5F}, 0\text{xA0}, 0\text{xAF}\}$ and the probability of a successful attack would be $0.125 \times 1/4 = 0.03125$.

Case 4 $mask \in \{0\text{x55}, 0\text{x5A}, 0\text{xA5}, 0\text{xAA}\}$ and the probability of a successful attack would be $0.125 \times 1/4 = 0.03125$.

Access Password Attack (MSB)

16 possible values for the MSB of $APWD_M$ and $APWD_L$!

$$Prob(\text{successful recovery of all bits in } APWD_M[0...7] \,||\, APWD_L[0...7])$$

$$= \begin{cases} \frac{5}{2^5} = 0.15625 & \text{if} \quad mask \in \{0x00, 0x0F, 0xF0, 0xFF\} \\ \frac{1}{2^5} = 0.03125 & \text{if} \quad mask \in \{0x05, 0x0A, 0x50, 0x55, 0x5A, 0x5F \\ & \quad 0xA0, 0xA5, 0xAA, 0xAF\ 0xF5, 0xFA\} \end{cases}$$

Kill Password Attack (MSB)

Assumption: 8 least significant bits of $APWD_M$ and $APWD_L$

(1) $T \rightarrow R$:	$\{EPC, RN_1^{Tag}, RN_2^{Tag}\}$
(2) $R \rightarrow T$:	$\{CCPwd_{M1}, CCPwd_{L1}, RN_1^{Rdr}, RN_2^{Rdr}, RN_3^{Rdr}, RN_4^{Rdr}\}$
(5) $Tag \rightarrow Reader$:	$\{RN_3^{Tag}, RN_4^{Tag}, CCPwd_{M2}, CCPwd_{L2}\}$

$$
\begin{aligned}
PAD_1[8...15] &= CCPwd_{M1}[8...15] \oplus APWD_M[8...15] \\
PAD_2[8...15] &= CCPwd_{L1}[8...15] \oplus APWD_L[8...15] \\
PAD_3[8...15] &= CCPwd_{M2}[8...15] \oplus APWD_M[8...15] \\
PAD_4[8...15] &= CCPwd_{L2}[8...15] \oplus APWD_L[8...15]
\end{aligned}
$$

Kill Password Attack (MSB)

$$\begin{aligned} PAD_i &= PadGen(----, RN_i^{Tag})[KPWD] \\ &= PadGen(----, H_{i,0}^{Tag} H_{i,1}^{Tag} H_{i,2}^{Tag} H_{i,3}^{Tag})[KPWD] \quad [Base\ 16] \end{aligned}$$

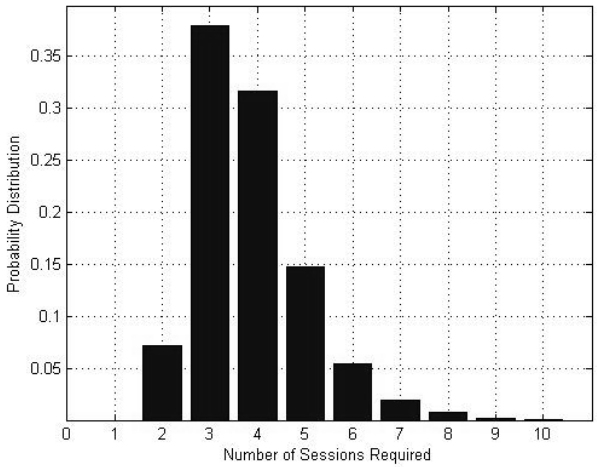
$$\begin{aligned} PAD_i[8...15] &= k_{H_{i,0}^{Tag}} k_{H_{i,1}^{Tag}} k_{H_{i,2}^{Tag}} k_{H_{i,3}^{Tag}} \ || \\ & \quad k_{H_{i,0}^{Tag}+16} k_{H_{i,1}^{Tag}+16} k_{H_{i,2}^{Tag}+16} k_{H_{i,3}^{Tag}+16} \quad [Base\ 2] \end{aligned}$$

For PAD_i $(i \in \{1,2,3,4\})$:

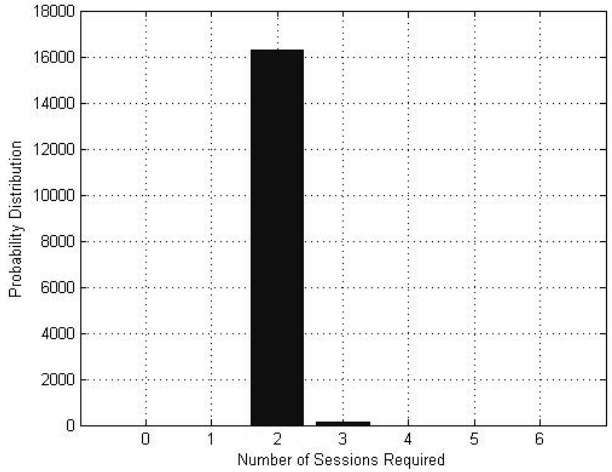
$$\begin{aligned} k_{H_{i,0}^{Tag}} &= PAD_i[8] \\ k_{H_{i,1}^{Tag}} &= PAD_i[9] \\ k_{H_{i,2}^{Tag}} &= PAD_i[10] \\ k_{H_{i,3}^{Tag}} &= PAD_i[11] \end{aligned}$$

$$\begin{aligned} k_{H_{i,0}^{Tag}+16} &= PAD_i[12] \\ k_{H_{i,1}^{Tag}+16} &= PAD_i[13] \\ k_{H_{i,2}^{Tag}+16} &= PAD_i[14] \\ k_{H_{i,3}^{Tag}+16} &= PAD_i[15] \end{aligned}$$

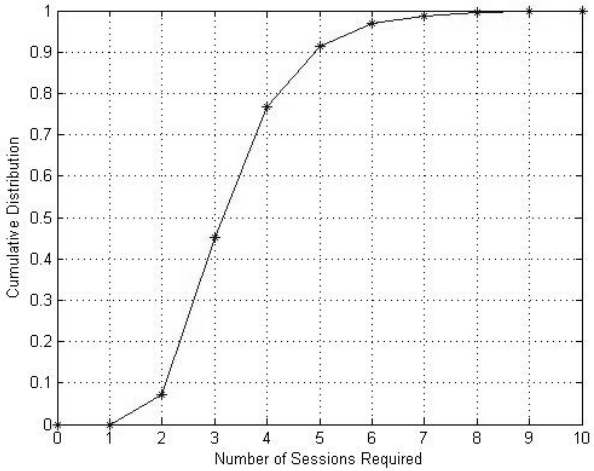
Kill Password Attack (MSB)



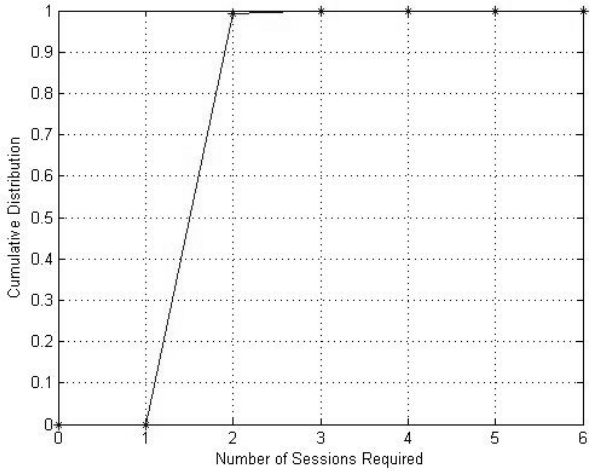
(a) Passive Attacker



(b) Active Attacker



(c) Passive Attacker



(d) Active Attacker

Conclusions

- EPC-C1G2 standard: important security problems
- Konidola et.'s scheme:
  Kill and access password can be adquiered with high probability!
  - Access Password: p(MSB) $< 2^{-5}$ and p(LSB) $= 2^{-2}$
  - Kill Password: 2^{-2}
- The design of new proposals under the EPC-C1G2 is imperative

Questions?

Thank you

pperis@inf.uc3m.es

http://www.lightweightcryptography.com/

UNIVERSIDAD CARLOS III DE MADRID

Ph.D. THESIS

Lightweight Cryptography in Radio Frequency Identification (RFID) Systems

Author:
Pedro Peris López

Supervisors:
Dr. D. Julio C. Hernández Castro
Dr. D. Arturo Ribagorda Garnacho

Computer Science Department

Leganés, October 2008

Ph.D. THESIS

Lightweight Cryptography in Radio Frequency Identification (RFID) Systems

Author: Pedro Peris-Lopez

`http://www.lightweightcryptography.com/peristhesis.pdf`


T.L. Lim, and T. Li, "Addressing the Weakness in a Lightweight RFID Tag-Reader Mutual Authentication Scheme", in *Proceedings of the IEEE Int'l Global Telecommunications Conference (GLOBECOM) 2007*, pp. 59-63, Nov 2007.


D.M. Konidala, Z. Kim, and K. Kim, "A Simple and Cost-effective RFID Tag-Reader Mutual Authentication Scheme", in *Proceedings of Int'l Conference on RFID Security 2007 (RFIDSec 07)*, pp. 141-152, Jul. 11-13, 2007, Malaga, Spain.