On the Security of two RFID Mutual Authentication Protocols

Seyed Farhad Aghili, Nasour Bagheri, Praveen Gauravaram*, Masoumeh Safkhani, Somitra Kumar Sanadhya

* TCS Innovation Labs, Hyderabad, India

The 9th Workshop on RFID Security, July 9-11, 2013, Graz, Austria

OUTLINE

1. RFID Systems Overview
2. HYCLT Protocol
3. Security Analysis of HYCLT
4. HLL Protocol
5. Security Analysis of HLL
6. Conclusion

OUTLINE

1. RFID Systems Overview
2. HYCLT Protocol
3. Security Analysis of HYCLT
4. HLL Protocol
5. Security Analysis of HLL
6. Conclusion

EPC C1 G2 RFID Standard

RFIDsec 2013

- EPCglobal Class-1 Gen-2 (EPC C1 G2) is one of the most important standards proposed by EPCglobal .
- This standard was adopted in 2004.
- 18months later (March–April 2006) ratified by ISO.
- It was published as an amendment to 18000-6 standard.

The most important properties of EPC-C1G2 :

- Tags are passive.
- Tags operate on the UHF band (860–960 MHz).
- EPC-C1 G2 tags cannot afford traditional cryptographic primitives.
- Tags include on chip a 16-bit Pseudo-Random Number Generator (PRNG) and a 16-bit Cyclic Redundancy Code (CRC) checksum.

EPC C1 G2 RFID Standard

- Tags have two 32-bit passwords:

- Kill Password: is a 32-bit value stored in reserved memory (00h to 1Fh).

A reader shall use a tag's kill password once, to kill the tag and render it silent there after.

- Access Password : is a 32-bit value stored in reserved memory (20h to 3Fh).

Tags with a nonzero access password shall require a reader to issue this password before transitioning to the secured state, which will allow it to read or write in the password fields.

EPC C1 G2 Security

- Bailey and A. Juels and Peris-Lopez et al. pointed out the weakness in the EPC C1G2 reader-to-tag authentication protocol.
- Konidala et al.'s proposed an alternative scheme which is known to be flawed. In Konidala et al.'s scheme, the *PadGen* function is the key component in constructing the 16-bit pads to mask the password which is transferred over an insecure channel. However, this masking leaks information related to the tag's secrets.

- To solve Konidala et al. protocol's weaknesses two novel protocols have been proposed by Huang *et al.* and Huang, Lin and Li respectively.

- We consider security of these protocols which are denoted by *HYCLT* designed by Huang *et al.* and *HLL* designed by Huang, Lin and Li respectively.

OUTLINE

RFIDsec 2013

1. RFID Systems Overview
2. HYCLT Protocol
3. Security Analysis of HYCLT
4. HLL Protocol
5. Security Analysis of HLL
6. Conclusion

HYCLT Protocol

R_i :	*RFID* reader *i*
T_i :	*RFID* tag *i*
Req_R :	Reader request
R_{Tx} :	Random numbers generated by the tag.
R_{Mx} :	Random numbers generated by the server.
EPC :	Electronic product code.
Apwd :	*Access password*
Kpwd :	*Kill password*
PAD_x :	*Masking values.*
$CCPwd_{M_1}$:	$Apwd_M \oplus PAD_1$
$CCPwd_{L_1}$:	$Apwd_M \oplus PAD_2$
$X\|_i$:	i^{th} bit of string X
$\oplus$:	Exclusive or operation
$\|\|$:	Concatenation operation
X_{m-n} :	A fraction of X from the m^{th} bit to the n^{th} bit.

HYCLT Protocol

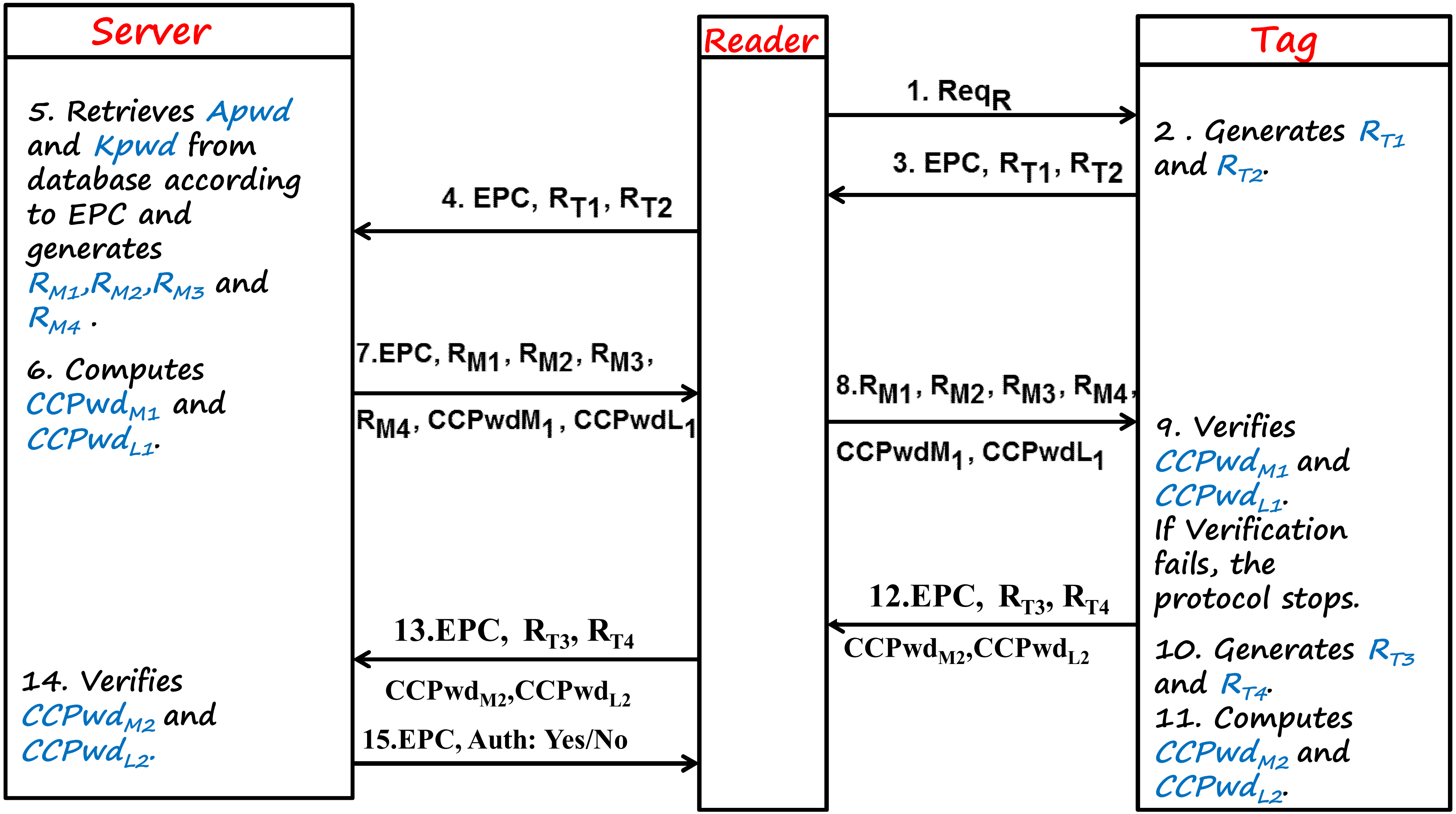
- Huang et al. have proposed (HYCLT) based on a new PadGen and also demonstrated the FPGA hardware implementation of it.

- Any tag in HYCLT protocol have two 32-bit passwords called *Kill* and *Access* password.

- We show that an adversary can determine the complete *Access* password of HYCLT.

HYCLT Protocol

RFIDsec 2013



PadGen Function of HYCLT

The simple PadGen function proposed in HYCLT accepts a 32-bit value and two 16-bit values as input and outputs 16 bits.

$X \in \{0,1\}^{32}, Y \in \{0,1\}^{16}, Z \in \{0,1\}^{16}$

$X = X_0 X_1 X_2 X_3 \ldots X_{31} \qquad X_i \in \{0,1\}$

$Y = d_{Y1} d_{Y2} d_{Y3} d_{Y4}$

$Z = d_{Z1} d_{Z2} d_{Z3} d_{Z4} \qquad d_{Zi} \in \{0, 1, \ldots, 15\} \quad i \in \{1, 2, 3, 4\}$ [base 10]

Example,

$Z = 1101\ 0110\ 1000\ 1001$ can be represented as $Z = 13\ 06\ 08\ 09$

which means that

$d_{Z1} = 13;\ d_{Z2} = 06;\ d_{Z3} = 08;\ d_{Z4} = 09$

$Y = h_{Y1} h_{Y2} h_{Y3} h_{Y4}$

$Z = h_{Z1} h_{Z2} h_{Z3} h_{Z4}, \qquad h_{Zi} \in \{0, 1, \ldots, F\} \quad i \in \{1, 2, 3, 4\}$ [base 16]

Example,

$Z = 1101\ 0110\ 1000\ 1001$ can be represented as $Z = C\ 6\ 8\ 9$

which means that

$h_{Z1} = C;\ h_{Z2} = 6;\ h_{Z3} = 8;\ h_{Z4} = 9.$

PadGen Function of HYCLT

$$PadGen(x, y, z)$$
$$= x_{d_{y1}} x_{d_{y1}+16} x_{d_{y2}} x_{d_{y2}+16} \| x_{d_{z1}} x_{d_{z1}+16} x_{d_{z2}} x_{d_{z2}+16} \|$$
$$x_{d_{y3}} x_{d_{y3}+16} x_{d_{y4}} x_{d_{y4}+16} \| x_{d_{z3}} x_{d_{z3}+16} x_{d_{z4}} x_{d_{z4}+16}$$

$$X = 1001\ 1111\ 0011\ 1011\ 0000\ 0011\ 1100\ 0101$$

The location of the extracted bits

$$Y = 0111\ 0100\ 0110\ 1011$$
$$Z = 1101\ 0110\ 1000\ 1001$$

$$PadGen(x, y, z)$$
$$= x_7\ x_{7+16} x_4\ x_{4+16} \| x_{13}\ x_{13+16} x_6\ x_{6+16} \|$$
$$x_6\ x_{6+16} x_{11}\ x_{11+16} \| x_8\ x_{8+16} x_9\ x_{9+16}$$

$$= 1110\ 0011\ 1110\ 0101$$

PadGen Function of HYCLT

$$Apwd = a_0\, a_1\, a_2\, a_3\, \ldots a_{31} \qquad a_i \in \{0, 1\}$$

$$Apwd_L = a_0\, a_1\, a_2\, a_3\, \ldots a_{15}$$

$$Apwd_M = a_{16}\, a_{17}\, a_{18}\, a_{19}\, \ldots a_{31}$$

$$Kpwd = k_0\, k_1\, k_2\, k_3\, \ldots k_{31} \qquad k_i \in \{0, 1\}$$

$$R_{Tx} = d_{t1} d_{t2} d_{t3} d_{t4}$$

$$R_{Mx} = d_{m1} d_{m2} d_{m3} d_{m4} \qquad x \in \{1, 2, 3, 4\} \quad \text{[base 10]}$$

$$R_{Tx} = h_{t1} h_{t2} h_{t3} h_{t4}$$

$$R_{Mx} = h_{m1} h_{m2} h_{m3} h_{m4} \qquad h_{mj} \in \{0, \ldots, F\} \quad j \in \{1, 2, 3, 4\} \quad \text{[base 16]}$$

PadGen Function of HYCLT

PadGen function is used to compute masking values PAD_x**, where** $x \in \{1, 2, 3, 4\}$

$$
\begin{aligned}
R_{Vx} &= PadGen(Apwd, R_{TX}, R_{MX}) \\
&= a_{d_{t1}} a_{d_{t1}+16} a_{d_{t2}} a_{d_{t2}+16} \| a_{d_{m1}} a_{d_{m1}+16} a_{d_{m2}} a_{d_{m2}+16} \| \\
&\quad a_{d_{t3}} a_{d_{t3}+16} a_{d_{t4}} a_{d_{t4}+16} \| a_{d_{m3}} a_{d_{m3}+16} a_{d_{m4}} a_{d_{m4}+16} \\
&= d_{v1} d_{v2} d_{v3} d_{v4}
\end{aligned}
$$

$$
\begin{aligned}
PAD_X &= PadGen(Kpwd, R_{Vx}, R_{Tx}) \\
&= k_{d_{v1}} k_{d_{v1}+16} k_{d_{v2}} k_{d_{v2}+16} \| k_{d_{t1}} k_{d_{t1}+16} k_{d_{t2}} k_{d_{t2}+16} \| \\
&\quad k_{d_{v3}} k_{d_{v3}+16} k_{d_{v4}} k_{d_{v4}+16} \| k_{d_{t3}} k_{d_{t3}+16} k_{d_{t4}} k_{d_{t4}+16} \\
&= h_{p1} h_{p2} h_{p3} h_{p4}
\end{aligned}
$$

PadGen Function of HYCLT

To increase the security level of HYCLT, authors also proposed a more complex way to use R_{Tx} and R_{Mx} as follows:

$$R_{Vx} = PadGen(Apwd, R_{Tx}, R_{Mx}) = a_{w1}a_{w2}a_{w3}a_{w4} \| a_{w5}a_{w6}a_{w7}a_{w8} \| a_{w9}a_{w10}a_{w11}a_{w12} \| a_{w13}a_{w14}a_{w15}a_{w16} = d_{v1}\, d_{v2}\, d_{v3}\, d_{v4}$$

$$PAD_X = PadGen(Kpwd, R_{Vx}, R_{Tx}) = k_{z1}k_{z2}k_{z3}k_{z4} \| k_{z5}k_{z6}k_{z7}k_{z8} \| k_{z9}k_{z10}k_{z11}k_{z12} \| k_{z13}k_{z14}k_{z15}k_{z16} = h_{p1}\, h_{p2}\, h_{p3}\, h_{p4}$$

$CCPwd_{M_1} = Apwd_M \oplus PAD_1$ **and** $CCPwd_{L_1} = Apwd_L \oplus PAD_2$

PadGen Function of HYCLT

$$w_{1-4} = d_{t1} + d_{m1},\ d_{t1} + d_{m2},\ d_{t1} + d_{m3},\ d_{t1} + d_{m4}$$
$$w_{5-8} = d_{t2} + d_{m1},\ d_{t2} + d_{m2},\ d_{t2} + d_{m3},\ d_{t2} + d_{m4}$$
$$w_{9-12} = d_{t3} + d_{m1},\ d_{t3} + d_{m2},\ d_{t3} + d_{m3},\ d_{t3} + d_{m4}$$
$$w_{13-16} = d_{t4} + d_{m1},\ d_{t4} + d_{m2},\ d_{t4} + d_{m3},\ d_{t4} + d_{m4}$$

$$z_{1-4} = d_{t1} + d_{v1},\ d_{t1} + d_{v2},\ d_{t1} + d_{v3},\ d_{t1} + d_{v4}$$
$$z_{5-8} = d_{t2} + d_{v1},\ d_{t2} + d_{v2},\ d_{t2} + d_{v3},\ d_{t2} + d_{v4}$$
$$z_{9-12} = d_{t3} + d_{v1},\ d_{t3} + d_{v2},\ d_{t3} + d_{v3},\ d_{t3} + d_{v4}$$
$$z_{13-16} = d_{t4} + d_{v1},\ d_{t4} + d_{v2},\ d_{t4} + d_{v3},\ d_{t4} + d_{v4}$$

OUTLINE

1. RFID Systems Overview
2. HYCLT Protocol
3. **Security Analysis of HYCLT**
4. HLL Protocol
5. Security Analysis of HLL
6. Conclusion

Security Analysis of Complex HYCLT

Passive Adversary:

Assume that an adversary impersonates the target tag and sends $R_{Tx} = d_{t1}d_{t2}d_{t3}d_{t4}$ to the reader such that $d_{t1}=d_{t2}=d_{t3}=d_{t4}$ e.g. $R_{Tx}=0$

$$w_{1-4} = w_{5-8} = w_{9-12} = w_{13-16}$$
$$d_{v1} = d_{v2} = d_{v3} = d_{v4}$$

$$Z_1 = Z_2 = \ldots = Z_{16} = Z$$

$$PAD_X = PadGen(Kpwd, d_{v1}d_{v2}d_{v3}d_{v4}, R_{Tx}) = k_Z \| k_Z \| k_Z \| k_Z$$
$$Z \in \{0,1,\ldots,F\}$$

$$PAD_X = PadGen(Kpwd, d_{v1}d_{v2}d_{v3}d_{v4}, R_{Tx}) \in \{0000, FFFF\}$$

$CCPwd_{M_1} = Apwd_M \oplus PAD_1$ **and** $CCPwd_{L_1} = Apwd_L \oplus PAD_2$

The adversary can determine $Apwd_M \| Apwd_L$ **with the probability of** 2^{-2}

Security Analysis of Complex HYCLT

Active Adversary

Assume that an active adversary intercepts the message from the tag to the reader in step 2 and replaces R_{T1} by $R_{T1} = d_{t1} \| d_{t2} \| d_{t3} \| d_{t4}$

where $d_{t1} = d_{t2} = d_{t3} = d_{t4} = X$

$$\Rightarrow R_{T1} = i \| i \| i \| i \,, \quad 0 \le i \le 15$$

$$R_{V1} = PadGen(Apwd, R_{T1}, R_{M1})$$
$$= a_x \; a_{x+16} a_x \; a_{x+16} \| a_{d_{m1}} \; a_{d_{m1}+16} a_{d_{m2}} \; a_{d_{m2}+16} \|$$
$$a_x \; a_{x+16} a_x \; a_{x+16} \| a_{d_{m3}} \; a_{d_{m3}+16} a_{d_{m4}} \; a_{d_{m4}+16}$$
$$= d_{v1} d_{v2} d_{v1} d_{v4}$$

$d_{v1} = d_{v3}$

$$PAD_1 = PadGen(Kpwd, R_{V1}, R_{T1})$$
$$= k_{d_{v1}} \; k_{d_{v1}+16} k_{d_{v2}} \; k_{d_{v2}+16} \| k_{d_{t1}} \; k_{d_{t1}+16} k_{d_{t2}} \; k_{d_{t2}+16} \|$$
$$k_{d_{v1}} \; k_{d_{v1}+16} k_{d_{v4}} \; k_{d_{v4}+16} \| k_{d_{t3}} \; k_{d_{t3}+16} k_{d_{t4}} \; k_{d_{t4}+16}$$
$$= h_{p1} h_{p2} h_{p3} h_{p4}$$

Security Analysis of Complex HYCLT

Given that $CCPwd_{M1} = Apwd_M \oplus PAD_1$ and $APwd_M = a_{16}a_{17}...a_{31}$, we can extract:

$$(CCPwd_{M1})|_0 \oplus (CCPwd_{M1})|_8 = a_{16} \oplus a_{24}$$
$$(CCPwd_{M1})|_1 \oplus (CCPwd_{M1})|_9 = a_{17} \oplus a_{25}$$

which used to recognize a target tag with the success probability of $1-2^{-4}$.

For the simple version of PadGen in HYCLT protocol, we can recover both Apwd and Kpwd.

OUTLINE

1. RFID Systems Overview
2. HYCLT Protocol
3. Security Analysis of HYCLT
4. HLL Protocol
5. Security Analysis of HLL
6. Conclusion

HLL Protocol

- Huang, Lin and Li presented another protocol with a different *PadGen* function based on a set of values i.e. (R_V, R_W), which is not under the direct control of the adversary.

- Any tag in HLL have two 32-bit passwords called *Kill* and *Access* passwords.

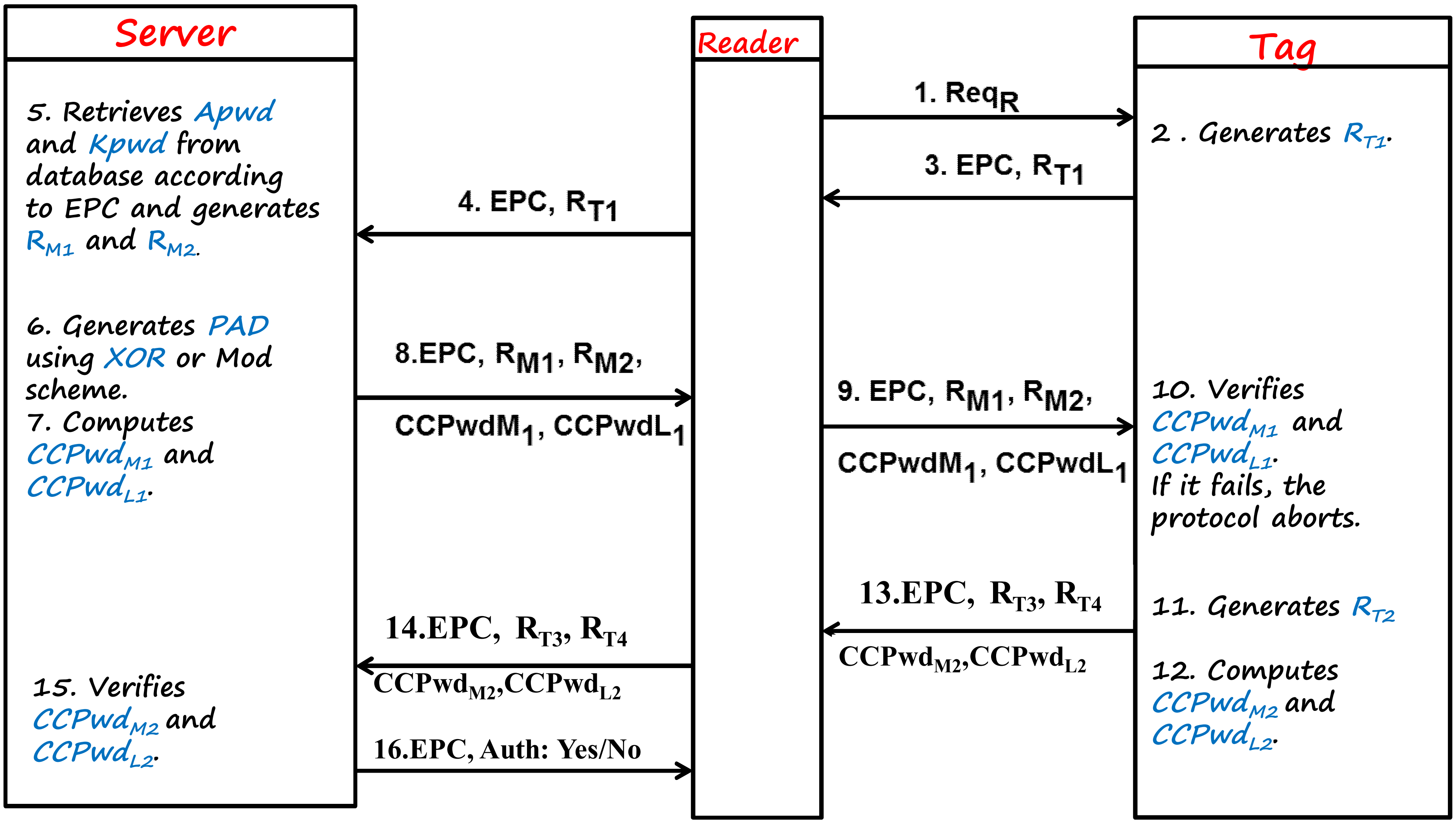
- The main difference between HYCLT and HLL is their *PadGen* function calculations.

- HLL against HYCLT is based on *XOR* or *MOD* operation to generate *PadGen* function.

- We show several attacks on *XOR* based.

- Our attack does not work for the *MOD* mode.

HLL Protocol



PadGen Function of HLL

$R_{T_i} \quad i \in \{1,2\}$ → R_T $\qquad$ $R_{M_i} \quad i \in \{1,2\}$ → R_M

in HLL defined that $R_T \oplus R_M = R_{T\oplus M} = d_{x1} d_{x2} d_{x3} d_{x4}$

$$R_W = PadGen(Apwd, R_T, R_{T\oplus M})$$

$$= a_{d_{t1}} a_{d_{t2}} a_{d_{t3}} a_{d_{t4}} \| a_{d_{t1}+16} a_{d_{t2}+16} a_{d_{t3}+16} a_{d_{t4}+16} \|$$

$$a_{d_{x1}} a_{d_{x2}} a_{d_{x3}} a_{d_{x4}} \| a_{d_{x1}+16} a_{d_{x2}+16} a_{d_{x3}+16} a_{d_{x4}+16}$$

$$= d_{w1} d_{w2} d_{w3} d_{w4}$$

$$R_V = PadGen(Apwd, R_{T_x}, R_{M_x})$$

$$= a_{d_{t1}} a_{d_{t2}} a_{d_{t3}} a_{d_{t4}} \| a_{d_{t1}+16} a_{d_{t2}+16} a_{d_{t3}+16} a_{d_{t4}+16} \|$$

$$a_{d_{m1}} a_{d_{m2}} a_{d_{m3}} a_{d_{m4}} \| a_{d_{m1}+16} a_{d_{m2}+16} a_{d_{m3}+16} a_{d_{m4}+16}$$

$$= d_{v1} d_{v2} d_{v3} d_{v4} \qquad \text{[base10]}$$

PadGen Function of HLL

$$PAD_1 = PadGen(Kpwd, R_V, R_W)$$
$$= k_{d_{v1}} k_{d_{v2}} k_{d_{v3}} k_{d_{v4}} \| k_{d_{v1}+16} k_{d_{v2}+16} k_{d_{v3}+16} k_{d_{v4}+16} \|$$
$$k_{d_{w1}} k_{d_{w2}} k_{d_{w3}} k_{d_{w4}} \| k_{d_{w1}+16} k_{d_{w2}+16} k_{d_{w3}+16} k_{d_{w4}+16}$$
$$= h_{q1} h_{q2} h_{q3} h_{q4}$$

in HLL defined that $R_V \oplus R_W = R_{V \oplus W} = d_{s1} d_{s2} d_{s3} d_{s4}$

$$PAD_2 = PadGen(Kpwd, R_V, R_{V \oplus W})$$
$$= k_{d_{v1}} k_{d_{v2}} k_{d_{v3}} k_{d_{v4}} \| k_{d_{v1}+16} k_{d_{v2}+16} k_{d_{v3}+16} k_{d_{v4}+16} \|$$
$$k_{d_{s1}} k_{d_{s2}} k_{d_{s3}} k_{d_{s4}} \| k_{d_{s1}+16} k_{d_{s2}+16} k_{d_{s3}+16} k_{d_{s4}+16}$$
$$= h_{r1} h_{r2} h_{r3} h_{r4}$$

OUTLINE

RFIDsec 2013

1. RFID Systems Overview
2. HYCLT Protocol
3. Security Analysis on HYCLT
4. HLL Protocol
5. **Security Analysis of HLL**
6. Conclusion

Security Analysis of HLL

Observation 1: It can be seen that :

$$d_{v1} = d_{w1} = a_{d_{t1}}\ a_{d_{t2}} a_{d_{t3}}\ a_{d_{t4}}$$

$$d_{v2} = d_{w2} = a_{d_{t1}+16}\ a_{d_{t2}+16} a_{d_{t3}+16}\ a_{d_{t4}+16}$$

Observation 2: Following Observation 1

$$k_{d_{v1}} = k_{d_{w1}}, k_{d_{v2}} = k_{d_{w2}}$$

$$k_{d_{v1}+16} = k_{d_{w1}+16}$$

$$k_{d_{v2}+16} = k_{d_{w2}+16}$$

Security Analysis of HLL

Following Observation 2:

$$PAD_1 = k_{d_{v1}} k_{d_{v2}} k_{d_{v3}} k_{d_{v4}} \| k_{d_{v1}+16} k_{d_{v2}+16} k_{d_{v3}+16} k_{d_{v4}+16} \|$$
$$k_{d_{v1}} k_{d_{v2}} k_{d_{w3}} k_{d_{w4}} \| k_{d_{v1}+16} k_{d_{v2}+16} k_{d_{w3}+16} k_{d_{w4}+16}$$
$$= h_{q1} h_{q2} h_{q3} h_{q4}$$

Given that $CCPwd_{M1} = Apwd_M \oplus PAD_1$ and $APwd_M = a_{16} a_{17} \ldots a_{31}$, we extract:

$$(CCPwd_{M1})|_0 \oplus (CCPwd_{M1})|_8 = a_{16} \oplus a_{24}$$
$$(CCPwd_{M1})|_1 \oplus (CCPwd_{M1})|_9 = a_{17} \oplus a_{25}$$
$$(CCPwd_{M1})|_4 \oplus (CCPwd_{M1})|_{12} = a_{20} \oplus a_{28}$$
$$(CCPwd_{M1})|_5 \oplus (CCPwd_{M1})|_{13} = a_{21} \oplus a_{29}$$

which is used to recognize a target tag with the success probability of $1-2^{-4}$.

Security Analysis of HLL

RFIDsec 2013

Observation 3: Following Observation 1

One can state that $d_{s1} = d_{s2} = 0$ **and** $R_{V \oplus W} = 00 d_{s3} d_{s4}$

Hence, we can rewrite PAD_2 as :

$$PAD_2 = Kpwd - PadGen(R_V, R_{V \oplus W})$$
$$= k_{d_{v1}} k_{d_{v2}} k_{d_{v3}} k_{d_{v4}} \| k_{d_{v1}+16} k_{d_{v2}+16} k_{d_{v3}+16} k_{d_{v4}+16} \|$$
$$k_0 k_0 k_{d_{s3}} k_{d_{s4}} \| k_{16} k_{16} k_{d_{s3}+16} k_{d_{s4}+16} = h_{r1} h_{r2} h_{r3} h_{r4}$$

$$CCPwd_{L1} = XXXX \| XXXX \| (k_0 \oplus a_8)(k_0 \oplus a_9) XX \|$$
$$(k_{16} \oplus a_{12})(k_{16} \oplus a_{13}) XX$$

Which is used to recognize a target tag with the success probability of $1-2^{-4}$.

Security Analysis of HLL

Comparing PAD_1 and PAD_2 , we can see:

$$h_{q1}h_{q2} = h_{r1}h_{r2}$$
$$PAD_1 = h_{q1}h_{q2}h_{q3}h_{q4}$$
$$PAD_2 = h_{r1}h_{r2}h_{r3}h_{r4}$$
$$CCPwd_{M1} = Apwd_M \oplus PAD_1$$
$$CCPwd_{L1} = Apwd_L \oplus PAD_2$$
$$PAD_1 \oplus PAD_2 = 0000 \| 0000 \| XXXX \| XXXX, \quad \text{(Observation 4)}$$
$$Apwd_L = a_0a_1 \ldots a_{15} \quad , \quad Apwd_M = a_{16}a_{17} \ldots a_{31}$$
$$CCPwd_{L1} \oplus CCPwd_{M1} = (a_0 \oplus a_{16})(a_1 \oplus a_{17})(a_2 \oplus a_{18})(a_3 \oplus a_{19}) \|$$
$$(a_4 \oplus a_{20})(a_5 \oplus a_{21})(a_6 \oplus a_{22})(a_7 \oplus a_{23}) \| XXXX \| XXXX$$

- 8- LSB of $CCPwd_{M1} \oplus CCPwd_{L1}$ is independent of the random values, R_T and R_M
- These 8 bits of $CCPwd_{M1} \oplus CCPwd_{L1}$ are only dependent on $Apwd_L \oplus Apwd_M$.
- Adversary can use these 8- LSB of $CCPwd_{M1} \oplus CCPwd_{L1}$ as a measure to trace a tag.

Secret Disclosure Attack on HLL

Active Adversary

Assume that an active adversary intercepts the message from the tag to the reader in step 2 and replaces R_{T1} by $R^i_{T1} = d^i_{t1} \| d^i_{t2} \| d^i_{t3} \| d^i_{t4} = i \| i \| i \| i$, $0 \geq i \geq 15.$

Then, one can state that $d^i_{v1} = d^i_{w1} = a_i a_i a_i a_i \in \{0000,1111\}$

If $d^i_{v1} = d^i_{w1}$ then $k_{d^i_{v1}} \oplus k_{d^i_{w1}} = 0$

If $d^i_{v1} \neq d^i_{w1}$ then $k_{d^i_{v1}} \oplus k_{d^i_{w1}} = k_0 \oplus k_{15}$

We assume that $k_0 \oplus k_{15} = k_{16} \oplus k_{31} = 1$ *to disitinguish* $d^i_{v1} = d^i_{w1}$ from $d^i_{v1} \neq d^i_{w1}$ given $k_{d^i_{v1}} \oplus k_{d^i_{w1}}$ .it is valid with the probability of 2^{-2}

Secret Disclosure Attack on HLL

Some details, given $CCPwd^{i}_{M1}$ and $CCPwd^{j}_{M1}$:

$$CCPwd^{i}_{M1} \oplus CCPwd^{j}_{M1} = Apwd_{M} \oplus PAD^{i}_{1} \oplus Apwd_{M} \oplus PAD^{j}_{1}$$

$$= PAD^{i}_{1} \oplus PAD^{j}_{1}$$

$$= (k_{d^{i}_{v1}} \oplus k_{d^{j}_{v1}})(k_{d^{i}_{v2}} \oplus k_{d^{j}_{v2}})(k_{d^{i}_{v3}} \oplus k_{d^{j}_{v3}})(k_{d^{i}_{v4}} \oplus k_{d^{j}_{v4}})||$$

$$(k_{d^{i}_{v1}+16} \oplus k_{d^{j}_{v1}+16})(k_{d^{i}_{v2}+16} \oplus k_{d^{j}_{v2}+16})(k_{d^{i}_{v3}+16} \oplus k_{d^{j}_{v3}+16})(k_{d^{i}_{v4}+16} \oplus k_{d^{j}_{v4}+16})||$$

$$(k_{d^{i}_{w1}} \oplus k_{d^{j}_{w1}})(k_{d^{i}_{w2}} \oplus k_{d^{j}_{w2}})(k_{d^{i}_{w3}} \oplus k_{d^{j}_{w3}})(k_{d^{i}_{w4}} \oplus k_{d^{j}_{w4}})||$$

$$(k_{d^{i}_{w1}+16} \oplus k_{d^{j}_{w1}+16})(k_{d^{i}_{w2}+16} \oplus k_{d^{j}_{w2}+16})(k_{d^{i}_{w3}+16} \oplus k_{d^{j}_{w3}+16})(k_{d^{i}_{w4}+16} \oplus k_{d^{j}_{w4}+16})||$$

Secret Disclosure Attack on HLL

$\left(CCPwd_{M1}^{0} \oplus CCPwd_{M1}^{1}\right)\Big|_{0} = k_{d_{v1}^{0}} \oplus k_{d_{v1}^{1}}$ and $d_{v1}^{0} = a_0a_0a_0a_0$ and $d_{v1}^{1} = a_1a_1a_1a_1$;

$\left(CCPwd_{M1}^{0} \oplus CCPwd_{M1}^{2}\right)\Big|_{0} = k_{d_{v1}^{0}} \oplus k_{d_{v1}^{2}}$ and $d_{v1}^{2} = a_2a_2a_2a_2$;

$\left(CCPwd_{M1}^{0} \oplus CCPwd_{M1}^{i}\right)\Big|_{0} = k_{d_{v1}^{0}} \oplus k_{d_{v1}^{i}}$ and $d_{v1}^{2} = a_ia_ia_ia_i$;

Given that $k_0 \oplus k_{15} = 1$ if $k_{d_{v1}^{0}} \oplus k_{d_{v1}^{i}} = 0$ then $a_0 = a_i$ otherwise $a_0 \neq a_i$;

In this way we receive 16 equations that each of them includes a_0 and another bit of $Apwd_L$.

We guess a_0 (with the probaility of 0.5) and determine $a_1, ..., a_{15}$ which gives $Apwd_L$;

A similar approach is use to determine $Apwd_M$;

Given $Apwd$ We can also determine $KPwd$;

The total success probability of this attack is $2^{-2} \times 2^{-1} \times 2^{-1}$.

OUTLINE

1. RFID Systems Overview
2. HYCLT Protocol
3. Security Analysis of HYCLT
4. HLL Protocol
5. Security Analysis of HLL
6. **Conclusion**

Conclusion

- We considered the security of two RFID mutual authentication protocols conforming to the EPC-C1G2 standard.
- We showed that an attacker can obtain the *Access* and *Kill* passwords with high probability.
- We showed that for HYCLT protocol an adversary can determine the *Access* password with a probability of 2^{-2}
- We showed in HLL scheme, the passive adversary can trace a tag with a probability of $1-2^{-4}$
- We showed in HLL scheme the active adversary can determine all bits of *Access* password with a probability of 2^{-4}

THANK YOU