Weaknesses in Two Recent Lightweight RFID Authentication Protocols

Pedro Peris-Lopez[1] Julio C. Hernandez-Castro[2]
J. M. E. Tapiador[3] Tieyan Li[4] Jan C.A. van der Lubbe[1]

Information and Communication Theory Group, Delft University of Technology

School of Computing, University of Portsmouth

Department of Computer Science, University of York,

Institute for Infocomm Research, A*STAR Singapore

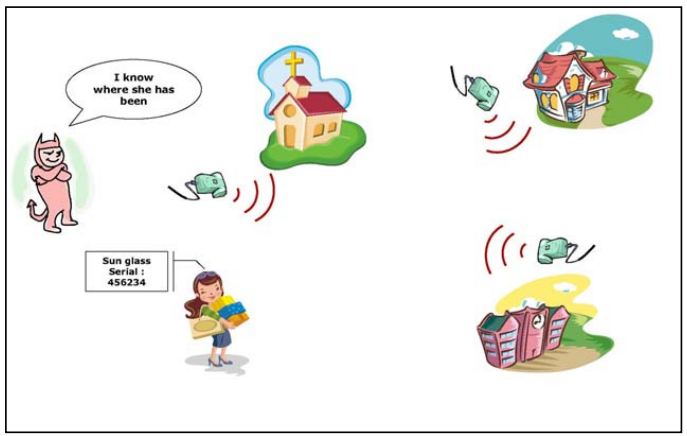
The 5th Workshop on RFID Security

RFID Technology

RFID systems may emerged one of the most pervasive technologies in history...

Privacy

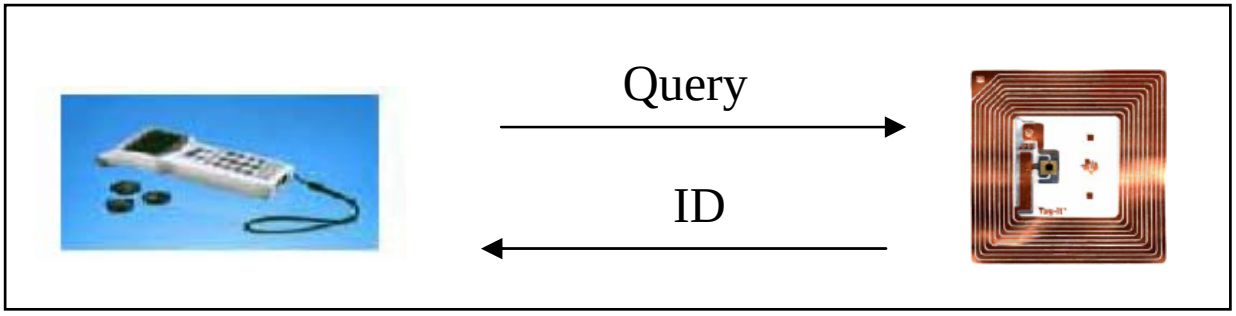
Tracking



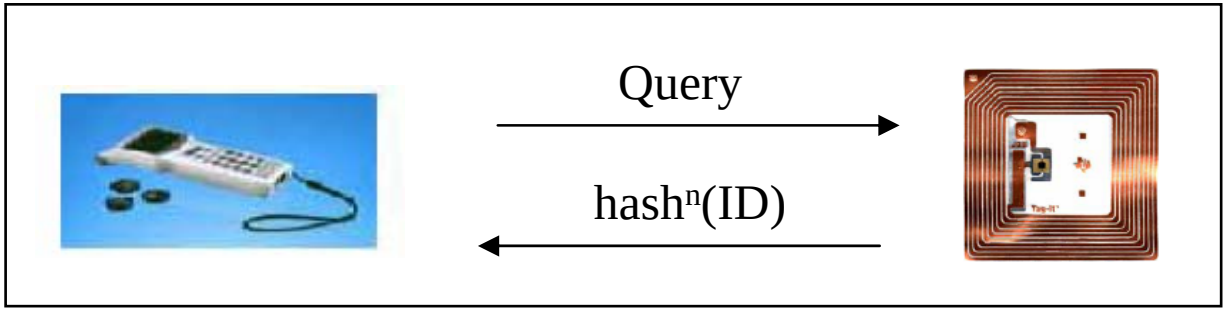
Others problems: eavesdropping, traffic analysis, physical attacks, denial of service, spoofing, counterfeiting, spoofing, etc.

Standard solutions

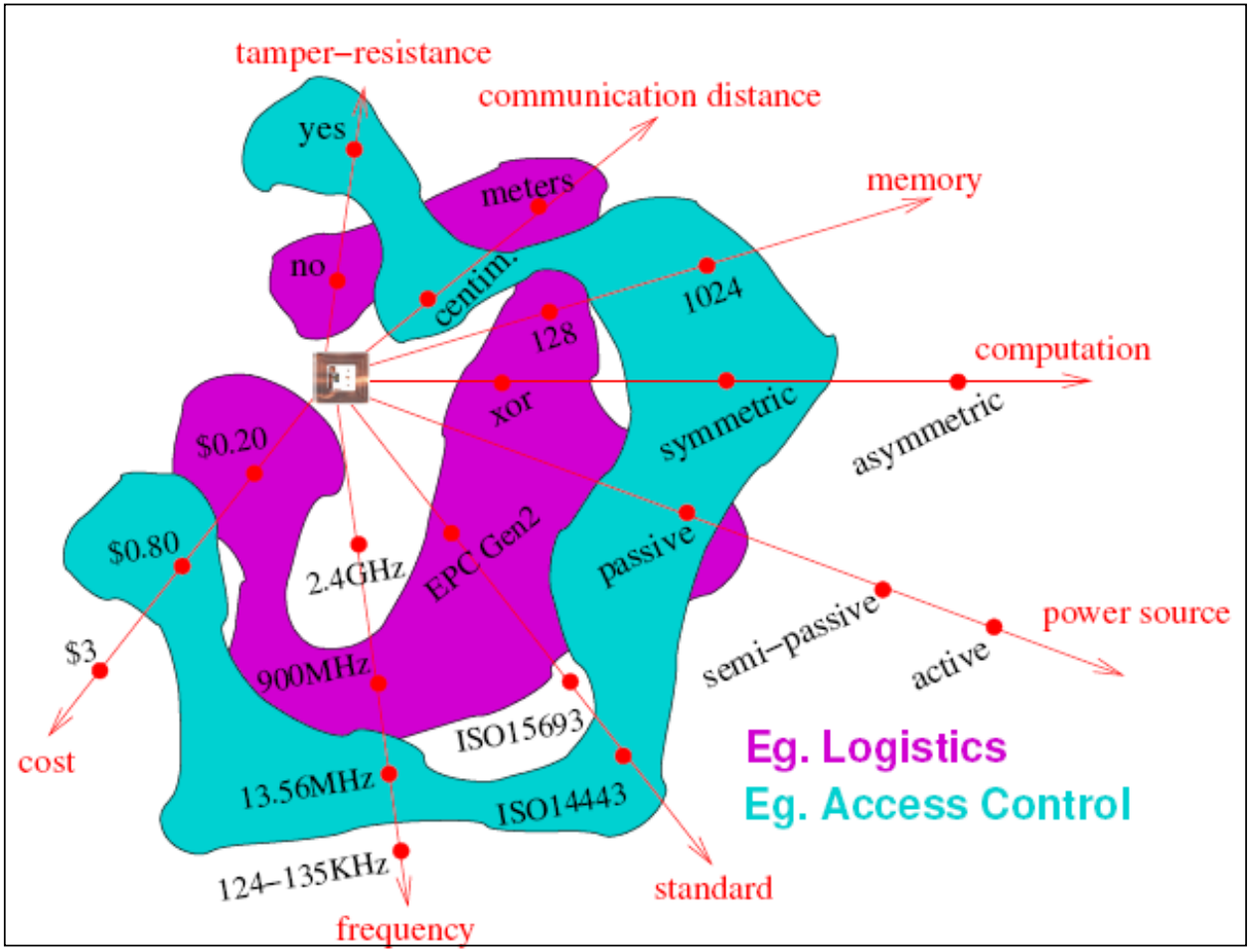
Non-secure Identification Systems



Hash-based Solution [1, 2, 3, 4, 5, 6]



Tag Characteristics



Tag Classification

Chien's classification [7]

- High-cost
  - Full-fledged tags: conventional cryptographic (i.e. symmetric/asymetric cryptography)
  - Simple tags: PRNG + one-way hash functions
- Low-cost
  - **Lightweight**: PRNG + simple functions (i.e. CRC checksum)
  - Ultra-lightweight: bitwise operations (i.e. XOR, AND, OR, etc.)

Mitra's Protocol (I)

- Author: Mala Mitra (2008) [8]
  (International Journal of Computer Science and Network Security)
- Objectives: traceability and cloning protection
- Assumptions:
  - Tags: simple operations + PRNG
  - Reader: computation of a modulo
  - Communications: backward and forward channel $\Longrightarrow$ eavesdropping
  - Memory requirements:
    - Tags: a static identifier $\{EPC_i\}$ and a key $\{K_i\}$
    - Readers: back-end database $\Longrightarrow$ key $\{K_i\}$

Mitra's Protocol (II)

Tags ($\mathcal{T}$) are authenticated by readers ($\mathcal{R}$):

Step 1 - $\mathcal{R} \rightarrow \mathcal{T}_i$: Request message

Step 2 - $\mathcal{T}_i$: Encrypted and anonymized version of its static identifier:

$$E_i(n) = RND(n) * K_i + EPC_i \tag{1}$$

Step 3 - $\mathcal{T}_i \rightarrow \mathcal{R}$: $E_i(n)$

Step 4 - $\mathcal{R}$: $EPC_i' = E_i(n) \mod K_i$

Cloning Attack (I)

Symmetric-Key cryptography:

Step 1 - $\mathcal{R} \rightarrow \mathcal{T}_i$: $RND(n)$

Step 2 - $\mathcal{T}_i \rightarrow \mathcal{R}$: $H_i(n) = g(K_i, RND(n))$

Step 3 - $\mathcal{R}$: Computes $H'_i(n) = g(K_i, RND(n))$ and checks if its value is identical to tag's answer H_i.

- g function: hash or encryption algorithm
- Low-cost RFID tags: severe resource limitations
- Mitra: $H_i(n) = E_i(n) = RND(n) * K_i + EPC_i$

Cloning Attack (II)

Theorem

In the TC-RFID protocol, an attacker that eavesdrops on two (non necessarily consecutive) authentication sessions $\{E_i(n), E_i(n+p)\}$ *between the target tag* $(\mathcal{T}_i)$ *and a legitimate reader* $(\mathcal{R})$ *is able to supplant a tag indefinitely by sending* $E_i' = E(n) + RND_r(q) * \Delta$ *as its authentication token, where*

$$\Delta = E_i(n) - E_i(n+p) = (RND(n) - R(n+p)) * K_i.$$

Step 1 - An attacker eavesdrops two authentication sessions

$$E_i(n) = RND(n) * K_i + EPC_i \quad (2)$$

$$E_i(n+p) = RND(n+p) * K_i + EPC_i \quad (3)$$

Step 2 - The attacker computes the difference:

$$\Delta = (RND(n) - RND(n+p)) * K_i \quad (4)$$

Step 3 - The attacker can supplant the tag:

$$E' = E(n) + \aleph * \Delta \quad (5)$$

Untraceability Problem

Defined as a game $\mathcal{G}$ divided into the following phases:

Phase 1 (Learning): $\mathcal{A}$ can send $\mathrm{Execute}$ queries to eavesdrop on protocol messages. Specifically, $\mathcal{A}$ sends r-$\mathrm{Execute}$ queries $(\{\mathrm{Execute}(\mathcal{R}, \mathcal{T}_0, i\}_{i=n}^{n+r})$ acquiring the following values: $\{E_0(i) = RND(i) * K_0 + EPC_0\}_{i=n}^{n+r}$

Phase 2 (Challenge): $\mathcal{A}$ chooses two fresh tags whose associated identifiers are EPC_0 and EPC_1. Then he sends $\mathrm{Test}(i, \mathcal{T}_0, \mathcal{T}_1)$ query. $\mathcal{A}$ is given a challenge cipher text $E_b(q)$ from the set $\{E_0(q), E_1(q)\}$, which depends on a chosen random bit $b \in \{0, 1\}$.

Phase 3 (Guessing): $\mathcal{A}$ finishes the game and outputs a bit d ($d \in \{0, 1\}$) as a guess of the value of b.

So the advantage of $\mathcal{A}$ in distinguishing whether he received EPC_0 or EPC_1, is defined as below:

$$\begin{aligned} Adv_{\mathcal{A}}^{UNT}(t, r) &= |Pr[\mathcal{A}\ wins] - Pr[random\ coin\ flip]| \\ &= |Pr[d = b] - \frac{1}{2}| \end{aligned} \tag{6}$$

Traceability Attack (I)

Theorem

The TC-RFID protocol, in an RFID system ($S = \{R_i, \mathcal{T}_0, \mathcal{T}_1, ...\}$) in which an adversary $\mathcal{A}$ can invoke two $\mathrm{Execute}(\mathcal{R}, \mathcal{T}, i)$ queries and one $\mathrm{Test}(i, \mathcal{T}_0, \mathcal{T}_1)$ query in an untraceability game $\mathcal{G}$, is vulnerable to traceability attacks, since the advantage for an adversary to win $\mathcal{G}$ is significant: $Adv_{\mathcal{A}}^{UNT}(t, 2) = 0.5 \gg \varepsilon(t, 2)$.

Phase 1 (Learning): $\mathcal{A}$ sends two $\mathrm{Execute}$ queries to $\mathcal{T}_0$.

$$E_0(n) = RND(n) * K_0 + EPC_0 \quad (7)$$

$$E_0(n+m) = RND(n+m) * K_0 + EPC_0 \quad (8)$$

Phase 2 (Challenge): $\mathcal{A}$ sends $\mathrm{Test}(q, \mathcal{T}_0, \mathcal{T}_1)$ query:

$$E_i(q) = \begin{cases} RND(q) * K_0 + EPC_0 & \text{if } b = 0 \\ RND(q) * K_1 + EPC_1 & \text{if } b = 1 \end{cases} \quad (9)$$

Traceability Attack (II)

Phase 3 (Guessing) $\mathcal{A}$ finishes $\mathcal{G}$ and outputs a bit d ($d \in \{0,1\}$) as his guess of the value b.

1. $\mathcal{A}$ computes the difference between Equations 7, 8:

$$\begin{aligned} \Delta_1 &= |E_0(n) - E_0(n+m)| \\ &= |(RND(n) * K_0 + EPC_0) - RND(n+m) * K_0 - EPC_0| \\ &= |(RND(n) - RND(n+m)) * K_0| \end{aligned}$$

2. $\mathcal{A}$ computes the difference between Equations 7, 9:

$$\Delta_2 = \begin{cases} |(RND(n) - RND(q)) * K_0| & \text{if } b = 0 \\ |RND(n) * K_0 - RND(q) * K_1 + EPC_0 - EPC_1| & \text{if } b = 1 \end{cases}$$

3. $\mathcal{A}$ uses the following decision rule:

$$d = \begin{cases} \text{if } gcd(\Delta_1, \Delta_2) \geq 2^{L/2} & d = 0 \\ \text{if } gcd(\Delta_1, \Delta_2) < 2^{L/2} & d = 1 \end{cases}$$

We have run 1000 experiments, with 2^{20} executions of the above game ($\mathcal{G}$) in each experiment

$$\begin{aligned} Adv_{\mathcal{A}}^{UNT}(t,2) &= |Pr[\mathcal{A} \text{ wins}] - Pr[\text{random coin flip}]| \\ &= |1.000 - \frac{1}{2}| = 0.5 \end{aligned} \quad (10)$$

Full Disclosure Attack (I)

Theorem

In the TC-RFID protocol, an adversary that eavesdrops on t (non necessarily consecutive) authentication sessions $\{E_i(n+c_1), E_i(n+c_2), ..., E_i(n+c_t)\}$ *between the target tag* $(\mathcal{T}_i)$ *and a legitimate reader* $(\mathcal{R})$ *is able to disclosure the secret key* K_i *by computing the greatest common divisor of the* $t-1$*independent differences* $\{|E_i(n+c_1) - E_i(n+c_2)|, ..., |E_i(n+c_1) - E_i(n+c_t)|\}$. *The probability of success is given by the equation bellow:*

$$Pr[\mathcal{A} \text{ reveals } K_i] = \frac{1}{\zeta(t-1)} \tag{11}$$

where c_i *represents an arbitrary constant value* ($c_q > c_p$; *if* $q > p$) *and* ζ *refers to the Riemann* ζ *function.*

Full Disclosure Attack (II)

The adversary starts observing the difference between three consecutive authentication messages linked with $\mathcal{T}_i$:

$$\begin{aligned} \delta_1 &= |RND(n+c_1) - RND(n+c_2)| * K_i = A * K_i \\ \delta_2 &= |RND(n+c_1) - RND(n+c_3)| * K_i = B * K_i \end{aligned} \tag{12}$$

Number theory $\Longrightarrow$ A and B are relative primes (coprimes)

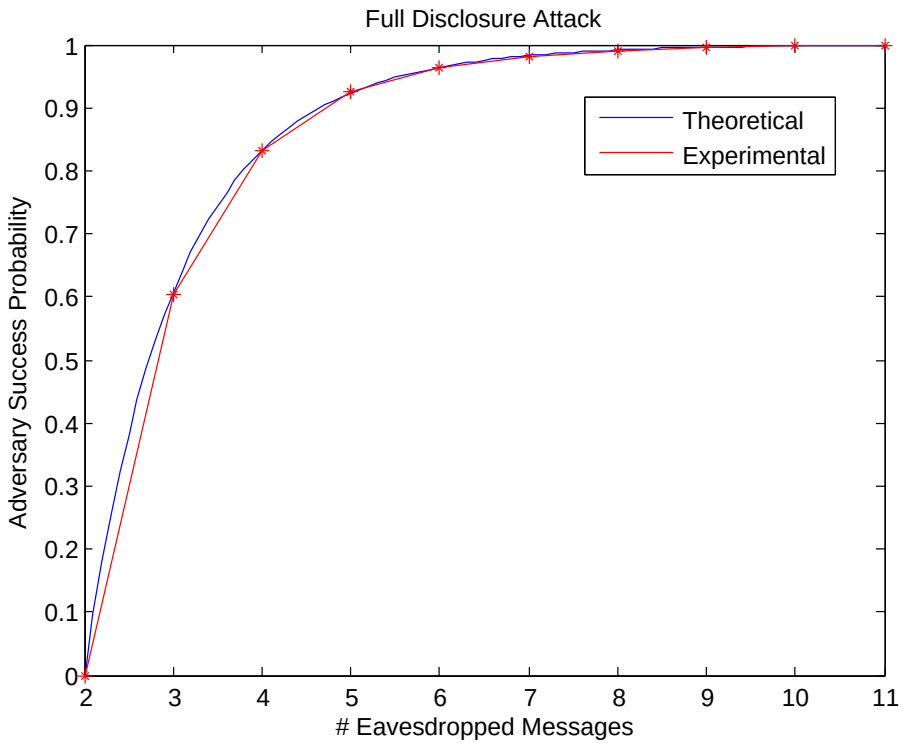
$$P(gcd(x_1, x_2) = 1) = \prod_p^{\infty}(1 - \frac{1}{p^2}) = (\prod_p^{\infty} \frac{1}{1-p^{-2}})^{-1} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2} \tag{13}$$

In general terms,

$$P(gcd(x_1, x_2, x_3, ..., x_q) = 1) = \prod_p^{\infty}(1 - \frac{1}{p^q}) = (\prod_p^{\infty} \frac{1}{1-p^{-q}})^{-1} = \frac{1}{\zeta(q)} \tag{14}$$

Full Disclosure Attack (III)

We run 10,000 experiments in order to estimate the probability of success to an adversary:



Qingling et al.'s Protocol (I)

- Author: Cai Qingling, Zhan Yiju and Wang Yonghua [9]
- Objectives:
  - Conforming to EPC Class-1 Generation-2 Standard
  - Correct its security weaknesses
- Gen-2 tags:
  - Tags are passive
  - Computation:
    - 16-bit PRNG + 16-bit CRC
    - Simple operations
  - 32-bit Kill and 32-bit Access Password
- Assumptions: Tags $\Longleftrightarrow$ Reader - a 32-bit EPC unique identifier (TID^{Tag_i}) and a 32-bit Access password ($APWD^{Tag_i}$)

Qingling et al.'s Protocol (II)

Step 1: $\mathcal{R} \rightarrow \mathcal{T}_i$: $Query$, RND^{Rdr}

Step 2: $\mathcal{T}_i \rightarrow \mathcal{R}$: M^{Tag_i}, RND^{Tag_i}

$$\begin{aligned} M_L^{Tag_i} &= CRC(TID_L^{Tag_i} \oplus RND^{Rdr} \oplus RND^{Tag_i}) \oplus APDW_L^{Tag_i} \\ M_M^{Tag_i} &= CRC(TID_M^{Tag_i} \oplus RND^{Rdr} \oplus RND^{Tag_i}) \oplus APDW_M^{Tag_i} \\ M^{Tag_i} &= M_L^{Tag_i} || M_M^{Tag_i} \end{aligned} \quad (15)$$

Step 3: The reader verifies whether the equation $M^{Tag_i} \oplus APDW^{Tag_i} = CRC(TID_L^{Tag_i} \oplus RND^{Rdr} \oplus RND^{Tag_i}) || CRC(TID_M^{Tag_i} \oplus RND^{Rdr} \oplus RND^{Tag})$ holds for any tag registered in the back-end database.

Step 4: $\mathcal{R} \rightarrow \mathcal{T}_i$: M^{Rdr}

$$\begin{aligned} M_L^{Rdr} &= CRC(TID_L^{Tag_i} \oplus RND^{Tag_i}) \oplus APDW_L^{Tag_i} \\ M_M^{Rdr} &= CRC(TID_M^{Tag_i} \oplus RND^{Tag_i}) \oplus APDW_M^{Tag_i} \\ M^{Rdr} &= M_L^{Rdr} || M_M^{Rdr} \end{aligned} \quad (16)$$

Step 5: On receiving M^{Rdr}, the tag verifies the equation $M^{Rdr} \oplus APDW^{Tag_i} = CRC(TID_L^{Tag_i} \oplus RND^{Tag_i}) || CRC(TID_M^{Tag_i} \oplus RND^{Tag_i})$.

Cyclic Redundancy Check (CRC)

Definition

The *crc* value for a given binary stream is the remainder $\{r(x)\}$ of dividing the polynomial associated with this stream $\{i(x)\}$ over another fixed polynomial $\{g(x)\}$, commonly known as the generator polynomial. The stream should be multiplied by x^N (N being the degree of the *crc* polynomial) prior to division:

$$i(x) \cdot x^N = d(x) \cdot g(x) + r(x) \qquad with \quad |r(x)| < |g(x)| \tag{17}$$

CRC functions possesses some properties that are undesirable from a security point of view:

Theorem

For any CRC (independent of its generator polynomial) and for any values a, $b \in F_2[x]$, it holds that:

$$CRC(a) \oplus CRC(b) = CRC(a \oplus b) \tag{18}$$

Tag Impersonation Attack

Theorem

A passive attacker, after eavesdropping one authentication session between an authentic tag ($\mathcal{T}_i$) and a genuine reader ($\mathcal{R}$), can impersonate the target tag by sending message $M_L^{Tag_i} \oplus CRC(\alpha) || M_M^{Tag_i} \oplus CRC(\alpha), RND_{new}^{Tag_i}$, where $\delta = RND_{new}^{Tag_i} \oplus RND^{Tag_i}$, $\gamma = RND_{new}^{Rdr} \oplus RND^{Rdr}$, and $\alpha = \delta \oplus \gamma$.

(1) $\mathcal{R} \rightarrow \mathcal{T}$: $Query$, RND^{Rdr}
(2) $\mathcal{T} \rightarrow \mathcal{R}$: M^{Tag_i}, RND^{Tag_i}

An attacker ($\mathcal{A}$) is able to correctly answer the readers's queries:

(1) $\mathcal{R} \rightarrow \mathcal{A}$: $Query$, RND_{new}^{Rdr}
(2) $\mathcal{A} \rightarrow \mathcal{R}$: $M_L^{Tag_i} \oplus CRC(\alpha) || M_M^{Tag_i} \oplus CRC(\alpha)$, $RND_{new}^{Tag_i}$

where $\delta = RND_{new}^{Tag_i} \oplus RND^{Tag_i}$, $\gamma = RND_{new}^{Rdr} \oplus RND^{Rdr}$, and $\alpha = \delta \oplus \gamma$.

Reader Impersonation Attack

Theorem

On capturing messages transmitted in a valid authentication session between an authentic tag ($\mathcal{T}_i$) and a genuine reader ($\mathcal{R}$), an adversary can supplant a reader by sending message $M_L^{Rdr} \oplus CRC(\delta) || M_M^{Tag_i} \oplus CRC(\delta)$, where $\delta = RND_{new}^{Tag_i} \oplus RND^{Tag_i}$.

First, the attacker observes the messages exchanged in a valid authentication session:

(1) $\mathcal{R} \rightarrow \mathcal{T}$: $Query$, RND^{Rdr}
(2) $\mathcal{T} \rightarrow \mathcal{R}$: M^{Tag_i}, RND^{Tag_i}
(2) $\mathcal{R} \rightarrow \mathcal{T}$: M^{Rdr}

The attacker ($\mathcal{A}$) can compute valid authentication messages to be sent to an authentic tag:

(1) $\mathcal{A} \rightarrow \mathcal{T}$: $Query$, RND_{new}^{Rdr}
(2) $\mathcal{T} \rightarrow \mathcal{A}$: $M_{new}^{Tag_i}$, $RND_{new}^{Tag_i}$
(3) $\mathcal{A} \rightarrow \mathcal{T}$: $M_L^{Rdr} \oplus CRC(\delta) || M_M^{Tag_i} \oplus CRC(\delta)$

where $\delta = RND_{new}^{Tag_i} \oplus RND^{Tag_i}$.

Traceability Attack (I)

Authors: untraceability $\Longrightarrow$ nonces

Experiment:

1. An attacker sends two fixed queries $\{Query, RND^{Rdr}\}$ to the target tag.
2. The tag responds with M^{Tag_i}, $RND_p^{Tag_i}$:

$$\{CRC(TID_L^{Tag_i} \oplus RND_p^{Tag_i} \oplus RND^{Rdr}) \oplus APDW_L^{Tag_i} \quad || \\ CRC(TID_M^{Tag_i} \oplus RND_q^{Tag_i} \oplus RND^{Rdr}) \oplus APDW_M^{Tag_i}\}_{p=q}^{p=q+1}$$

Theorem

QYY-Gen2 protocol, in an RFID system ($S = \{R_i, \mathcal{T}_0, \mathcal{T}_1, ...\}$ in which an adversary $\mathcal{A}$ can invoke one $\mathrm{Execute}(\mathcal{R}, \mathcal{T}, i)$ and $\mathrm{Test}(i, \mathcal{T}_0, \mathcal{T}_1)$ query in an untraceability game $\mathcal{G}$, is vulnerable to traceability attacks, since the advantage for an adversary to win the $\mathcal{G}$ is not negligible: $Adv_{\mathcal{A}}^{UNT}(t, r = 1) \simeq 0.499999 \gg \varepsilon(t, 1)$, t being a security parameter (i.e the bit length of the access and key password) and $\varepsilon(.)$ some negligible function.

Traceability Attack (II)

An adversary $\mathcal{A}$ performs the following steps to track tags:

Phase 1 (Learning): $\mathcal{A}$ sends an $\mathrm{Execute}$ query to $\mathcal{T}_0$. $\mathcal{A}$ acquires the random numbers used in the session and the tag's authentication message: RND^{Rdr}, $RND_q^{Tag_0}$, M^{Tag_0}.

$$\begin{aligned} M_L^{Tag_0} &= CRC(TID_L^{Tag_0} \oplus RND^{Rdr} \oplus RND_q^{Tag_0}) \oplus APDW_L^{Tag_0} \\ M_M^{Tag_0} &= CRC(TID_M^{Tag_0} \oplus RND^{Rdr} \oplus RND_q^{Tag_0}) \oplus APDW_M^{Tag_0} \\ M^{Tag_0} &= M_L^{Tag_0} || M_M^{Tag_0} \end{aligned} \tag{19}$$

Phase 2 (Challenge): $\mathcal{A}$ chooses two fresh tags whose associated identifiers are TID^{Tag_0} and TID^{Tag_1}. Then he sends query $\mathrm{Test}(q, \mathcal{T}_0, \mathcal{T}_1)$. As a result, $\mathcal{A}$ is given two random number messages RND_{new}^{Rdr}, $RND_{q+1}^{Tag_i}$, and an authentication message M^{Tag_i} from the set $\{M^{Tag_0}, M^{Tag_1}\}$, which depends on a chosen random bit $b \in \{0, 1\}$:

$$M^{Tag_i} = \begin{cases} CRC(TID_L^{Tag_0} \oplus RND_{new}^{Rdr} \oplus RND_{q+1}^{Tag_0}) \oplus APDW_L^{Tag_0} || \\ CRC(TID_M^{Tag_0} \oplus RND_{new}^{Rdr} \oplus RND_{q+1}^{Tag_0}) \oplus APDW_M^{Tag_0} & \text{if } b = 0 \\ CRC(TID_L^{Tag_1} \oplus RND_{new}^{Rdr} \oplus RND_{q+1}^{Tag_1}) \oplus APDW_L^{Tag_1} || \\ CRC(TID_M^{Tag_1} \oplus RND_{new}^{Rdr} \oplus RND_{q+1}^{Tag_1}) \oplus APDW_M^{Tag_1} & \text{if } b = 1 \end{cases} \tag{20}$$

Traceability Attack (III)

An adversary $\mathcal{A}$ performs the following steps to track tags:

Phase 3 (Guessing) $\mathcal{A}$ finishes $\mathcal{G}$ and outputs a bit d ($d \in \{0,1\}$) as its conjecture of value b. Specifically, we propose the following procedure to obtain d:

1. A constant value univocally associated with $\mathcal{T}_0$ is obtained by $\mathcal{A}$ (Equation 19):

$$\begin{aligned} X_L = M_L^{Tag_0} \oplus CRC(RND^{Rdr}) \oplus CRC(RND_q^{Tag_0}) &= \\ = CRC(TID_L^{Tag_0}) \oplus APDW_L^{Tag_0} & \\ X_M = M_M^{Tag_0} \oplus CRC(RND^{Rdr}) \oplus CRC(RND_q^{Tag_0}) &= \\ = CRC(TID_M^{Tag_0}) \oplus APDW_M^{Tag_0} & \\ X = X_L || X_M & \end{aligned} \tag{21}$$

2. $\mathcal{A}$ calculates the constant value associated with Equation 20:

$$Y = \begin{cases} CRC(TID_L^{Tag_0}) \oplus APDW_L^{Tag_0} || & \text{if } b = 0 \\ CRC(TID_M^{Tag_0}) \oplus APDW_L^{Tag_0} & \\ CRC(TID_L^{Tag_1}) \oplus APDW_L^{Tag_1} || & \text{if } b = 1 \\ CRC(TID_L^{Tag_1}) \oplus APDW_L^{Tag_1} & \end{cases} \tag{22}$$

Traceability Attack (IV)

Phase 3 (Guessing) - (cont.)

- $\mathcal{A}$ utilizes the following simple decision rule:

$$d = \begin{cases} 0 & \text{if } X = Y \\ 1 & \text{if } X \neq Y \end{cases} \tag{23}$$

The advantage of $\mathcal{A}$ in distinguishing whether the adversary interacts with $\mathcal{T}_0$ or $\mathcal{T}_1$:

$$Adv_{\mathcal{A}}^{UNT}(t, r) \quad = \quad |Pr[d = b] - \frac{1}{2}| = \frac{1}{2} - \frac{1}{2^{32}}$$

Note: there is a negligible probability $(1/2^n)$ that the value $CRC(TID_L^{Tag_i}) \oplus APDW_L^{Tag_i} || CRC(TID_M^{Tag_i}) \oplus APDW_L^{Tag_i}$ be equal for different tags (i.e T_0 and T_1)

Conclusions

- The cryptanalysis of two lightweight RFID protocols is presented
  - The use of random numbers is necessary but not sufficient condition to assure untraceability
  - *CRC* should be confined to detect error transmissions
  - Combining simple linear (i.e. bitwise operations) and non triangular operations (rotations)
  - EPC-C1G2 enhancements schemes are equal insecure as the standard
  - Rigorous security analysis are necessary

Questions?

Thank you

More information:
`http://www.lightweightcryptography.com/`


E.Y. Choi, S.M. Lee, and D.H. Lee.
Efficient RFID authentication protocol for ubiquitous computing environment.
In *Proc. of SECUBIQ'05*, LNCS, 2005.


D. Henrici and P. Müller.
Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers.
In *Proc. of PERSEC'04*, pages 149–153. IEEE Computer Society, 2004.


S.M. Lee, Y.J. Hwang, D.H. Lee, and J.I.L. Lim.
Efficient authentication for low-cost RFID systems.
In *Proc. of ICCSA'05*, volume 3480 of *LNCS*, pages 619–627, 2005.


M. Ohkubo, K. Suzuki, and S. Kinoshita.
Cryptographic approach to "privacy-friendly" tags.
In *Proc. of RFID Privacy Workshop*, 2003.


S.A. Weis, S.E. Sarma, R.L. Rivest, and D.W. Engels.
Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems.
In *Proc. of Security in Pervasive Comp.*, volume 2802 of *LNCS*, pages 201–212, 2004.


J. Yang, J. Park, H. Lee, K. Ren, and K. Kim.
Mutual authentication protocol for low-cost RFID.
Hand. of Ecrypt Workshop on RFID and Lightweight Crypto, 2005.


H.-Y. Chien. "SASI: A New Ultralightweight RFID Authentication Protocol Providing Strong Authentication and Strong Integrity". *IEEE Transactions on Dependable and Secure Computing* 4(4):337–340. Oct.-Dec. 2007.


Mitra, M.:
Privacy for RFID systems to prevent tracking and cloning.
International Journal of Computer Science and Network Security **8**(1) (January 2008) 1–5


Qingling, C., Yiju, Z., Yonghua, W.:
A minimalist mutual authentication protocol for RFID system & BAN logic analysis.
In: Proc. of CCCM '08, IEEE Computer Society (2008) 449–453