Authentication for RFID Tags: Observations on the HB Protocols

Erik Zenner

Technical University of Denmark (DTU)
Department of Mathematics
e.zenner@mat.dtu.dk

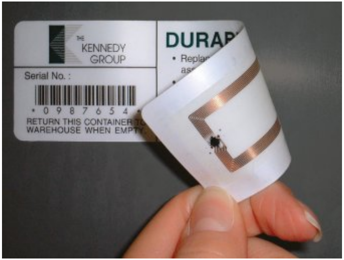
Aalborg, April 23, 2009

1. RFID Basics
2. The Original HB Protocol
3. The HB+ Protocol
4. Extensions, Observations, and Open Problems

Outline

What is RFID?

- RFID = Radio Frequency Identification
- **Idea:** Small devices (tags) identify themselves to a reader by radio signals.
- **Applications:** Retail, medicine, logistics, passport, payments, animals, humans...
- **Main focus today:** Cheap RFID tags for low-cost applications (5-cent chip)



Security challenges

- Depend on application
- Main security goals: Authentication, privacy
- Problem: RFID Chips very limited (often even no battery)

	Sample RFID chip (2005)	Requirements AES-128
RO memory	128-512 bit	key: 128 bit
RW memory	32-128 bit	state: 256 bit
Security circuit	200-2,000 gates	e.g. 3,400 gates
Performance	100 reads/sec	-

- Standard cryptographic primitives and protocols not usable
- New light-weight solutions required

Outline

Protocol description

- Protocol proposed by Hopper and Blum (Asiacrypt 2001)
- **Goal:** Provide light-weight entity authentication
- **Assumption:** Tag and Reader share a key $x \in \{0,1\}^n$
- **One round:** (round j)

Tag		**Reader**
	$\xleftarrow{a^j}$	Draw $a^j \in_R \{0,1\}^n$
Compute $u^j = a^j \circ x$ Draw $\epsilon^j \in_\eta \{0,1\}$		
Compute $z^j = u^j \oplus \epsilon^j$	$\xrightarrow{z^j}$	Check $z_j \stackrel{?}{=} a^j \circ x$

- Repeat r times ($j = 1, \ldots, r$)
- Accept if a clear majority of responses is correct

Adversary view

- For the adversary, a full protocol run (r rounds) looks as follows:

$$\begin{pmatrix} a_1^1 & a_2^1 & \dots & a_n^1 \\ a_1^2 & a_2^2 & \dots & a_n^2 \\ a_1^3 & a_2^3 & \dots & a_n^3 \\ \dots & \dots & \dots & \dots \\ a_1^r & a_2^r & \dots & a_n^r \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix} \oplus \begin{pmatrix} \epsilon_1 \\ \epsilon_2 \\ \epsilon_3 \\ \dots \\ \epsilon_r \end{pmatrix} = \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ \dots \\ z_r \end{pmatrix}$$

- Retrieving $(x_1, \dots, x_n)$ corresponds to decoding a random linear code.
- Known as "Learning Parity with Noise" (LPN) problem, NP-hard.
- LPN forms the basis for security proof (against passive adversary).

The active adversary case

Known problem: Vulnerable against active adversary

- Active adversary can **choose** the challenges $a^1, \ldots, a^r$
- Pick the first challenges as $a^j = (1, 0, 0, \ldots, 0)$
  - Tag always computes

$$
\begin{aligned}
y^j &= 1 \cdot x_1 \oplus 0 \cdot x_2 \oplus \ldots \oplus 0 \cdot x_n \oplus \epsilon^j \\
&= x_1 \oplus \epsilon^j
\end{aligned}
$$

  - All answers are noisy versions of x_1
  - Majority decision reveals true value of x_1
- Repeat for $x_2, \ldots, x_n$

Improvement/Generalisation: (D. Ruano)

- Choose the a^j s.th. they form a particularly efficient linear code
  $\Rightarrow$ This reduces the number of chosen challenges required

Outline

1. RFID Basics
2. The Original HB Protocol
3. The HB+ Protocol
4. Extensions, Observations, and Open Problems

Protocol description

- Protocol proposed by Juels and Weis (Crypto 2005)
- **Goal:** Make HB resistant against active attacks
- **Assumption:** Tag and Reader share **two** keys $x, y \in \{0,1\}^n$
- **One round:** (round j)

Tag		**Reader**
Draw $b^j \in_R \{0,1\}^n$	$\xrightarrow{b^j}$	
	$\xleftarrow{a^j}$	Draw $a^j \in_R \{0,1\}^n$
$u^j = (a^j \circ x) \oplus (b^j \circ y)$ Draw $\epsilon^j \in_\eta \{0,1\}$		
$z^j = u^j \oplus \epsilon^j$	$\xrightarrow{z^j}$	$z_j \stackrel{?}{=} (a^j \circ x) \oplus (b^j \circ y)$

- Repeat r times ($j = 1, \ldots, r$)
- Accept if a clear majority of responses is correct

Security: GRS attack (1)

- HB+ comes with a proof of security against active adversary
- But there exists an efficient attack!
- GRS attack (Gilbert/Robshaw/Sibert 2006):
  - Attacker modifies all r challenges by adding $(1, 0, \ldots, 0)$
  - Tag computes

$$\begin{aligned} z^j &= ((a^j \oplus (1, 0, \ldots, 0)) \circ x) \oplus (b^j \circ y) \oplus \epsilon^j \\ &= (a^j \circ x) \oplus ((1, 0, \ldots, 0) \circ x) \oplus (b^j \circ y) \oplus \epsilon^j \\ &= (a^j \circ x) \oplus x_1 \oplus (b^j \circ y) \oplus \epsilon^j \end{aligned}$$

  - Thus, all responses are changed by x_1 (either all are flipped, or none)
  - Attacker observes reader's reaction: If he accepts, then $x_1 = 0$, otherwise $x_1 = 1$
  - Repeat for $x_2, \ldots, x_n$

Security: GRS attack (2)

- Attack is only applicable in certain applications
- Attack is very simple and efficient (only $n \cdot r$ challenge/response pairs)
- But why is it possible (didn't we have a security proof)?
  - Proof model: Adversary modifies the challenges and observes the **tag's** response.
  - Here: Adversary modifies the challenges and observes the **reader's** response.
- Two ways of fixing the problem:
  1. Use protocol only in situations that correspond to the original security model (detection-base model)
  2. Modify the protocol to be secure in the new security model

Outline

The Quest for a new HB variant

- Many HB variants proposed and broken

Protocol	Year	Attack	Year
HB	2001	active	2001
HB+	2005	GRS	2006
HB^{++}	2006	GRS	2008
HB-MP	2007	passive	2008
HB*	2007	GRS	2008
$HB\text{-}MP^{+}$	2008	passive	-
Trusted-HB	2008	MITM(*)	2009
$HB^{\#}$	2008	MITM(*)	2008

(*) requiring many challenge-response pairs

- Can HB be made resistant against GRS attacks without adding too much complexity?

HB+ limits: Upper bounds

The RFID chip itself puts **upper bounds** on the parameters:

- Total key size (x and y) < 450 bit, $n < 225$ bit
- Number of rounds $r \leq 100$
  (due to time and bandwidth constraints)
- Noise parameter small
  (to allow distinguishing between guessing and correct answers)

HB+ limits: Example

- Let us set $n = 224$, $r = 100$.
- Assume that we want a false acceptance (FA) rate of < 0.001
- Then we obtain the following false rejection (FR) rates:

η	0.30	0.25	0.20
threshold	34	34	34
FR rate	1:6	1:61	1:2976

i.e. we would need to use $\eta \leq 0.2$

HB+ limits: Lower bounds

On the other hand, attacks put **lower bounds** on the same parameters:

- Total key size (x and y) > 500 bit, $n > 250$ bit
  (due to best known LPN algorithm)
- Noise parameter ≥ 0.25
  (due to standard technique against random codes)

Thus, upper and lower bounds contradict each other!
$\Rightarrow$ No good set of parameters for HB+

Conclusions

- Real need for RFID-suitable algorithms and protocols exists
- HB family promising, but not good enough
- Research directions:
  - **Cryptanalysis 1:** Better algorithms for LPN problem
  - **Cryptanalysis 2:** Better attacks against protocols
  - **Design 1:** Modify HB family to give full security
  - **Design 2:** Modify HB family s.th. consistent parameters exist
  - **Design 3:** Develop different types of RFID protocols

Questions? Comments?

Questions? Comments?

Thank you
for your
attention!