

Strong Authentication and Strong Integrity (SASI) is not that Strong

Gildas Avoine Xavier Carpent Benjamin Martin

Université catholique de Louvain
Belgium

RFIDsec 2010



Ultralightweight Cryptography

Chien's classification

- Full-fledged
- Simple
- Lightweight
- **Ultralightweight**

Ultra-lightweight primitives

- Bitwise Operation: \vee , \wedge , \oplus , ...
- Other Operations: $+$ (mod 2^L), Rotation (Modular, Hamming Weight), ...

Previous Work

Main Protocols

Ultralightweight Mutual Authentication Protocols (UMAP) Family

In 2006, by Peris-Lopez, Hernandez-Castro, Estevez-Tapiador, and Ribagorda

- *LMAP* - Lightweight Mutual Authentication Protocol
- *M²AP* - Minimalist Mutual Authentication Protocol
- *EMAP* - Efficient Mutual Authentication Protocol

Other Proposals

- SASI in 2007 by Chien
- Gossamer in 2008 by Peris-Lopez *et al.*

Outline

1 Synchronized Protocols

2 SASI

3 Our Proposal

4 Conclusion

Synchronized Protocols

$R \xrightarrow{\text{hello}} T$

$R \xleftarrow{IDS} T$

$R \xrightarrow{M_R} T$

$R \xleftarrow{M_T} T$

Messages

$$M_R = f(ID, IDS, K, n)$$

$$M_T = g(ID, IDS, K, n)$$

Update

$$(IDS^{next}, K^{next}) = h(ID, IDS, K, n)$$

SASI

The Parameters

Strong Authentication and Strong Integrity (Chien, 2007)

- Based on the UMAP family
- Security Parameters:
 - 1 The unique identifier of a tag: ID .
 - 2 Length in bits of ID : L (Typically $L = 96$).
- Internal State of a Tag:
 - 1 The index pseudonym of a tag: IDS .
 - 2 A pair of keys: K_1, K_2 .

SASI

Protocol Description

$$R \xrightarrow{\text{hello}} T$$

$$R \xleftarrow{IDS} T$$

$$R \xrightarrow{A||B||C} T$$

$$R \xleftarrow{D} T$$

Messages

$$A = IDS \oplus K_1 \oplus n_1$$

$$B = (IDS \vee K_2) + n_2$$

$$\bar{K}_1 = \text{Rot}(K_1 \oplus n_2, K_1)$$

$$\bar{K}_2 = \text{Rot}(K_2 \oplus n_1, K_2)$$

$$C = (K_1 \oplus \bar{K}_2) + (\bar{K}_1 \oplus K_2)$$

$$D = (\bar{K}_2 + ID) \oplus ((K_1 \oplus K_2) \vee \bar{K}_1)$$

Update

$$IDS^{next} = (IDS + ID) \oplus n_2 \oplus \bar{K}_1$$

$$K_1^{next} = \bar{K}_1$$

$$K_2^{next} = \bar{K}_2$$

SASI

Protocol Description

$$R \xrightarrow{\text{hello}} T$$

$$R \xleftarrow{IDS} T$$

$$R \xrightarrow{A||B||C} T$$

$$R \xleftarrow{D} T$$

Messages

$$A = IDS \oplus K_1 \oplus n_1$$

$$B = (IDS \vee K_2) + n_2$$

$$\bar{K}_1 = \text{Rot}(K_1 \oplus n_2, K_1)$$

$$\bar{K}_2 = \text{Rot}(K_2 \oplus n_1, K_2)$$

$$C = (K_1 \oplus \bar{K}_2) + (\bar{K}_1 \oplus K_2)$$

$$D = (\bar{K}_2 + ID) \oplus ((K_1 \oplus K_2) \vee \bar{K}_1)$$

Update

$$IDS^{next} = (IDS + ID) \oplus n_2 \oplus \bar{K}_1$$

$$K_1^{next} = \bar{K}_1$$

$$K_2^{next} = \bar{K}_2$$

SASI

Known Attacks

Active Attacks

- Desynchronization and Full-disclosure:
 - D'Arco and De Santis 2008
 - Sun, Ting, and Wang 2009
- Traceability: Cao, Bertino, and Lei 2008

Passive Attacks

- Traceability: Phan 2008
- Full-disclosure: Hernandez-Castro, Estevez-Tapiador, Peris-Lopez, and Quisquater 2008

Our Proposal

Overview

Execute the traceability attack to get $[ID]_0$

repeat

if $[IDS]_0 = 1$ **then**

if the previous $[K_1]_0$ was known **then**

 Compute n_2 probabilistically (1)

 Compute ID probabilistically (2)

for all $i \in [1, L - 1]$ **do**

 Update the knowledge of $[ID]_i$ with the advantages
 of (1) and (2) and the rotation

end for

end if

 Compute $[K_1^{next}]_0 = [ID]_0 \oplus [B]_0 \oplus [IDS^{next}]_0$

end if

until all the bits of ID are found with satisfactory probability

Our Proposal

Overview

Execute the traceability attack to get $[ID]_0$

repeat

if $[IDS]_0 = 1$ **then**

if the previous $[K_1]_0$ was known **then**

 Compute n_2 probabilistically (1)

 Compute ID probabilistically (2)

for all $i \in [1, L - 1]$ **do**

 Update the knowledge of $[ID]_i$ with the advantages
 of (1) and (2) and the rotation

end for

end if

 Compute $[K_1^{next}]_0 = [ID]_0 \oplus [B]_0 \oplus [IDS^{next}]_0$

end if

until all the bits of ID are found with satisfactory probability

Our proposal

Traceability attack

Notation

Given X a bit vector, we denote $[X]_i$ the i -th bit of vector. By convention, $[X]_0$ is the Least Significant Bit.

Lemma

If $[IDS]_0 = 1$, and $[B]_0 \oplus [C]_0 \oplus [D]_0 \oplus [IDS^{next}]_0 = 1$, then

$$[ID]_0 = [B]_0 \oplus [IDS^{next}]_0 \oplus 1.$$

Result

At each eavesdropped session, we retrieve $[ID]_0$, with probability $1/4$.

Our proposal

Overview

Execute the traceability attack to get $[ID]_0$

repeat

if $[IDS]_0 = 1$ **then**

if the previous $[K_1]_0$ was known **then**

 Compute n_2 probabilistically (1)

 Compute ID probabilistically (2)

for all $i \in [1, L - 1]$ **do**

 Update the knowledge of $[ID]_i$ with the advantages
 of (1) and (2) and the rotation

end for

end if

 Compute $[K_1^{next}]_0 = [ID]_0 \oplus [B]_0 \oplus [IDS^{next}]_0$

end if

until all the bits of ID are found with satisfactory probability

Our proposal

Overview

Execute the traceability attack to get $[ID]_0$

repeat

if $[IDS]_0 = 1$ **then**

if the previous $[K_1]_0$ was known **then**

 Compute n_2 probabilistically (1)

 Compute ID probabilistically (2)

for all $i \in [1, L - 1]$ **do**

 Update the knowledge of $[ID]_i$ with the advantages
 of (1) and (2) and the rotation

end for

end if

 Compute $[K_1^{next}]_0 = [ID]_0 \oplus [B]_0 \oplus [IDS^{next}]_0$

end if

until all the bits of ID are found with satisfactory probability

Our proposal

Overview

Execute the traceability attack to get $[ID]_0$

repeat

if $[IDS]_0 = 1$ **then**

if the previous $[K_1]_0$ was known **then**

Compute n_2 probabilistically (1)

Compute ID probabilistically (2)

for all $i \in [1, L - 1]$ **do**

Update the knowledge of $[ID]_i$ with the advantages of (1) and (2) and the rotation

end for

end if

Compute $[K_1^{next}]_0 = [ID]_0 \oplus [B]_0 \oplus [IDS^{next}]_0$

end if

until all the bits of ID are found with satisfactory probability

Our proposal

Subproblem 1

Notation

Given A, B , two L -bits vectors, and i an index, $\mathcal{C}(A, B, i)$ is the carry at the index i of the sum $A + B$.

Notation

Given A, B , two L -bits vectors, and i an index, $\mathcal{B}(A, B, i)$ is the borrow at index i of the difference $A - B$.

$$[a + b]_i = [a]_i \oplus [b]_i \oplus \mathcal{C}(a, b, i - 1),$$

$$[a - b]_i = [a]_i \oplus [b]_i \oplus \mathcal{B}(a, b, i - 1).$$

Our proposal

Subproblem 1

Relation

$$B = (IDS \vee K_2) + n_2$$

$$n_2 = B - (IDS \vee K_2)$$

$$[n_2]_i = [B]_i \oplus [IDS \vee K_2]_i \oplus \mathcal{B}(B, IDS \vee K_2, i - 1).$$

Result

Knowing IDS and B , and the relation

$$B = (IDS \vee K_2) + n_2,$$

we can guess roughly one third of n_2 .

Our proposal

Overview

Execute the traceability attack to get $[ID]_0$

repeat

if $[IDS]_0 = 1$ **then**

if the previous $[K_1]_0$ was known **then**

Compute n_2 probabilistically (1)

Compute ID probabilistically (2)

for all $i \in [1, L - 1]$ **do**

Update the knowledge of $[ID]_i$ with the advantages of (1) and (2) and the rotation

end for

end if

Compute $[K_1^{next}]_0 = [ID]_0 \oplus [B]_0 \oplus [IDS^{next}]_0$

end if

until all the bits of ID are found with satisfactory probability

Our proposal

Overview

Execute the traceability attack to get $[ID]_0$

repeat

if $[IDS]_0 = 1$ **then**

if the previous $[K_1]_0$ was known **then**

Compute n_2 probabilistically (1)

Compute ID probabilistically (2)

for all $i \in [1, L - 1]$ **do**

Update the knowledge of $[ID]_i$ with the advantages of (1) and (2) and the rotation

end for

end if

Compute $[K_1^{next}]_0 = [ID]_0 \oplus [B]_0 \oplus [IDS^{next}]_0$

end if

until all the bits of ID are found with satisfactory probability

Our proposal

Subproblem 2

Relation

$$(IDS + ID) = (IDS) + (ID)$$

$$[IDS + ID]_i = [IDS]_i \oplus [ID]_i \oplus \mathcal{C}(IDS, ID, i - 1)$$

$$[ID]_i = [IDS]_i \oplus [IDS + ID]_i \oplus \mathcal{C}(IDS, ID, i - 1).$$

Result

Knowing IDS and having a little bit of information on $IDS + ID$, we can get a little bit of information on ID .

Our proposal

Overview

Execute the traceability attack to get $[ID]_0$

repeat

if $[IDS]_0 = 1$ **then**

if the previous $[K_1]_0$ was known **then**

Compute n_2 probabilistically (1)

Compute ID probabilistically (2)

for all $i \in [1, L - 1]$ **do**

Update the knowledge of $[ID]_i$ with the advantages of (1) and (2) and the rotation

end for

end if

Compute $[K_1^{next}]_0 = [ID]_0 \oplus [B]_0 \oplus [IDS^{next}]_0$

end if

until all the bits of ID are found with satisfactory probability

Our proposal

Overview

Execute the traceability attack to get $[ID]_0$

repeat

if $[IDS]_0 = 1$ **then**

if the previous $[K_1]_0$ was known **then**

 Compute n_2 probabilistically (1)

 Compute ID probabilistically (2)

for all $i \in [1, L - 1]$ **do**

 Update the knowledge of $[ID]_i$ with the advantages of (1) and (2) and the rotation

end for

end if

 Compute $[K_1^{next}]_0 = [ID]_0 \oplus [B]_0 \oplus [IDS^{next}]_0$

end if

until all the bits of ID are found with satisfactory probability

Our proposal

Knowledge Update – Analogy

Experiment : Biased coin (“dynamic” bias)

H	H	T	T	H
0.6	0.8	0.5	0.6	0.6

$$\Rightarrow \Pr(\text{Biased side} = H | \text{Observations}) \approx 0.86$$

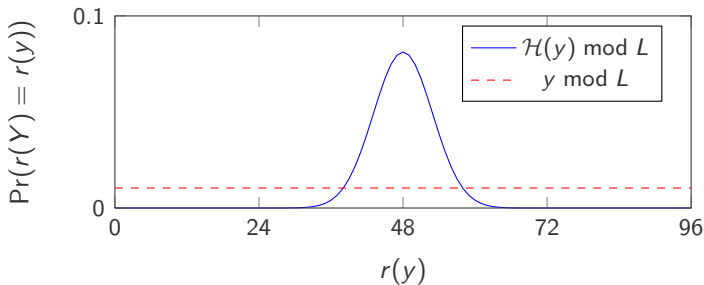
Our proposal

Rotations

$Rot(x, y) \rightarrow$ circular left shift of x of $r(y)$ bits

Hamming weight-based: $r(y) = \mathcal{H}(y) \bmod L$

Modular: $r(y) = y \bmod L$



Our proposal

Overview

Execute the traceability attack to get $[ID]_0$

repeat

if $[IDS]_0 = 1$ **then**

if the previous $[K_1]_0$ was known **then**

 Compute n_2 probabilistically (1)

 Compute ID probabilistically (2)

for all $i \in [1, L - 1]$ **do**

 Update the knowledge of $[ID]_i$ with the advantages of (1) and (2) and the rotation

end for

end if

 Compute $[K_1^{next}]_0 = [ID]_0 \oplus [B]_0 \oplus [IDS^{next}]_0$

end if

until all the bits of ID are found with satisfactory probability

Our proposal

Overview

Execute the traceability attack to get $[ID]_0$

repeat

if $[IDS]_0 = 1$ **then**

if the previous $[K_1]_0$ was known **then**

 Compute n_2 probabilistically (1)

 Compute ID probabilistically (2)

for all $i \in [1, L - 1]$ **do**

 Update the knowledge of $[ID]_i$ with the advantages
 of (1) and (2) and the rotation

end for

end if

 Compute $[K_1^{next}]_0 = [ID]_0 \oplus [B]_0 \oplus [IDS^{next}]_0$

end if

until all the bits of ID are found with satisfactory probability

Computing $[K_1^{next}]_0$

Relation

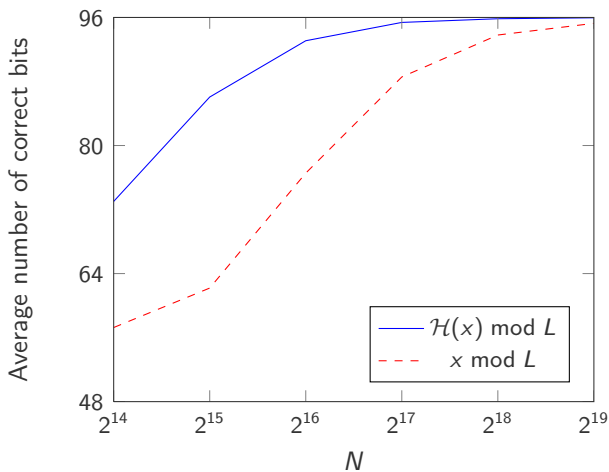
$$B = (IDS \vee K_2) + n_2$$
$$[B]_0 = ([IDS]_0 \vee [K_2]_0) \oplus [n_2]_0$$

Thus, if $[IDS]_0 = 1$, $[n_2]_0 = [B]_0 \oplus 1$. Furthermore,

Relation

$$IDS^{next} = (IDS + ID) \oplus n_2 \oplus K_1^{next}$$
$$[IDS^{next}]_0 = [IDS]_0 \oplus [ID]_0 \oplus [n_2]_0 \oplus [K_1^{next}]_0$$
$$[K_1^{next}]_0 = [IDS^{next}]_0 \oplus [IDS]_0 \oplus [ID]_0 \oplus [n_2]_0$$

Efficiency



Conclusion

SASI:

- Passive Adversary
- Roughly 2^{17} authentication sessions
⇒ Practically feasible (but optimizations possible)

Ultralightweight primitives:

- Equations such as $a = (b \vee c) + d$ weaker than they appear
- Rotations : non-triangularity but has weaknesses