Mihály Bárász, Balázs Boros,
Péter Ligeti, Krisztina Lója,
Dániel A. Nagy

Breaking LMAP

Eötvös Loránd University, Budapest, Hungary
ELTECRYPT Research Group

LMAP

Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estvez Tapiador, Arturo Ribagorda:

LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags

in: Proc. of RFIDSec06 Workshop on RFID Security, July 12-14, Graz, Austria, 2006.

LMAP Minimalist cryptography

Simple operations:

- Bitwise XOR ($\oplus$)
- Bitwise OR ($\vee$)
- Addition mod 2^m (+)

The goal:

- low complexity in the tags
- adequate level of security

Is it possible?

Active attack against LMAP

Tieyan Li, Guilin Wang:

Security Analysis of Two Ultra-Lightweight Mutual Authentication Protocol for Low-cost RFID tags,

IFIP SEC 2007.

- Active attack against the LMAP
  - de-synchronization attack
  - full-disclosure attack
- 96 rounds of authentication is needed

Breaking LMAP

Our attack:

- **Passive** attack
- Intercepting **a few consecutive rounds** of authentication of the same tag is enough to calculate the keys and all other secrets
- The attacker can **impersonate the tag** in the subsequent rounds

LMAP keys and secrets

$K = K_1 \| K_2 \| K_3 \| K_4$ the keys

384 bit = 96 + 96 + 96 + 96 bit

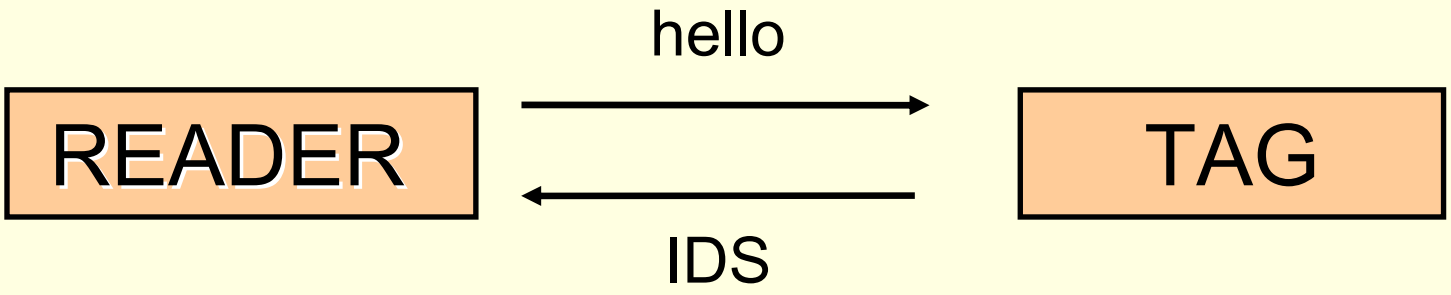
ID: a constant identification number (96 bit)

IDS: an identification number that must be updated after every round of authentication (96 bit)

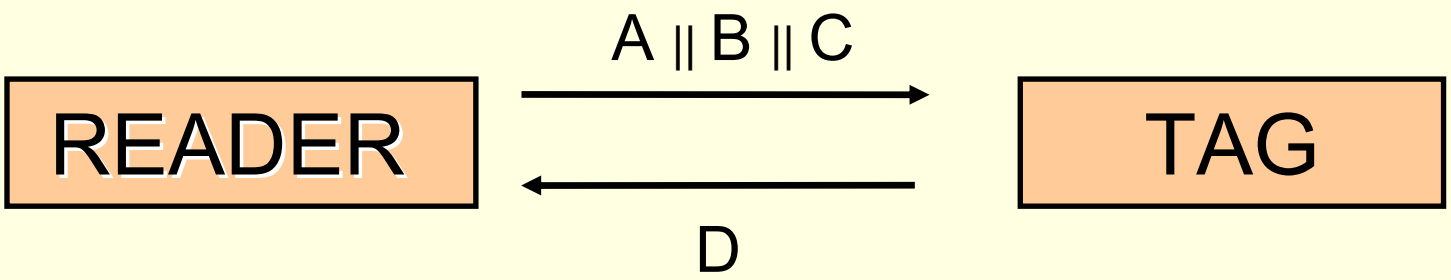
n_1, n_2: random numbers generated by the reader (96 bit)

Mutual authentication

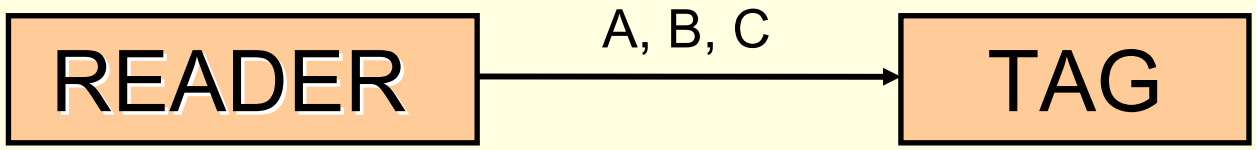
Tag identification



Mutual authentication



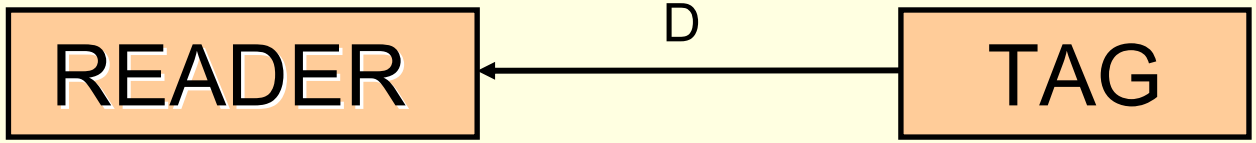
Messages A, B, C, D



A = IDS $\oplus$ K_1 $\oplus$ n_1 → now the tag knows n_1

B = (IDS $\vee$ K_2) + n_1 → reader authentication

C = IDS + K_3 + n_2 → the tag knows n_2



D = (IDS + ID) $\oplus$ n_1 $\oplus$ n_2 → tag authentication

Updating the keys and IDS

$$IDS^{(n+1)} = (IDS^{(n)} + (n_2^{(n)} \oplus K_4^{(n)})) \oplus ID$$

$$K_1^{(n+1)} = K_1^{(n)} \oplus n_2^{(n)} \oplus (K_3^{(n)} + ID)$$

$$K_2^{(n+1)} = K_2^{(n)} \oplus n_2^{(n)} \oplus (K_4^{(n)} + ID)$$

$$K_3^{(n+1)} = (K_3^{(n)} \oplus n_1^{(n)}) + (K_1^{(n)} \oplus ID)$$

$$K_4^{(n+1)} = (K_4^{(n)} \oplus n_1^{(n)}) + (K_2^{(n)} \oplus ID)$$

$A = IDS \oplus K_1 \oplus n_1$
$B = (IDS \vee K_2) + n_1$
$C = IDS + K_3 + n_2$
$D = (IDS + ID) \oplus n_1 \oplus n_2$

Weaknesses of the LMAP

- LMAP uses only bitwise operations and addition modulo 2^{96} ⟶ every bit depends only on the less significant bits
- For the least significant bits the XOR operation and addition modulo 2^{96} are the same ⟶ we can compute the least significant bits

$$A = IDS \oplus K_1 \oplus n_1$$
$$B = (IDS \vee K_2) + n_1$$
$$C = IDS + K_3 + n_2$$
$$D = (IDS + ID) \oplus n_1 \oplus n_2$$

$$IDS^{(n+1)} = (IDS^{(n)} + (n_2^{(n)} \oplus K_4^{(n)})) \oplus ID$$
$$K_1^{(n+1)} = K_1^{(n)} \oplus n_2^{(n)} \oplus (K_3^{(n)} + ID)$$
$$K_2^{(n+1)} = K_2^{(n)} \oplus n_2^{(n)} \oplus (K_4^{(n)} + ID)$$
$$K_3^{(n+1)} = (K_3^{(n)} \oplus n_1^{(n)}) + (K_1^{(n)} \oplus ID)$$
$$K_4^{(n+1)} = (K_4^{(n)} \oplus n_1^{(n)}) + (K_2^{(n)} \oplus ID)$$

Weaknesses of the LMAP

- The addition modulo 2^{96} means no difficulty if we know every less significant bit
- The bitwise OR ($\vee$) operation is a weak point in the protocol.

  $B = (IDS \vee K_2) + n_1 \longrightarrow$ information about n_1 with the help of 1 bits of the IDS

$A = IDS \oplus K_1 \oplus n_1$
$B = (IDS \vee K_2) + n_1$
$C = IDS + K_3 + n_2$
$D = (IDS + ID) \oplus n_1 \oplus n_2$

The steps of breaking LMAP

- We will need a few consecutive rounds of authentication of the same tag
- We compute the least significant bits (the 96^{th} bits) in a round where the least significant bit of the IDS is 1
- Next we compute the 95^{th} bits
- We will need *r* rounds so that

  $[IDS^{(n)}]_k \vee [IDS^{(n+1)}]_k \vee [IDS^{(n+2)}]_k \vee \ldots \vee [IDS^{(n+r-1)}]_k = 1$

  for every k = 1, 2, …, 96

  + two more rounds and we can compute every key and secret

$[M^{(n)}]_k$: the *k*-th bit of message M in round n

$A = IDS \oplus K_1 \oplus n_1$
$B = (IDS \vee K_2) + n_1$
$C = IDS + K_3 + n_2$
$D = (IDS + ID) \oplus n_1 \oplus n_2$

The least significant bits: n_1, K_1

Let us assume, that $[IDS^{(n)}]_{96} = 1$

$([IDS^{(n)}]_{96} \vee [K_2^{(n)}]_{96}) = 1$

$B = (IDS \vee K_2) + n_1$

$[B^{(n)}]_{96} = 1 \oplus [n_1^{(n)}]_{96}$

$[n_1^{(n)}]_{96} = [B^{(n)}]_{96} \oplus 1$

$[M^{(n)}]_k$: the *k*-th bit of message M in round n

Known

Unknown

Is actually calculated

Known: A, B, C, D, IDS

Unknown: K_1, K_2, K_3, K_4, ID, n_1, n_2

$[A^{(n)}]_{96} = [IDS^{(n)}]_{96} \oplus [K_1^{(n)}]_{96} \oplus [n_1^{(n)}]_{96}$

$[K_1^{(n)}]_{96} = [A^{(n)}]_{96} \oplus [IDS^{(n)}]_{96} \oplus [n_1^{(n)}]_{96}$

Unknown: K_1, K_2, K_3, K_4, ID, n_1, n_2

Known: the 96th bit of n_1, K_1

$A = IDS \oplus K_1 \oplus n_1$

$B = (IDS \vee K_2) + n_1$

$C = IDS + K_3 + n_2$

$D = (IDS + ID) \oplus n_1 \oplus n_2$

The least significant bits: K_4

$D = (IDS + ID) \oplus n_1 \oplus n_2$

$[D^{(n)}]_{96} = [IDS^{(n)}]_{96} \oplus [ID]_{96} \oplus [n_1^{(n)}]_{96} \oplus [n_2^{(n)}]_{96}$

$IDS^{(n+1)} = (IDS^{(n)} + (n_2^{(n)} \oplus K_4^{(n)})) \oplus ID$

$[IDS^{(n+1)}]_{96} = ([IDS^{(n)}]_{96} + ([n_2^{(n)}]_{96} \oplus [K_4^{(n)}]_{96})) \oplus$
$\oplus [ID]_{96}$

$[K_4^{(n)}]_{96} = [IDS^{(n+1)}]_{96} \oplus [D^{(n)}]_{96} \oplus [n_1^{(n)}]_{96}$

Unknown: the 96th bit of K_2, K_3, ID, n_2

Known: the 96th bit of n_1, K_1, K_4

$A = IDS \oplus K_1 \oplus n_1$
$B = (IDS \vee K_2) + n_1$
$C = IDS + K_3 + n_2$
$D = (IDS + ID) \oplus n_1 \oplus n_2$

Messages A, B, C, D in round n+1

$[A^{(n+1)}]_{96} = [IDS^{(n+1)}]_{96} \oplus [K_1^{(n)}]_{96} \oplus [n_2^{(n)}]_{96} \oplus [K_3^{(n)}]_{96} \oplus$
$\oplus [ID]_{96} \oplus [n_1^{(n+1)}]_{96}$

$[B^{(n+1)}]_{96} = ([IDS^{(n+1)}]_{96} \vee ([K_2^{(n)}]_{96} \oplus [n_2^{(n)}]_{96} \oplus [K_4^{(n)}]_{96} \oplus$
$\oplus [ID]_{96})) \oplus [n_1^{(n+1)}]_{96}$

$[C^{(n+1)}]_{96} = [IDS^{(n+1)}]_{96} \oplus [K_3^{(n)}]_{96} \oplus [n_1^{(n)}]_{96} \oplus [K_1^{(n)}]_{96} \oplus$
$\oplus [ID]_{96} \oplus [n_2^{(n+1)}]_{96}$

$[D^{(n+1)}]_{96} = [IDS^{(n+1)}]_{96} \oplus [ID]_{96} \oplus [n_1^{(n+1)}]_{96} \oplus [n_2^{(n+1)}]_{96}$

(If $[IDS^{(n+1)}]_{96} = 1$, then $[B^{(n+1)}]_{96} = 1 \oplus [n_1^{(n+1)}]_{96}$)

$A = IDS \oplus K_1 \oplus n_1$
$B = (IDS \vee K_2) + n_1$
$C = IDS + K_3 + n_2$
$D = (IDS + ID) \oplus n_1 \oplus n_2$

The least significant bits: $n_2^{(n+1)}$

$$[C^{(n+1)}]_{96} = [IDS^{(n+1)}]_{96} \oplus [K_3^{(n)}]_{96} \oplus [n_1^{(n)}]_{96} \oplus \oplus [K_1^{(n)}]_{96} \oplus [ID]_{96} \oplus [n_2^{(n+1)}]_{96}$$

$$[C^{(n)}]_{96} = [IDS^{(n)}]_{96} \oplus [K_3^{(n)}]_{96} \oplus [n_2^{(n)}]_{96}$$

$$[D^{(n)}]_{96} = [IDS^{(n)}]_{96} \oplus [ID]_{96} \oplus [n_1^{(n)}]_{96} \oplus [n_2^{(n)}]_{96}$$

$$[C^{(n)}]_{96} \oplus [D^{(n)}]_{96} = [ID]_{96} \oplus [n_1^{(n)}]_{96} \oplus [K_3^{(n)}]_{96}$$

$$[n_2^{(n+1)}]_{96} = [IDS^{(n+1)}]_{96} \oplus [C^{(n+1)}]_{96} \oplus [C^{(n)}]_{96} \oplus \oplus [D^{(n)}]_{96} \oplus [K_1^{(n)}]_{96}$$

Unknown: the 96th bit of K_2, K_3, ID, n_2

Known: the 96th bit of n_1, $n_2^{(n+1)}$, K_1, K_4

$A = IDS \oplus K_1 \oplus n_1$

$B = (IDS \vee K_2) + n_1$

$C = IDS + K_3 + n_2$

$D = (IDS + ID) \oplus n_1 \oplus n_2$

The least significant bits: $K_2^{(n)}$

$$[IDS^{(n+2)}]_{96} = [IDS^{(n+1)}]_{96} \oplus [n_2^{(n+1)}]_{96} \oplus$$
$$\oplus [K_4^{(n+1)}]_{96} \oplus [ID]_{96} =$$
$$= [IDS^{(n+1)}]_{96} \oplus [n_2^{(n+1)}]_{96} \oplus [K_4^{(n)}]_{96} \oplus [n_1^{(n)}]_{96} \oplus$$
$$[K_2^{(n)}]_{96}$$

$$[K_2^{(n)}]_{96} = [IDS^{(n+2)}]_{96} \oplus [IDS^{(n+1)}]_{96} \oplus [n_2^{(n+1)}]_{96} \oplus$$
$$\oplus [K_4^{(n)}]_{96} \oplus [n_1^{(n)}]_{96}$$

Unknown: the 96th bit of K_3, ID, n_2

Known: the 96th bit of n_1, $n_2^{(n+1)}$, K_1, K_2, K_4

$A = IDS \oplus K_1 \oplus n_1$
$B = (IDS \vee K_2) + n_1$
$C = IDS + K_3 + n_2$
$D = (IDS + ID) \oplus n_1 \oplus n_2$

The least significant bits: $n_1^{(n+1)}$, ID

$$[B^{(n+1)}]_{96} = ([IDS^{(n+1)}]_{96} \vee ([K_2^{(n)}]_{96} \oplus [n_2^{(n)}]_{96} \oplus [K_4^{(n)}]_{96} \oplus \oplus [ID]_{96})) \oplus [n_1^{(n+1)}]_{96}$$

$$[D^{(n)}]_{96} = [IDS^{(n)}]_{96} \oplus [ID]_{96} \oplus [n_1^{(n)}]_{96} \oplus [n_2^{(n)}]_{96}$$

$$[n_1^{(n+1)}]_{96} = [B^{(n+1)}]_{96} \oplus ([IDS^{(n+1)}]_{96} \vee ([K_2^{(n)}]_{96} \oplus [K_4^{(n)}]_{96} \oplus [D^{(n)}]_{96} \oplus [n_1^{(n)}]_{96}))$$

$$[D^{(n+1)}]_{96} = [IDS^{(n+1)}]_{96} \oplus [ID]_{96} \oplus [n_1^{(n+1)}]_{96} \oplus [n_2^{(n+1)}]_{96}$$

$$[ID]_{96} = [IDS^{(n+1)}]_{96} \oplus [D^{(n+1)}]_{96} \oplus [n_1^{(n+1)}]_{96} \oplus [n_2^{(n+1)}]_{96}$$

Unknown: the 96th bit of K_3, n_2

Known: the 96th bit of n_1, $n_1^{(n+1)}$, $n_2^{(n+1)}$, K_1, K_2, K_4, ID

$A = IDS \oplus K_1 \oplus n_1$

$B = (IDS \vee K_2) + n_1$

$C = IDS + K_3 + n_2$

$D = (IDS + ID) \oplus n_1 \oplus n_2$

The least significant bits: n_2, K_3

$$[D^{(n)}]_{96} = [IDS^{(n)}]_{96} \oplus [ID]_{96} \oplus [n_1^{(n)}]_{96} \oplus [n_2^{(n)}]_{96}$$

$$[n_2^{(n)}]_{96} = [IDS^{(n)}]_{96} \oplus [ID]_{96} \oplus [n_1^{(n)}]_{96} \oplus [D^{(n)}]_{96}$$

$$[C^{(n)}]_{96} = [IDS^{(n)}]_{96} \oplus [K_3^{(n)}]_{96} \oplus [n_2^{(n)}]_{96}$$

$$[K_3^{(n)}]_{96} = [IDS^{(n)}]_{96} \oplus [C^{(n)}]_{96} \oplus [n_2^{(n)}]_{96}$$

Now we know the least significant bit of every key and secret!

$A = IDS \oplus K_1 \oplus n_1$
$B = (IDS \vee K_2) + n_1$
$C = IDS + K_3 + n_2$
$D = (IDS + ID) \oplus n_1 \oplus n_2$

The 95th bits

$$[A^{(n)}]_{95} = [IDS^{(n)}]_{95} \oplus [K_1^{(n)}]_{95} \oplus [n_1^{(n)}]_{95}$$

$$[B^{(n)}]_{95} = ([IDS^{(n)}]_{95} \vee [K_2^{(n)}]_{95}) \oplus [n_1^{(n)}]_{95} \oplus$$
$$\oplus (([IDS^{(n)}]_{96} \vee [K_2^{(n)}]_{96}) \vee [n_1^{(n)}]_{96})$$

$$[C^{(n)}]_{95} = [IDS^{(n)}]_{95} \oplus [K_3^{(n)}]_{95} \oplus [n_2^{(n)}]_{95} \oplus$$
$$\oplus ([K_3^{(n)}]_{96} \vee [n_2^{(n)}]_{96})$$

$$[D^{(n)}]_{95} = [IDS^{(n)}]_{95} \oplus [ID]_{95} \oplus ([IDS^{(n)}]_{96} \vee [ID]_{96}) \oplus$$
$$\oplus [n_1^{(n)}]_{95} \oplus [n_2^{(n)}]_{95}$$

$A = IDS \oplus K_1 \oplus n_1$
$B = (IDS \vee K_2) + n_1$
$C = IDS + K_3 + n_2$
$D = (IDS + ID) \oplus n_1 \oplus n_2$

Computing all the bits

- If $[IDS^{(n)}]_{95} = 1$, then the problem is equivalent with that of least significant bits.
- If $[IDS^{(n)}]_{95} = 0$, then we have to wait for a later round where the 95^{th} bit of the IDS is 1.
- After this we will compute the 95^{th} bits in round *n* as well.
- After the 95^{th} bits we compute the 94^{th} bits and so on. (We use the same few rounds of authentication!)

$A = IDS \oplus K_1 \oplus n_1$
$B = (IDS \vee K_2) + n_1$
$C = IDS + K_3 + n_2$
$D = (IDS + ID) \oplus n_1 \oplus n_2$

Waiting for the bit 1 in the IDS

$P([IDS^{(n)}]_k = 1) = ½$

$P([IDS^{(n)}]_k = 1 \mid [IDS^{(n-1)}]_k = 0) =$

$P([IDS^{(n)}]_k = 1 \mid [IDS^{(n-1)}]_k = 1) = ½$

$IDS^{(n+1)} = (IDS^{(n)} + (n_2^{(n)} \oplus K_4^{(n)})) \oplus ID$

random

→ If $[IDS^{(n)}]_{95} = 0$, then in a later round it must be 1

Computing the bits in round n knowing the bits in round n+1

If $[IDS^{(n)}]_{95} = 0$ and $[IDS^{(n+1)}]_{95} = 1$

$[A^{(n)}]_{95} = [K_1^{(n)}]_{95} \oplus [n_1^{(n)}]_{95}$

$[B^{(n)}]_{95} = [K_2^{(n)}]_{95} \oplus [n_1^{(n)}]_{95} \oplus$

$\oplus ((([IDS^{(n)}]_{96} \vee [K_2^{(n)}]_{96}) \vee [n_1^{(n)}]_{96})$

$[C^{(n)}]_{95} = [K_3^{(n)}]_{95} \oplus [n_2^{(n)}]_{95} \oplus ([K_3^{(n)}]_{96} \vee [n_2^{(n)}]_{96})$

$[D^{(n)}]_{95} = [ID^{(n)}]_{95} \oplus ([IDS^{(n)}]_{96} \vee [ID^{(n)}]_{96}) \oplus [n_1^{(n)}]_{95} \oplus$

$\oplus [n_2^{(n)}]_{95}$

$A = IDS \oplus K_1 \oplus n_1$

$B = (IDS \vee K_2) + n_1$

$C = IDS + K_3 + n_2$

$D = (IDS + ID) \oplus n_1 \oplus n_2$

Computing the bits in round n knowing the bits in round n+1

$$[K_1^{(n+1)}]_{95} = [K_1^{(n)}]_{95} \oplus [n_2^{(n)}]_{95} \oplus [K_3^{(n)}]_{95} \oplus [ID]_{95} \oplus \oplus ([K_3^{(n)}]_{96} \vee [ID]_{96})$$

$$[C^{(n)}]_{95} = [K_3^{(n)}]_{95} \oplus [n_2^{(n)}]_{95} \oplus ([K_3^{(n)}]_{96} \vee [n_2^{(n)}]_{96})$$

$$[K_1^{(n)}]_{95} = [K_1^{(n+1)}]_{95} \oplus [ID]_{95} \oplus ([K_3^{(n)}]_{96} \vee [ID]_{96}) \oplus [C^{(n)}]_{95} \oplus \oplus ([K_3^{(n)}]_{96} \vee [n_2^{(n)}]_{96})$$

$$[A^{(n)}]_{95} = [K_1^{(n)}]_{95} \oplus [n_1^{(n)}]_{95}$$

$$[n_1^{(n)}]_{95} = [A^{(n)}]_{95} \oplus [K_1^{(n)}]_{95}$$

$A = IDS \oplus K_1 \oplus n_1$
$B = (IDS \vee K_2) + n_1$
$C = IDS + K_3 + n_2$
$D = (IDS + ID) \oplus n_1 \oplus n_2$

Computing the bits in round n knowing the bits in round n+1

$$[B^{(n)}]_{95} = [K_2^{(n)}]_{95} \oplus [n_1^{(n)}]_{95} \oplus \oplus (([IDS^{(n)}]_{96} \vee [K_2^{(n)}]_{96}) \vee [n_1^{(n)}]_{96})$$

$$[K_2^{(n)}]_{95} = [B^{(n)}]_{95} \oplus [n_1^{(n)}]_{95} \oplus \oplus (([IDS^{(n)}]_{96} \vee [K_2^{(n)}]_{96}) \vee [n_1^{(n)}]_{96})$$

$$[D^{(n)}]_{95} = [ID^{(n)}]_{95} \oplus ([IDS^{(n)}]_{96} \vee [ID^{(n)}]_{96}) \oplus [n_1^{(n)}]_{95} \oplus [n_2^{(n)}]_{95}$$

$$[n_2^{(n)}]_{95} = [D^{(n)}]_{95} \oplus [ID^{(n)}]_{95} \oplus ([IDS^{(n)}]_{96} \vee [ID^{(n)}]_{96}) \oplus [n_1^{(n)}]_{95}$$

$A = IDS \oplus K_1 \oplus n_1$
$B = (IDS \vee K_2) + n_1$
$C = IDS + K_3 + n_2$
$D = (IDS + ID) \oplus n_1 \oplus n_2$

Computing the bits in round n knowing the bits in round n+1

$$[C^{(n)}]_{95} = [K_3^{(n)}]_{95} \oplus [n_2^{(n)}]_{95} \oplus ([K_3^{(n)}]_{96} \vee [n_2^{(n)}]_{96})$$

$$[K_3^{(n)}]_{95} = [C^{(n)}]_{95} \oplus [n_2^{(n)}]_{95} \oplus ([K_3^{(n)}]_{96} \vee [n_2^{(n)}]_{96})$$

$$[IDS^{(n+1)}]_{95} = [n_2^{(n)}]_{95} \oplus [K_4^{(n)}]_{95} \oplus [ID]_{95}$$

$$[K4^{(n)}]_{95} = [IDS^{(n+1)}]_{95} \oplus [n_2^{(n)}]_{95} \oplus [ID]_{95}$$

$A = IDS \oplus K_1 \oplus n_1$
$B = (IDS \vee K_2) + n_1$
$C = IDS + K_3 + n_2$
$D = (IDS + ID) \oplus n_1 \oplus n_2$

The needed rounds

- We need r +2 rounds so that for every k =1, 2, …, 96

  $[IDS^{(n)}]_k \vee [IDS^{(n+1)}]_k \vee [IDS^{(n+2)}]_k \vee \ldots \vee [IDS^{(n+r-1)}]_k = 1$
- The expected number of r is about 7.93
- Expected number of the needed rounds: about 9.93

Distribution of r :

t	1	2	3	4	5	6	7
P(r =t)	$<10^{-29}$	$<10^{-11}$	$<10^{-5}$	$<10^{-2}$	0.05	0.17	0.25

t	8	9	10	11	12	13	14
P(r =t)	0.22	0.14	0.08	0.04	0.02	0.01	$<10^{-2}$

Conclusion

The attack is really effective:

- We have given an algorithm to break LMAP with a passive attack
- The probability that 15 consecutive rounds are enough is about 0.98
- The expected value is less than 10

Thank You for Your attention!

Partners & sponsors: