Mind your nonces: cryptanalysis of a privacy-preserving distance bounding protocol

J.-P. Aumasson[1] **A. Mitrokotsa**[2] P. Peris-Lopez[2]

[1]Nagravision SA, Switzerland

[2]EPFL, Switzerland

[3]TU Delft, Netherlands

9th International Conference on
Applied Cryptography & Network Security (ACNS 2011)
7 June 2011,
Nerja, Malaga, Spain

Outline

- Motivation
- Distance Bounding Protocols
- The Rasmussen - Čapkun (RČ) protocol
- Attack against the RČ protocol

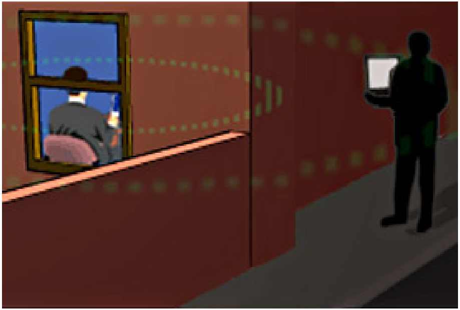
ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Motivation

Guarantees about the geographical location of a communicating device.

Secure Location Information

- Necessary in battlefield ad hoc networks
- Access Control Systems
- Satellite DTV conditional access systems
- Prevent location spoofing
- ...

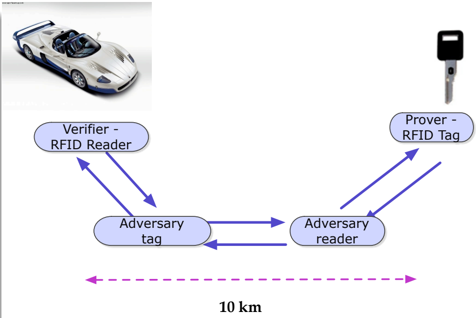


ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Relay attacks

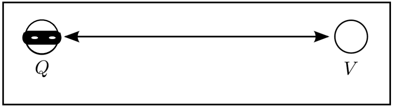
Relay attack

- Communication **Range**:
  a few **cm** or **dm** or even meters for RFID tags.
- Signal amplification⇒ increase this distance.
- Man-in-the-middle attack.
- The attacker relays messages from an authentic tag to a legitimate reader.



Relay Attacks

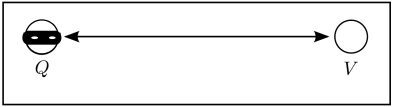
a) **Distance Fraud**
The attack is executed by a malicious prover Q. The goal is to shorten the distance measured by the verifier V.



Relay Attacks

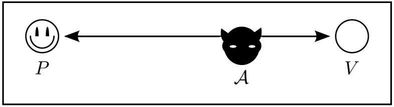
a) **Distance Fraud**

The attack is executed by a malicious prover Q. The goal is to shorten the distance measured by the verifier V.



b) **Mafia Fraud**

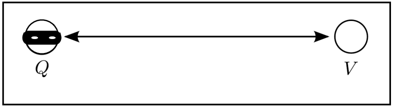
The attack is executed by an external attacker A. The goal is to shorten the distance between an honest prover P and a verifier V.



Relay Attacks

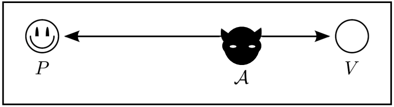
a) **Distance Fraud**

The attack is executed by a malicious prover Q. The goal is to shorten the distance measured by the verifier V.



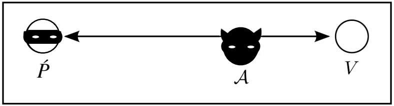
b) **Mafia Fraud**

The attack is executed by an external attacker A. The goal is to shorten the distance between an honest prover P and a verifier V.



c) **Terrorist Fraud**

The attack is executed by a malicious prover A, colluding with a legitimate but dishonest prover P'. The goal is for P' to shorten his distance to the verifier V.

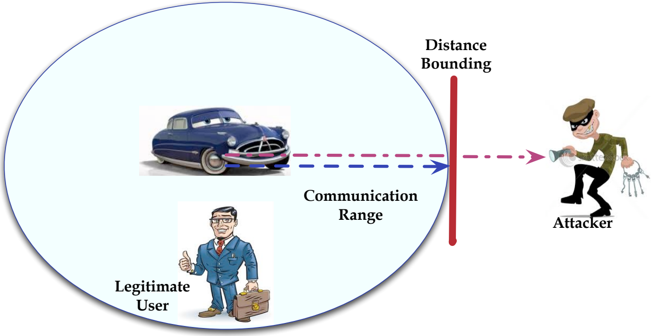


ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Distance Bounding Protocols

Countermeasure against relay attacks

- **Distance bounding** protocols: challenge-response authentication protocols.
- Enable a verifier (V) device to establish an upper bound on the physical distance to an untrusted prover device (P).
- Usually based on the response time of the prover (P) to estimate the distance.

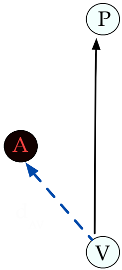


Distance Bounding Protocols

Prover P		**Verifier** V
shared key K		shared key K
	Initialization phase	
select a random N_P	$\xrightarrow{\text{commit}(N_P)}$	
	Rapid bit exchange	
		$c_1, \ldots, c_j \xleftarrow{\$} \{0,1\}$
	$\xleftarrow{c_1}$	
$r_1 \leftarrow f_{1,K}(c_1)$	$\xrightarrow{r_1}$	
$\ldots$	$\ldots$	$\ldots$
	$\xleftarrow{c_j}$	
$r_j \leftarrow f_{j,K}(c_j)$	$\xrightarrow{r_j}$	
		verify responses

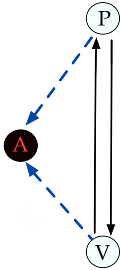
Information Leakage in DB Protocols

Information leaks though the measurement of messages' arrival times.



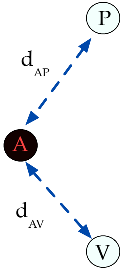
Information Leakage in DB Protocols

Information leaks though the measurement of messages' arrival times.



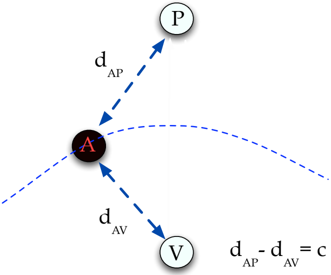
Information Leakage in DB Protocols

Information leaks though the measurement of messages' arrival times.



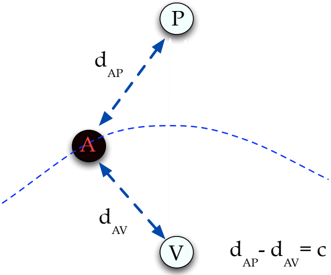
Information Leakage in DB Protocols

Information leaks though the measurement of messages' arrival times.



Information Leakage in DB Protocols

Information leaks though the measurement of messages' arrival times.



- Rasmussen & Čapkun have noted that DB protocols leak information about the distance and location of the *prover* and the *verifier*
- They proposed a *privacy - preserving* DB protocol.

The Rasmussen - Čapkun protocol

- P and V communicate over an insecure channel.
- When the protocol succeeds V is able to calculate an upper bound on the physical distance to P.
- Privacy preservation by hiding the RBE within a longer **uninterrupted stream** of bits.

The Rasmussen - Čapkun protocol

Notation

P and V share the knowledge of :

- A k-bit encryption key K_1.
- A k-bit authentication key K_2.
- A symmetric encryption scheme (Enc, Dec).
- A symmetric authentication scheme ($Sign$, $Verif$) i.e. a MAC.
- A pseudorandom generator connected to a source of physical entropy.
- A timestamp counter
- The bit length of N_P and N_V: n.
- The bit length of the *hidden marker* M: m

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

The Rasmussen - Čapkun protocol

Prover P		**Verifier** V
shared keys K_1, K_2		shared keys K_1, K_2
	Initialization phase	
$N_P \xleftarrow{\$} \{0,1\}^n$ $c_1 \leftarrow \mathsf{Enc}_{K_1}(N_P)$ $t_1 \leftarrow \mathsf{Sign}_{K_2}(N_P)$	$\xrightarrow{c_1 \,\Vert\, t_1}$	$c_1' \,\Vert\, t_1'$
		$N_P' \leftarrow \mathsf{Dec}_{K_1}(c_1')$ if $\mathsf{Verif}_{K_2}(N_P', t_1') = \mathsf{error}$ then return error $M \xleftarrow{\$} \{0,1\}^m$
$c_2' \,\Vert\, t_2'$	$\xleftarrow{c_2 \,\Vert\, t_2}$	$c_2 \leftarrow \mathsf{Enc}_{K_1}(M \Vert N_P')$ $t_2 \leftarrow \mathsf{Sign}_{K_2}(M \Vert N_P')$
$M' \Vert N_P'' \leftarrow \mathsf{Dec}_{K_1}(c_2')$ if $N_P'' \neq N_P$ or $\mathsf{Verif}_{K_2}(M' \Vert N_P'', t_2') = \mathsf{error}$ then return error		$N_V \xleftarrow{\$} \{0,1\}^n$

The Rasmussen - Čapkun protocol

Prover P		**Verifier** V
shared keys K_1, K_2		shared keys K_1, K_2
	Distance bounding phase	
monitor traffic for detecting M	$\xleftarrow{\mathrm{Rand}_V()}$	bit-stream without M as a substring
	$\xrightarrow{\mathrm{Rand}_V() \oplus \mathrm{Rand}_P()}$	
	$\xleftarrow{M \parallel N_V}$	
when M is detected		
	$\xrightarrow{M \oplus \mathrm{Rand}_P() \parallel N_V \oplus N_P}$	
	$\xleftarrow{\mathrm{Rand}_V()}$	
	$\xrightarrow{\mathrm{Rand}_V() \oplus \mathrm{Rand}_P()}$	
stop after a random delay		stop after a random delay

The Rasmussen - Čapkun protocol

- During the *RBE* the bit streams between V and P are transmitted continuously on two different communication channels.
- By the **end of the** *RBE*
  V counts the **# of bits** received between:
  - the time he transmitted the first bit of N_V and
  - the time he received the first bit of $N_V \oplus N_P$.
- Given the bit rate and the processing delay,
  V can calculate the round trip time
  $\Rightarrow$ an **upper bound** on the distance to P.

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Attack against the RČ protocol

- A **passive** attack that recovers N_P, N_V and M for two sessions of the RČ protocol.
- An attacker is able to deduce information on the relative distance of P and V during each of those sessions.
- The distance between P and V does **not** need to be the same at each session.
- **How?** $\Rightarrow$ with repeated occurrences of the same N_P in two distinct sessions we can recover the ephemeral secrets of those sessions.

Attack against the RČ protocol

The attacker observes many sessions between P and V and:

Step 1: For each session observed:

- Record the two data streams exchanged after the c_2 is sent.
- Store the c_1's in a dynamically sorted table.
- When a c_1 value is repeated twice:
  - stop recording sessions,
  - delete the sessions where the repetitions do not occur.

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Attack against the RČ protocol

Step 2: For each of the two sessions with the same N_P, do:

- divide the V-to-P stream into n-bit windows VP_0, VP_1, ...
- divide the P-to-V stream into n-bit windows PV_0, PV_1, ...
- construct and sort a table containing all $VP_i \oplus PV_j$ values where $0 < i < j$.

Create two tables T_1 and T_2 one for each session using the same N_P.

Each table will contain an element equal to N_P.

Indeed the XOR between VP_i's and PV_i's will cancel the value of each N_V.

$(N_V \oplus (N_V \oplus N_P) = N_P)$.

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Attack against the RČ protocol

Step 3: Search for a collision between an element of T_1 and an element of T_2. If a unique collision is found then the value is N_P.

Step 4: Given $N_P \Rightarrow$ identify M and N_V in the bit-streams of each session.

Count the number of bits between the reception of N_V from the V and the reception of P's response

$\Rightarrow$ to **deduce** information on the relative **positions** of P and V.

Complexity analysis

- $\ell \rightarrow$ the least number of bits sent by either P or V during the distance bounding phase.

Memory required before detecting a collision

- N_P is n-bit long
- N_P will be repeated after approximately $2^{n/2}$

$\Rightarrow$ One needs to record $2 \cdot \ell \cdot 2^{n/2}$

Memory to store the tables

- $W = \ell - n + 1$, distinct windows of n-bits in the V-to-P stream.
- i-th window is XORed with $W - i - 1$, n-bit windows of the P-to-V stream. Thus, in total there are:

$$N = \sum_{i=1}^{W} (W - 1 - i) = \frac{W^2 - 3W}{2}$$

entries in each table.

Efficiency for typical parameters

- Communication channel of bit rate $1 Gbps$.
- Hidden marker M with length $m = 160$ bits.
- Distance bounding phase lasts 500 milliseconds.

(n, ℓ)	sessions monitored	memory required	tables size (N)	sorting time	number of collisions
$(32, 2^{10})$	2^{16}	2^{27}	2^{19}	2^{11}	2^{6}
$(32, 2^{20})$	2^{16}	2^{37}	2^{39}	2^{21}	2^{45}
$(64, 2^{10})$	2^{32}	2^{43}	2^{19}	2^{10}	1
$(64, 2^{20})$	2^{32}	2^{53}	2^{39}	2^{21}	2^{14}
$(64, 2^{30})$	2^{32}	2^{63}	2^{59}	2^{31}	2^{53}
$(128, 2^{10})$	2^{64}	2^{75}	2^{19}	2^{11}	1
$(128, 2^{20})$	2^{64}	2^{85}	2^{39}	2^{21}	1
$(128, 2^{30})$	2^{64}	2^{95}	2^{59}	2^{31}	1

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Strengthening the RČ protocol

- Probabilistic encryption: this way repetitions of N_P cannot be detected.
- Better nonces: unique N_P nonces should be used
  for example by using Bloom filters (to save memory)
- Encrypt-then-sign: instead of encrypt and sign
- Distinct keys: for authentication and encryption

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

Conclusions

- Security analysis of the Rasmussen - Čapkun (RČ) protocol.
- Presented an attack that exploits nonce collisions.
- Proposed modifications of the protocol to thwart the attack.

Thank you for your attention!