

# Distance Bounding Protocols: Challenges and Directions

Katerina Mitrokotsa

12<sup>th</sup> of November 2013,  
Department of Computer Science and Engineering  
Chalmers University of Technology  
Sweden

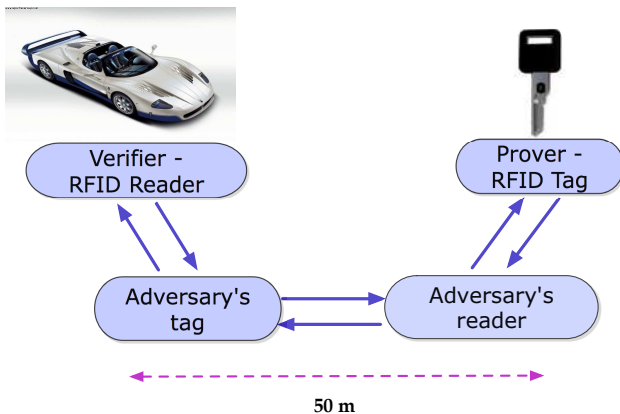


**CHALMERS**  
UNIVERSITY OF TECHNOLOGY

# Motivation

## Relay attack

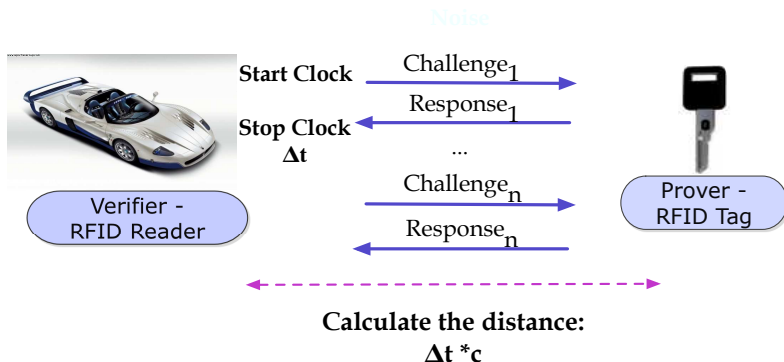
- Communication **Range**: a few **cm** or **dm** (for LH, HF) or a few **meters** (for UHF)
- **Man-in-the-middle** attacker: **increases** this distance, **relays** messages



# Distance Bounding Protocols

## Countermeasure against relay attacks

- **Distance bounding** protocols: challenge-response authentication protocols.
- The verifier (V) can **upper bound** the distance to an **untrusted** prover P.
- Based on **response time** of the prover to **estimate the distance**
- **Simple** calculations required for cheap devices.

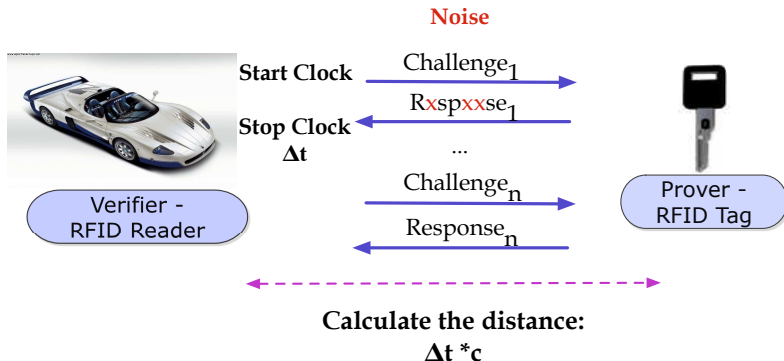


# Distance Bounding Protocols

## Countermeasure against relay attacks

- **Distance bounding** protocols: challenge-response authentication protocols.
- The verifier (V) can **upper bound** the distance to an **untrusted** prover P.
- Based on **response time** of the prover to **estimate the distance**
- **Simple** calculations required for cheap devices.

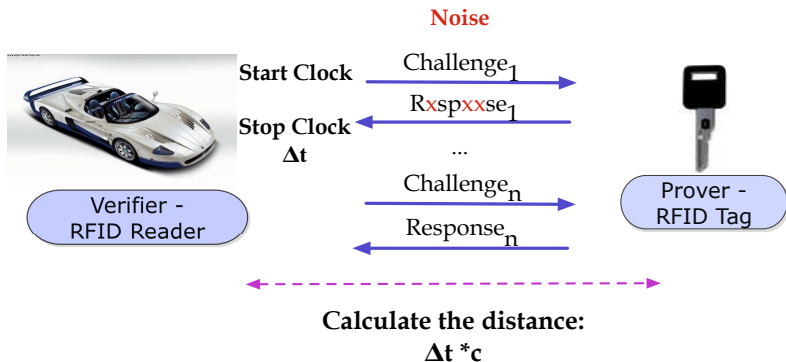
**Problem:** **noise** increases the probability of error.



# Distance Bounding Protocols

## Goals

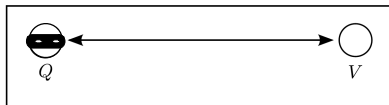
- **Minimise** the **resource cost**:  
Longer Protocols  $\rightarrow$  **higher accuracy** but also **higher resource** use.
- **Maximise/Minimise** the probability of authenticating a **legitimate user/attacker**.



# Relay Attacks

## a) Distance Fraud

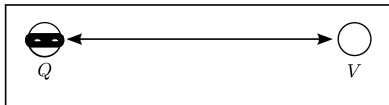
The attack is executed by a malicious prover  $Q$ . The goal is to shorten the distance measured by the verifier  $V$ .



# Relay Attacks

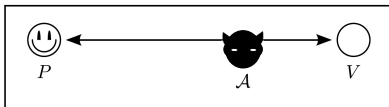
## a) Distance Fraud

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



## b) Mafia Fraud

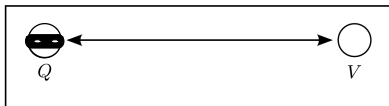
The attack is executed by an external attacker  $A$ . The goal is to shorten the distance between an honest prover  $P$  and a verifier  $V$ .



# Relay Attacks

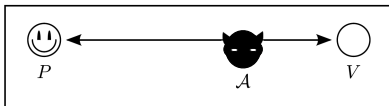
## a) Distance Fraud

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



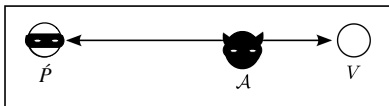
## b) Mafia Fraud

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



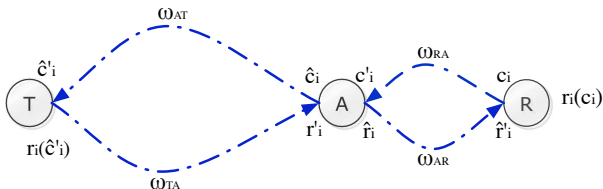
## c) Terrorist Fraud

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  $V$ .





## Distance Bounding Protocols: Mafia Fraud attack



## Notation:

A: attacker, R: reader, T : Tag.

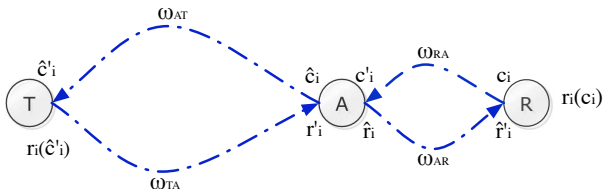
$c \rightarrow$  **challenge**,  $r \rightarrow$  **response**.

$x$ : a message **transmitted**  $\rightarrow x'$  is the message **received** (due to errors, noise).

$\hat{x}$ : attacker's **guesses** for possible values of message  $x$  (challenge or response).

$\omega_{BC}$  : **noise** between the transmission channel of B and C.

## Distance Bounding Protocols: Mafia Fraud attack



A similar **attack** has been launched against the **Dutch transport system** (OV-chipkaart) in 2008.

## Notation:

$A$ : attacker,  $R$ : reader,  $T$ : Tag.

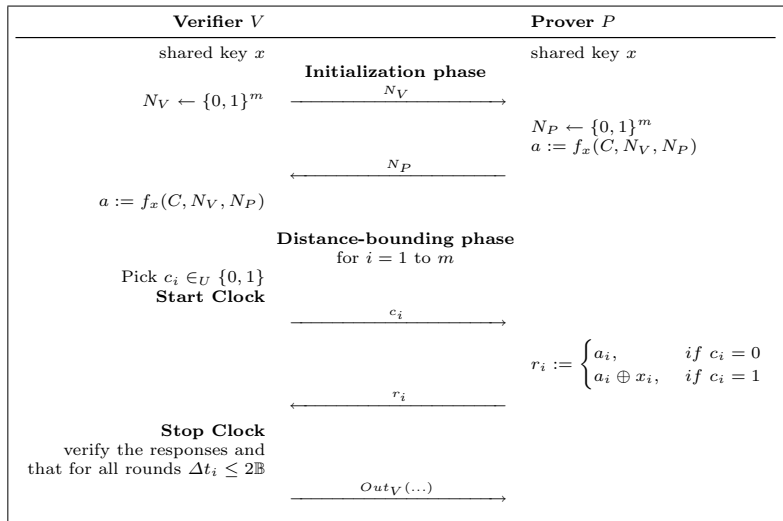
$c \rightarrow$  **challenge**,  $r \rightarrow$  **response**.

$x$ : a message **transmitted**  $\rightarrow x'$  is the message **received** (due to errors, noise).

$\hat{x}$ : attacker's **guesses** for possible values of message  $x$  (challenge or response).

$\omega_{BC}$ : **noise** between the transmission channel of  $B$  and  $C$ .

## General Structure of DB protocols



# Distance bounding protocols

## Problem

- The **noise** necessitates the use of a **tolerance threshold**  $\tau$
- How do you choose the **threshold**?
- How do you choose the **number of rounds**?
- We propose an **expected loss** framework for characterising and deriving optimal solutions.

C. Dimitrakakis, A. Mitrokotsa, S. Vaudenay, "Expected loss analysis of thresholded authentication protocols in noisy conditions", INFOCOM'12

# Distance bounding protocols

## Problem

- The **noise** necessitates the use of a **tolerance threshold**  $\tau$
- How do you choose the **threshold**?
- How do you choose the **number of rounds**?
- We propose an **expected loss** framework for characterising and deriving optimal solutions.

Similar problem with CAPTCHA authentication.

# Overview of our proposal

## Constrained channel authentication

- **Challenge-response phase:** lasting  $n$  rounds with no error correction.
- **Success:** iff the response is  $\tau$ -close to the correct response, with  $\tau$  a tolerance threshold  $\tau$ .
- **Losses:** Trade off false acceptance, false rejection and communication cost.

## Standard cryptographic authentication

- **Challenge-response phase:** lasting  $n$  rounds assuming error-free channel.
- **Success:** iff the response is perfectly correct.

## Our Solution: Expected loss analysis

Integrated error analysis with cryptographic analysis.

# Overview

## Our contributions

- We propose an **expected loss model** for authentication.
- We formulate the problem as **minimising** the worst-case expected loss.
- We suggest an **algorithm** for doing so.
- We prove tight upper and lower **bounds**.
- We apply these bounds to **RFID** authentication.
- We show that our approach **strictly dominates** others in practice.

# Additive-error challenge-response authentication protocol

## Definition

- 1 Select the number of challenge-response **rounds**  $n$ .
- 2 Select a **threshold**  $\tau$ .
- 3 At the  $i$ -th round:
  - (i) The verifier sends a **challenge**  $c_i$ .
  - (ii) The prover **responds** with  $r_i$ .
  - (iii) The verifier calculates an **error**  $\varepsilon_i \in [0, 1]$ .
- 4 The verifier calculates the error function

$$\varepsilon \triangleq \sum_{i=1}^n \varepsilon_i$$

- 5 The verifier  $\mathcal{V}$  **rejects** the prover (authenticator)  $\mathcal{P}$ , if and only if  $\varepsilon \geq \tau$ .



# Expected Loss Analysis

## Loss

- $\ell_A$ : **loss** if we **authenticate** a **malicious party**  $A$  (*attacker*).
- $\ell_U$ : **loss** if we **fail to authenticate** a **valid party**  $U$  (*user*).
- $\ell_B$ : **cost** of **each round** of the challenge-response phase.

## Total loss

The **loss** when the prover  $P$  is:

$$L = \begin{cases} n\ell_B + \ell_U, & \text{if } \varepsilon \geq \tau \text{ and } \mathcal{P} = U \\ n\ell_B + \ell_A, & \text{if } \varepsilon < \tau \text{ and } \mathcal{P} = A \\ n\ell_B, & \text{otherwise.} \end{cases}$$

# Expected Loss Analysis

## Expected Loss

The *expected loss* when the communicating party is an *attacker*  $A$  or the *user*  $U$  is given by respectively:

$$\mathbb{E}(L \mid A) = n\ell_B + \Pr(\varepsilon < \tau \mid A) \cdot \ell_A + \Pr(\varepsilon \geq \tau \mid A) \cdot 0$$

$$\mathbb{E}(L \mid U) = n\ell_B + \Pr(\varepsilon < \tau \mid U) \cdot 0 + \Pr(\varepsilon \geq \tau \mid U) \cdot \ell_U.$$

# Expected Loss Analysis

## Expected Loss

The *expected loss* when the communicating party is an *attacker*  $A$  or the *user*  $U$  is given by respectively:

$$\mathbb{E}(L \mid A) = n\ell_B + \Pr(\varepsilon < \tau \mid A) \cdot \ell_A$$

$$\mathbb{E}(L \mid U) = n\ell_B + \Pr(\varepsilon \geq \tau \mid U) \cdot \ell_U.$$

# Expected Loss Analysis

## Expected Loss

The *expected loss* when the communicating party is an *attacker*  $A$  or the *user*  $U$  is given by respectively:

$$\begin{aligned}\mathbb{E}(L \mid A) &= n\ell_B + \Pr(\varepsilon < \tau \mid A) \cdot \ell_A \\ \mathbb{E}(L \mid U) &= n\ell_B + \Pr(\varepsilon \geq \tau \mid U) \cdot \ell_U.\end{aligned}$$

Our goal: minimise worst-case expected loss

The *expected loss* is in any case **bounded by** the *worst-case expected loss*:

$$\mathbb{E} L \leq \max \{ \mathbb{E}(L \mid A), \mathbb{E}(L \mid U) \}.$$

# Overview of the Analysis

- We must choose  $\tau, n$  so that **no matter** if  $\mathcal{P} = A$  or  $\mathcal{P} = U$ , the expected loss  $\mathbb{E}(L \mid \mathcal{P})$  is *as small as possible*.
- Problems:
  - as we *increase* the threshold  $\tau$ ,  $\mathbb{E}(L \mid \mathcal{P} = U)$  *decreases*, while  $\mathbb{E}(L \mid \mathcal{P} = A)$  *increases*.
  - as we *decrease* the threshold  $\tau$ ,  $\mathbb{E}(L \mid \mathcal{P} = U)$  *increases*, while  $\mathbb{E}(L \mid \mathcal{P} = A)$  *decreases*.
- Intuitively, this happens when  $\mathbb{E}(L \mid \mathcal{P} = A, \tau) \approx \mathbb{E}(L \mid \mathcal{P} = U, \tau)$ .
- First, we choose a nearly-optimal threshold  $\tau$  for a fixed rounds  $n$ .
- Then, we optimise  $n$ .

C. Dimitrakakis, A. Mitrokotsa, S. Vaudenay, Expected loss analysis analysis of thresholded authentication protocols in noisy conditions, INFOCOM 2012

# Choice of threshold

## Theorem (Expected loss for fixed $n$ )

Let  $\rho \triangleq \ell_A/\ell_U$  and select

$$\hat{\tau}_n^* \triangleq \frac{n(p_A + p_U)}{2} - \frac{\ln \rho}{4\Delta}$$

If  $np_U \leq \tau \leq np_A$ , then the expected loss  $\mathbb{E} L$  is bounded by:

$$\mathbb{E}(L \mid n, \hat{\tau}_n^*) \leq n\ell_B + \exp\left(-\frac{n}{2}\Delta^2\right) \sqrt{\ell_A\ell_U}.$$

with  $\Delta \triangleq p_A - p_U$ .

Where:

- $p_A \leq \mathbb{E}(\varepsilon_i \mid A)$ : a *lower bound* on the expected per-round error of the *attacker A*.
- $p_U \geq \mathbb{E}(\varepsilon_i \mid U)$ : an *upper bound* on the expected per-round error of a *legitimate user U*.

C. Dimitrakakis, A. Mitrokotsa, S. Vaudenay, Expected loss analysis analysis of thresholded authentication protocols in noisy conditions, INFOCOM 2012

# Choice of the number of rounds

## Theorem (Upper bound on expected loss)

Assume  $\ell_A, \ell_U, \ell_B > 0$ . If we choose  $\tau = \hat{\tau}_n^*$  and

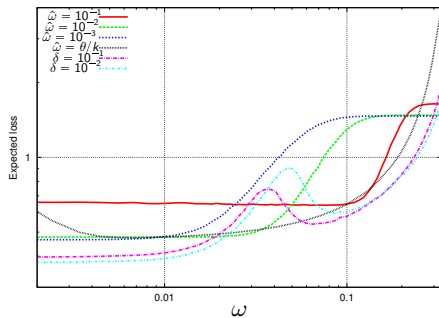
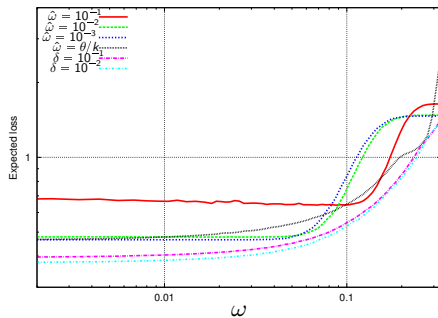
$$\hat{n}^* \triangleq \frac{\sqrt{1 + 2CK} - 1}{C},$$

where  $C = \Delta^2$  and  $K = \sqrt{\ell_A \ell_U} / \ell_B$ , then the expected loss  $\mathbb{E} L$  is bounded as:

$$\mathbb{E}(L \mid \hat{\tau}_n^*, \hat{n}^*) \leq \frac{1}{\Delta} \sqrt{8\ell_B (\ell_A \ell_U)^{1/4}}$$

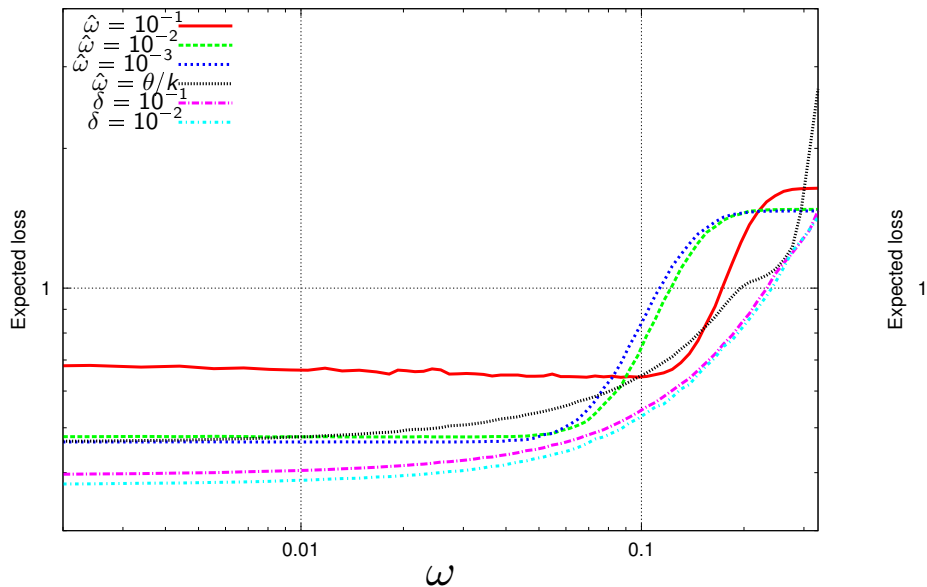
C. Dimitrakakis, A. Mitrokotsa, S. Vaudenay, Expected loss analysis analysis of thresholded authentication protocols in noisy conditions, INFOCOM 2012

# Comparison of losses

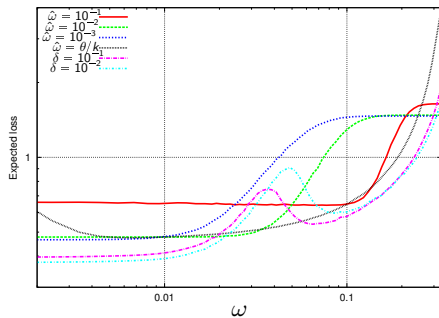
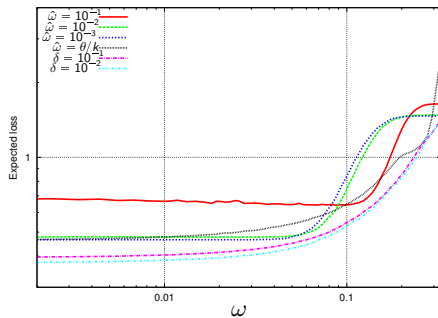




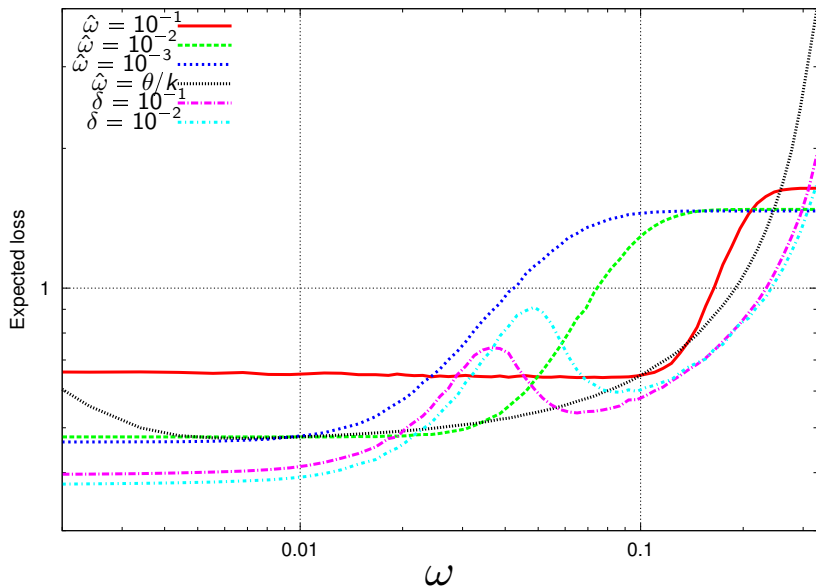
## Comparison of losses



# Comparison of losses



## Comparison of losses



# Distance bounding protocols: Contributions

- A simple (dictionary) attack successful against 4 protocols
- Leads to the full recovery of the key.
- Depends of the **length** of the nonces (random values) used to hide relationships between repeated authentication attempts.
- **Nonce repetition:** Compromise security.
- Martingale analysis of the **birthday paradox**.

## Theorem

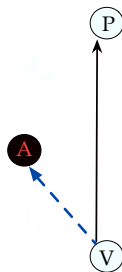
For some  $q \in [0, 1]$ , when  $d \in \mathbb{N}$  is the number of possible nonces, we can recover a key of length  $k$ , with probability at least  $1 - \delta$ ,  $\forall \delta \in [0, 1]$  after at most  $t$  sessions:

$$t = O\left(\max\left\{\ln(k), d^{2/3}\right\}\right) \quad (1)$$

# Information Leakage in DB Protocols

## Information Leakage

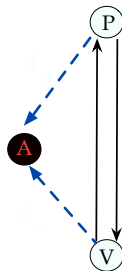
- Can we keep the location of a prover **private**?
- Information **leaks** through the measurement of messages' arrival times.



# Information Leakage in DB Protocols

## Information Leakage

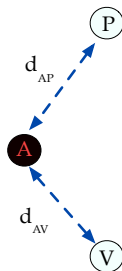
- Can we keep the location of a prover **private**?
- Information **leaks** through the measurement of messages' arrival times.



# Information Leakage in DB Protocols

## Information Leakage

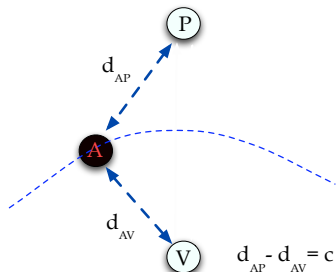
- Can we keep the location of a prover **private**?
- Information **leaks** through the measurement of messages' arrival times.



# Information Leakage in DB Protocols

## Information Leakage

- Can we keep the location of a prover **private**?
- Information **leaks** through the measurement of messages' arrival times.

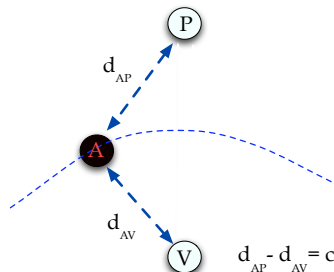




# Information Leakage in DB Protocols

## Information Leakage

- Can we keep the location of a prover **private**?
- Information **leaks** through the measurement of messages' arrival times.



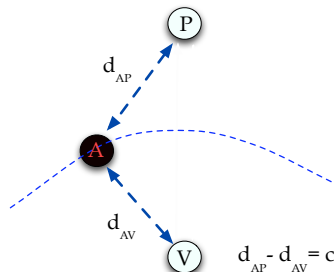
## Privacy-Preserving DB

- Rasmussen & Čapkun proposed a **privacy-preserving** DB protocol.
- We showed that their protocol is **susceptible** to multiple attacks.
- We proved: it is theoretically impossible to achieve location privacy for powerful adversaries.
- For limited adversaries, carefully chosen parameters allow **computationally provable secure** location privacy.
- Proposed a new privacy-preserving DB protocol.

# Information Leakage in DB Protocols

## Information Leakage

- Can we keep the location of a prover **private**?
- Information **leaks** through the measurement of messages' arrival times.



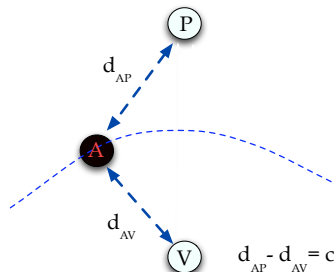
## Privacy-Preserving DB

- Rasmussen & Čapkun proposed a **privacy-preserving** DB protocol.
- We showed that their protocol is **susceptible** to multiple attacks.
- We proved: it is theoretically impossible to achieve location privacy for powerful adversaries.
- For limited adversaries, carefully chosen parameters allow **computationally provable secure** location privacy.
- Proposed a new privacy-preserving DB protocol.

# Information Leakage in DB Protocols

## Information Leakage

- Can we keep the location of a prover **private**?
- Information **leaks** through the measurement of messages' arrival times.



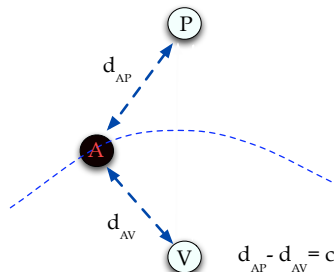
## Privacy-Preserving DB

- Rasmussen & Čapkun proposed a **privacy-preserving** DB protocol.
- We showed that their protocol is **susceptible** to multiple attacks.
- We proved: it is **theoretically impossible** to achieve location privacy for powerful adversaries.
- For limited adversaries, carefully chosen parameters allow **computationally provable secure** location privacy.
- Proposed a new privacy-preserving DB protocol.

# Information Leakage in DB Protocols

## Information Leakage

- Can we keep the location of a prover **private**?
- Information **leaks** through the measurement of messages' arrival times.



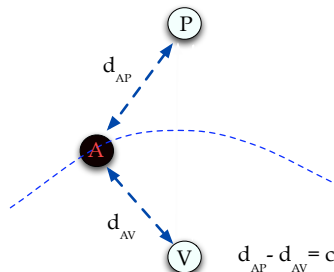
## Privacy-Preserving DB

- Rasmussen & Čapkun proposed a **privacy-preserving** DB protocol.
- We showed that their protocol is **susceptible** to multiple attacks.
- We proved: it is **theoretically impossible** to achieve location privacy for powerful adversaries.
- For limited adversaries, carefully chosen parameters allow **computationally provable secure** location privacy.
- Proposed a new privacy-preserving DB protocol.

# Information Leakage in DB Protocols

## Information Leakage

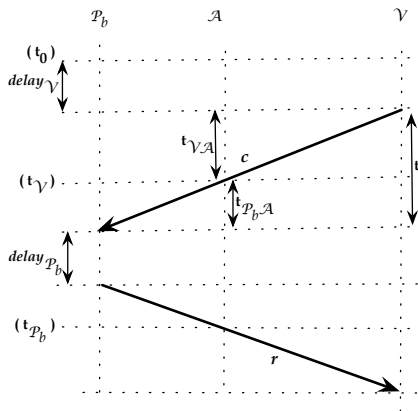
- Can we keep the location of a prover **private**?
- Information **leaks** through the measurement of messages' arrival times.



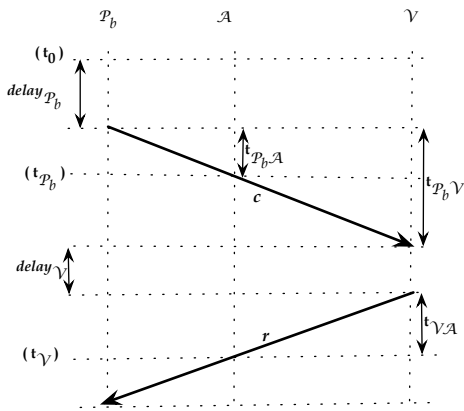
## Privacy-Preserving DB

- Rasmussen & Čapkun proposed a **privacy-preserving** DB protocol.
- We showed that their protocol is **susceptible** to multiple attacks.
- We proved: it is **theoretically impossible** to achieve location privacy for powerful adversaries.
- For limited adversaries, carefully chosen parameters allow **computationally provable secure** location privacy.
- Proposed a new privacy-preserving DB protocol.

## Location Privacy - preview



Case 1



Case 2

## Lemma

If  $d_b$  follows the uniform distribution in the range  $[0, B]$  and denotes the pdf of the  $\text{delay}_{P_b}$  while  $\text{delay}_V$  is always equal to 0 then the best distinguisher based on  $t_P - t_V$  and the locations satisfies:

$$\text{Adv}_A = \frac{2t_{\max}}{B}$$

# Terrorist Fraud Attacks Need for stronger encryption

Distance-Bounding for RFID: Effectiveness of “Terrorist Fraud” in the Presence of Bit Errors [Hancke IEEE RFID-TA 2012]

## Terrorist Fraud & Bit errors

- The malicious prover  $\mathcal{P}'$  helps the adversary  $\mathcal{A}$  in the initialisation phase.
- $\mathcal{P}'$  provides the answers  $r'_i$  required with  $\tau$  of them flipped.
- $\mathcal{A}$  answers in the [distance-bounding](#) phase using these  $r'_i$ s.
- Since there are  $n - \tau$  correct responses  $\mathcal{A}$  is authenticated by  $\mathcal{V}$
- $\mathcal{A}$  cannot reconstruct the key  $x$  based on the noisy responses  $r'_i$

# Distance-bounding protocols: Contributions

## Contributions

- **Analysed the security of existing distance-bounding protocols** [Mitrokotsa, Dimitrakakis, Peris-Lopez, IEEE Com. Let. 2010], [Mitrokotsa, Peris-Lopez, Dimitrakakis, Vaudenay Computer Journal 2013].
- Described attacks that can be launched against [Bay, Boureanu, Mitrokotsa, Spulber, Vaudenay, INSCRYPT2012] [Boureanu, Mitrokotsa, Vaudenay, LATINCRYPT 2012]
- Proposed new protocols that do not suffer of identified vulnerabilities [Boureanu, Mitrokotsa, Vaudenay, LIGHTSEC 2013].
- Formalised & analysed distance-bounding protocols in the context of provable security, something that has not been done before [Boureanu, Mitrokotsa, Vaudenay, Lightsec 2013].



# Distance-bounding protocols: Contributions

## Contributions

- **Analysed the security of existing distance-bounding protocols** [Mitrokotsa, Dimitrakakis, Peris-Lopez, IEEE Com. Let. 2010], [Mitrokotsa, Peris-Lopez, Dimitrakakis, Vaudenay Computer Journal 2013].
- **Described attacks that can be launched against** [Bay, Boureanu, Mitrokotsa, Spulber, Vaudenay, Inscrypt 2012] [Boureanu, Mitrokotsa, Vaudenay LATINCRYPT 2012]
- Proposed new protocols that do not suffer of identified vulnerabilities [Boureanu, Mitrokotsa, Vaudenay, LIGHTSEC 2013].
- Formalised & analysed distance-bounding protocols in the context of provable security, something that has not been done before [Boureanu, Mitrokotsa, Vaudenay, Lightsec 2013].

# Distance-bounding protocols: Contributions

## Contributions

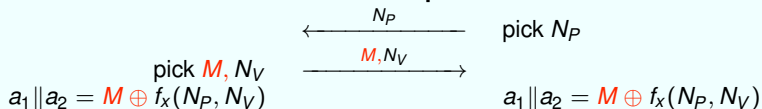
- **Analysed the security of existing distance-bounding protocols** [Mitrokotsa, Dimitrakakis, Peris-Lopez, IEEE Com. Let. 2010], [Mitrokotsa, Peris-Lopez, Dimitrakakis, Vaudenay Computer Journal 2013].
- **Described attacks that can be launched against** [Bay, Boureanu, Mitrokotsa, Spulber, Vaudenay, Inscrypt 2012] [Boureanu, Mitrokotsa, Vaudenay LATINCRYPT 2012]
- **Proposed new protocols that do not suffer of identified vulnerabilities** [Boureanu, Mitrokotsa, Vaudenay, LIGHTSEC 2013].
- Formalised & analysed distance-bounding protocols in the context of provable security, something that has not been done before [Boureanu, Mitrokotsa, Vaudenay, Lightsec 2013].

# Distance-bounding protocols: Contributions

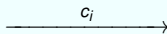
## Contributions

- **Analysed the security of existing distance-bounding protocols** [Mitrokotsa, Dimitrakakis, Peris-Lopez, IEEE Com. Let. 2010], [Mitrokotsa, Peris-Lopez, Dimitrakakis, Vaudenay Computer Journal 2013].
- **Described attacks that can be launched against** [Bay, Boureanu, Mitrokotsa, Spulber, Vaudenay, Inscrypt 2012] [Boureanu, Mitrokotsa, Vaudenay LATINCRYPT 2012]
- **Proposed new protocols that do not suffer of identified vulnerabilities** [Boureanu, Mitrokotsa, Vaudenay, LIGHTSEC 2013].
- **Formalised & analysed distance-bounding protocols in the context of provable security, something that has not been done before** [Boureanu, Mitrokotsa, Vaudenay, LIGHTSEC 2013]

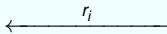
## Distance-Bounding Protocols : The SKI protocol

**Verifier**secret:  $x$ **Prover**secret:  $x$ **initialization phase****distance bounding phase**for  $i = 1$  to  $n$ pick  $c_i \in \{1, 2, 3\}$ 

start clock



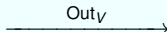
stop clock



$$r_i = \begin{cases} a_{1,i} & \text{if } c_i = 1 \\ a_{2,i} & \text{if } c_i = 2 \\ x_i \oplus a_{1,i} \oplus a_{2,i} & \text{if } c_i = 3 \end{cases}$$

check  $\tau$  responses

check timers



## Distance-Bounding Protocols: The SKI protocol

## Circular keying

- We require that leaking  $f_x(y)$ , or  $f_x(y) \oplus x$  or a mixture of both do not compromise security.
- An adversary  $\mathcal{A}$  making queries of the form  $(y_i, a_i, b_i)$  to an oracle:

$$y, a, b \rightarrow (a \cdot x') + (b \cdot f_{x(y)})$$

cannot distinguish if  $x = x'$  or  $x$  and  $x'$  are independent.

## Theorem

If  $f$  is a circular-keying secure PRF and  $V$  requires at least  $\tau$  correct responses:

- All DISTANCE-FRAUDS have a success probability bounded by  $\Pr[\text{success}] \geq B(b, \tau, \frac{3}{4})$
- All MIM attacks have a success probability bounded by  $\Pr[\text{success}] \geq B(b, \tau, \frac{2}{3})$
- For all COLLUSION FRAUDS such that  $\Pr[\text{CF succeeds}] \geq B(\frac{n}{2}, \tau - \frac{n}{2}, \frac{2}{3})^{1-c}$  there is an associated MIM with  $P^*$  such that:

$$\Pr[\text{MIM SUCCEEDS}] \geq \left(1 - B\left(\frac{n}{2}, \tau - \frac{n}{2}, \frac{2}{3}\right)^c\right)^n$$

$$B(n, \tau, \rho) = \sum_{i=\tau}^n \binom{n}{i} \rho^i (1 - \rho)^{n-i}$$

# Distance-Bounding Protocols: The SKI protocol

## Summary regarding DB

- several proposed protocols from the literature are insecure
- several security proofs from the literature are incorrect
- **SKI** [Serge - Katerina - Ioana] offers provable security

**Thank you for your attention !**