

RFID distance bounding protocol with mixed challenges to prevent relay attacks

Chong-Hee Kim and Gildas Avoine

Université catholique de Louvain, Louvain-la-Neuve, Belgium

CANS, Kanazawa, Japan, Dec. 2009

- RFID in a nutshell.
- Relay attacks.
- Our distance bounding protocol.
- Comparison with existing solutions.

RFID IN A NUTSHELL

- **RFID** = Radio-Frequency IDentification.
- **Tags** and **Readers** (possibly connected to a back-end system).
- Tags are **low-capability** devices, passive, up to smartcards.
- With or without microprocessor.
- Communication distance: a few **centimeters** to a few **meters**.

■ Supply chain tracking.

- Track boxes, pallets, ...



■ Pet identification.

- Replace common tattoos by electronic ones



■ Access control.

- Building, Public transportation.



■ Payment.

- SpeedPass, PayPass,

■ Electronic documents.

- ePassports, ...



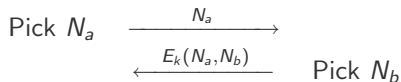
Security Particularities

- **Wireless** communication.
 - Easy access to the channel.
- Tags answer **without agreement** of their holders.
 - Implicit agreement = being in the reader's field.
- **Low capabilities** of the tags.
 - Lightweight cryptography.

Variant of ISO 9798-2 Protocol 3

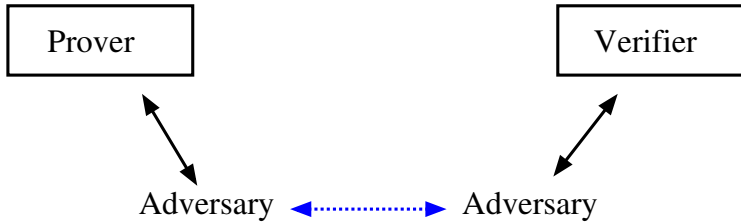
Verifier (secret k)

Prover (secret k)

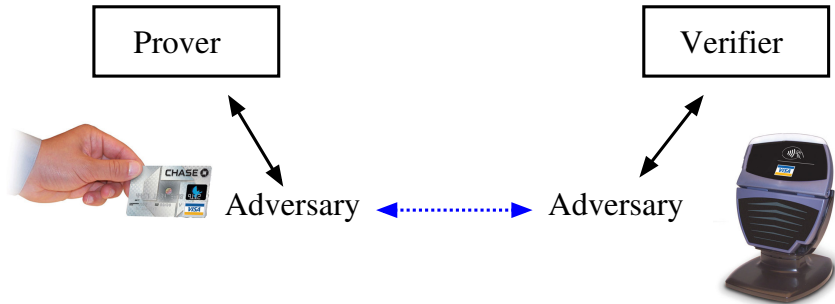


Protocol **secure** under common assumptions on E , k , N_a , and N_b .

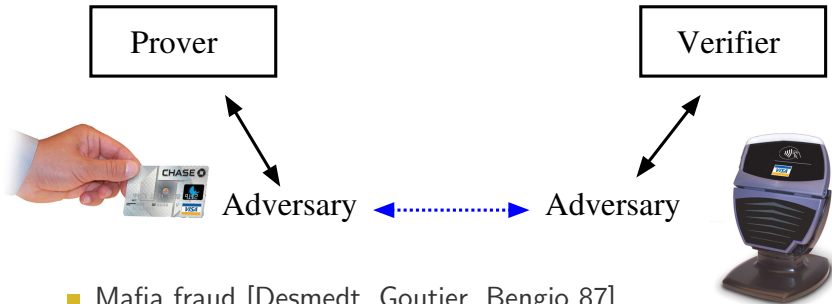
Mafia Fraud



Mafia Fraud



Mafia Fraud



- Mafia fraud [Desmedt, Goutier, Bengio 87].
- Aka chess grandmaster, man-in-the-middle, wormhole,...

Mafia Fraud



- Mafia fraud [Desmedt, Goutier, Bengio 87].
- Aka chess grandmaster, man-in-the-middle, wormhole,...
- **Successful** practical attacks.
 - Radio link over 50 meters (G. Hancke 05).
 - With some ACR122 (A. Laurie 09).

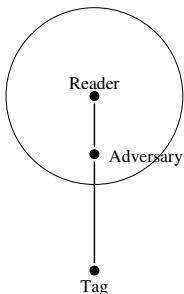
DISTANCE BOUNDING

Mafia and Distance Frauds

- We define a neighborhood as a zone around a reader.
- A tag present in the neighborhood agrees to authenticate.

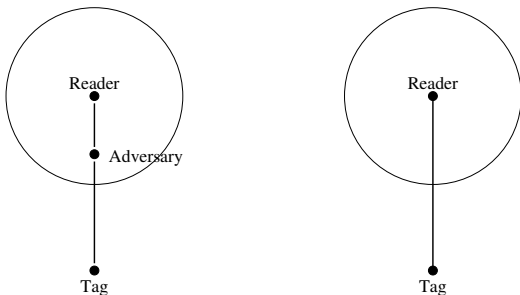
Mafia and Distance Frauds

- We define a neighborhood as a zone around a reader.
- A tag present in the neighborhood agrees to authenticate.



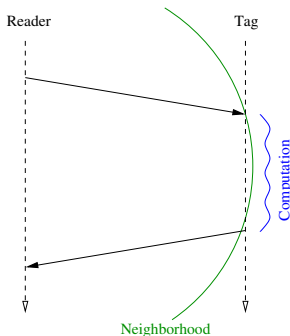
Mafia and Distance Frauds

- We define a neighborhood as a zone around a reader.
- A tag present in the neighborhood agrees to authenticate.



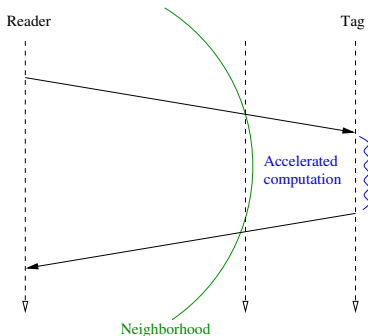
Distance Bounding (Proximity Check)

- Measure the **round-trip-time** (RTT) of a given message.
 - Provide a bound on the distance (proximity check).
 - Idea introduced by Beth and Desmedt [Crypto90].

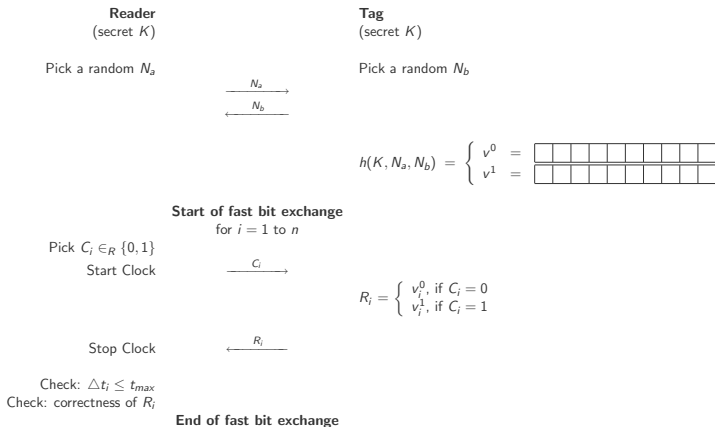


Distance Bounding (Proximity Check)

- Measure the **round-trip-time** (RTT) of a given message.
 - Provide a bound on the distance (proximity check).
 - Idea introduced by Beth and Desmedt [Crypto90].



Hancke and Kuhn's Protocol



- Can we design a distance bounding protocol without final signature and with 1-bit challenges that resists to the Mafia fraud with probability better than $(3/4)^n$?
- In HK, if the adversary sends a wrong C_i during the *pre-ask* phase, she is not penalized for the following rounds.
- Our idea consists in using **mixed** challenges: **predefined** or **random** challenges.

Kim and Avoine's Protocol

Reader
(secret K)

Pick a random N_a



Tag
(secret K)

Pick a random N_b

$$h(K, N_a, N_b) = \begin{cases} T = & \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \\ D = & \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \\ v^0 = & \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \\ v^1 = & \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \boxed{} \end{cases}$$

Start of fast bit exchange

for $i = 1$ to n

If $T_i = 1$ then $C_i \in_R \{0, 1\}$

If $T_i = 0$ then $C_i := D_i$

Start Clock



$$\text{If } T_i = 1, \text{ then } R_i = \begin{cases} v_i^0, & \text{if } C_i = 0 \\ v_i^1, & \text{if } C_i = 1 \end{cases}$$

$$\text{If } T_i = 0, \text{ then } R_i = \begin{cases} v_i^0, & \text{if } C_i = D_i \\ \text{random}, & \text{if } C_i \neq D_i \end{cases} \quad (\text{error detected})$$

Stop Clock



Check: $\Delta t_i \leq t_{max}$

Check: correctness of R_i

End of fast bit exchange

Mafia fraud: Probability of not being detected by the reader in round i :

$$P(\bar{A}_i) = \frac{1}{2} + \frac{1}{4} \left(\frac{1}{2} + \frac{1}{2} p_r \right)^{i-1}.$$

The probability of adversary success over n rounds is:

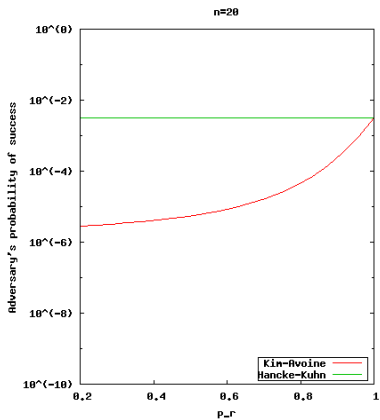
$$\prod_{i=1}^n P(\bar{A}_i).$$

For example, when $p_r = \frac{1}{2}$:

$$P(\bar{A}_1) = \frac{3}{4}, \quad P(\bar{A}_2) = \frac{11}{16}, \quad P(\bar{A}_3) = \frac{41}{64}, \quad P(\bar{A}_4) = \frac{155}{256}, \dots$$

Distance fraud: $1 - \frac{1}{4} p_r$ instead of $\frac{3}{4}$.

Comparison



CONCLUSION

- The first protocol (without signature) with an adversary success probability **less than $(3/4)^n$** .
- Are such protocols practicable?
- Which **parameters** can be modified?
- No **practical** and **secure** solution today in the market.

- RFID Security and Privacy Lounge:
 - <http://sites.uclouvain.be/security/>
- RFID Security and Privacy Training Week:
 - <http://sites.uclouvain.be/security/rfidtraining.html>