

# An Efficient Distance Bounding RFID Authentication Protocol: Balancing False-Acceptance Rate and Memory Requirement

Gildas Avoine<sup>1</sup> and Aslan Tchamkerten<sup>2</sup>

<sup>1</sup>Université catholique de Louvain, Louvain-la-Neuve, Belgium

<sup>2</sup>Telecom ParisTech, Paris, France

Information Security Conference, Pisa, Italy, Sept. 2009

# Summary

- A brief introduction to RFID.
- Authentication and Mafia fraud.
- Key-references in distance bounding.
- Our Protocol.

# RFID in a Nutshell

- RFID = Radio-Frequency IDentification.
- Tags and Readers (possibly connected to a back-end system).
- Tags are low-capability devices, passive.
- With or without microprocessor.
- Communication distance: a few cm to a few meters.
- Tags answer without agreement of their holders.
- Implicit agreement = being in the reader's field.

# RFID Applications

- Pet identification.
- Supply chain.
- Electronic passports.
- Mass transportation.
- Access control.
- Payment.

# Authentication

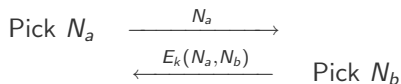
*“Entity authentication is the process whereby one party is assured (through acquisition of corroborative evidence) of the identity of a second party involved in a protocol, and that the second has actually participated (i.e., is active at, or immediately prior to, the time the evidence is acquired)”*

Handbook of Applied Crypto, Menezes, Oorschot, Vanstone.

# ISO 9798-2 Protocol 3 Unilateral

**Verifier** (secret  $k$ )

**Prover** (secret  $k$ )

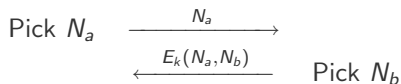


Protocol secure under some common assumptions on  $E$ ,  $k$ , and  $N_a$ .

# ISO 9798-2 Protocol 3 Unilateral

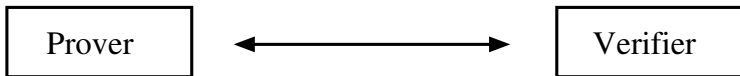
**Verifier** (secret  $k$ )

**Prover** (secret  $k$ )



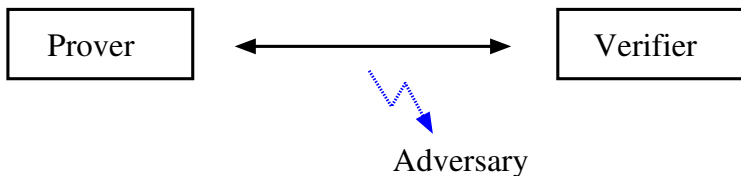
Protocol secure under some common assumptions on  $E$ ,  $k$ , and  $N_a$ .

# Mafia Fraud



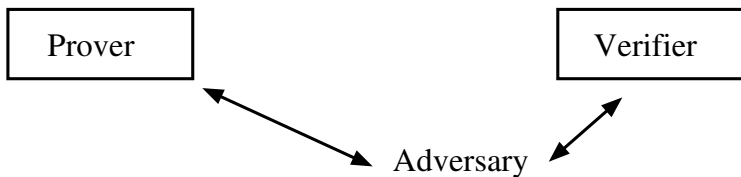
- Mafia fraud.
- Desmedt, Goutier, Bengio [Crypto87].
- Shamir about Fiat-Shamir protocol [Crypto86]: “I can go to a Mafia-owned store a million successive times and they still will not be able to misrepresent themselves as me.” (The NY Times, February 17, 1987, James Gleick).

# Mafia Fraud



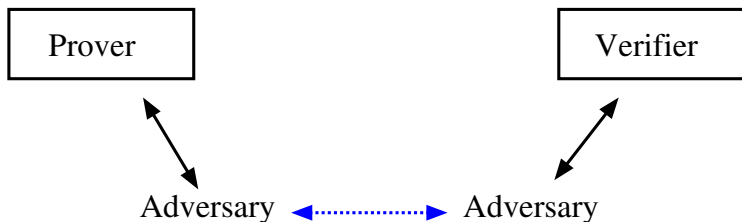
- Mafia fraud.
- Desmedt, Goutier, Bengio [Crypto87].
- Shamir about Fiat-Shamir protocol [Crypto86]: “I can go to a Mafia-owned store a million successive times and they still will not be able to misrepresent themselves as me.” (The NY Times, February 17, 1987, James Gleick).

# Mafia Fraud



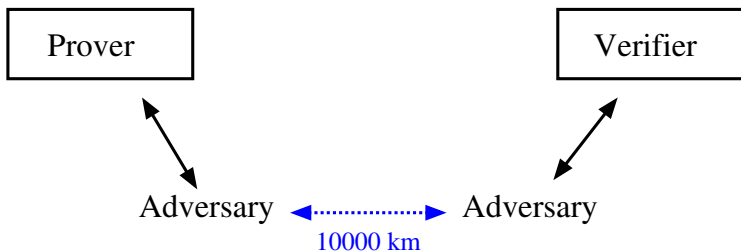
- Mafia fraud.
- Desmedt, Goutier, Bengio [Crypto87].
- Shamir about Fiat-Shamir protocol [Crypto86]: “I can go to a Mafia-owned store a million successive times and they still will not be able to misrepresent themselves as me.” (The NY Times, February 17, 1987, James Gleick).

# Mafia Fraud



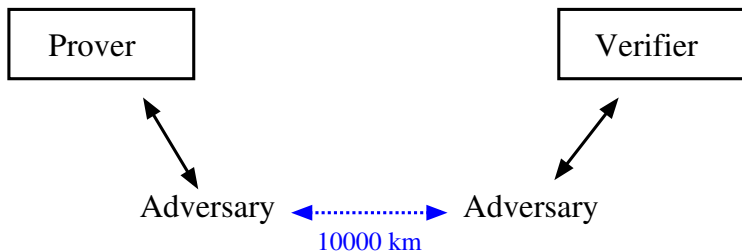
- Mafia fraud.
- Desmedt, Goutier, Bengio [Crypto87].
- Shamir about Fiat-Shamir protocol [Crypto86]: “I can go to a Mafia-owned store a million successive times and they still will not be able to misrepresent themselves as me.” (The NY Times, February 17, 1987, James Gleick).

# Mafia Fraud



- Mafia fraud.
- Desmedt, Goutier, Bengio [Crypto87].
- Shamir about Fiat-Shamir protocol [Crypto86]: "I can go to a Mafia-owned store a million successive times and they still will not be able to misrepresent themselves as me." (The NY Times, February 17, 1987, James Gleick).

# Mafia Fraud



- Mafia fraud.
- Desmedt, Goutier, Bengio [Crypto87].
- Shamir about Fiat-Shamir protocol [Crypto86]: “I can go to a Mafia-owned store a million successive times and they still will not be able to misrepresent themselves as me.” (The NY Times, February 17, 1987, James Gleick).

# Mafia Fraud: Example in a Queue



# Do-ability of Mafia Fraud

- Successful attacks.
  - Co-axial cable over 50 cm (T. Gross 06).
  - Radio link over 50 meters (G. Hancke 05).
- Reader starts a timer when sending a message.
  - To avoid semi-open connections.
- ISO 14443 “Proximity Cards” .
  - Used in most secure applications.
  - Standard on the low-layers (physical, collision-avoidance).
  - Default timer is around 5 ms.
  - Prover can require more time, up to 4949 ms.

# Do-ability of Mafia Fraud

- Successful attacks.
  - Co-axial cable over 50 cm (T. Gross 06).
  - Radio link over 50 meters (G. Hancke 05).
- Reader starts a timer when sending a message.
  - To avoid semi-open connections.
- ISO 14443 “Proximity Cards” .
  - Used in most secure applications.
  - Standard on the low-layers (physical, collision-avoidance).
  - Default timer is around 5 ms.
  - Prover can require more time, up to 4949 ms.

# Distance Bounding (Proximity Check)

- Literature

- Beth and Desmedt [Crypto90]
- Brands and Chaum [Eurocrypt93]
- Hancke and Kuhn [SecureComm05]
- ...

- The verifier calculates the round trip time of a message.

- Message needs to be authenticated.
- Authentication is time-consuming.
- Round trip time is noised.

# Adversary Model

- Can eavesdrop, intercept, modify or inject messages.
- Cannot correctly encrypt, decrypt, or sign messages without knowledge of the appropriate key.
- Can increase or decrease the clock frequency of a tag and thus the computation speed.
- Can increase the transmission speed on the channel up to a given bound (speed of light).

# Adversary Model

- We define a neighborhood as a zone around a reader.
- We consider that a tag present in a neighborhood agrees to authenticate.
- We say that a tag  $T$  has been impersonated if an execution of the protocol convinced a reader that it has authenticated  $T$  while the latter was not present inside the neighborhood during the said execution.

# Brands and Chaum's Protocol

**Verifier** (secret  $k$ )

**Prover** (secret  $k$ )

**Start of fast phase**

for  $i = 1$  to  $n$

Start Clock  $\xrightarrow{C_i \in_R \{0,1\}}$

Stop Clock  $\xleftarrow{R_i \in_R \{0,1\}}$

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

**End of fast phase**

Check signature  $\xleftarrow{\text{Sign}_k(C_1 || R_1 || \dots || C_n || R_n)}$

# Brands and Chaum's Drawbacks

- Security of the protocol:  $(1/2)^n$ .
  - On-the-fly authentication should take less than 50 ms.
  - Turn-around time does not allow a large  $n$ .
  - Security is degraded.
- There is a final signature.
  - If the protocol is interrupted, no rational decision can be taken by the verifier.

# Hancke and Kuhn's Protocol

**Verifier** (secret  $k$ )

**Prover** (secret  $k$ )

Random  $N_a$   $\xrightarrow{N_a}$   
 $\xleftarrow{N_b}$

Random  $N_b$

$$v^0 \| v^1 := H_k(N_a, N_b) \quad \text{where} \quad |v^0| = |v^1| = n$$

**Start of fast phase**

for  $i = 1$  to  $n$

Start Clock  $\xrightarrow{C_i \in_R \{0,1\}}$

Stop Clock  $\xleftarrow{R_i}$

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

**End of fast phase**

Check correctness of  
 $R_i$ 's and  $\Delta t_i \leq \Delta t_{\max}$

# Hancke and Kuhn's Drawbacks

- The final signature is no longer needed.
- Security of the protocol still depends on  $n$ .
- Security of the protocol is  $(3/4)^n$  instead of  $(1/2)^n$ .

# Open Problem

- Can we design a distance bounding protocol without final signature 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 a tree instead of 2 registers.

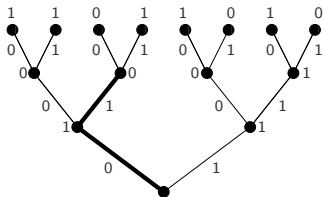
# Open Problem

- Can we design a distance bounding protocol without final signature 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 a tree instead of 2 registers.

# Open Problem

- Can we design a distance bounding protocol without final signature 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 a tree instead of 2 registers.

# The Decision Tree



**Figure:** Decision tree with  $n = 3$ . The thick line path in the tree corresponds to the verifier's challenges 0, 1, 0 and the prover's replies 1, 0, 0.

# Our Protocol

**Verifier** (secret  $k$ )

Compute  $H_k(N_a, N_b)$

$\xrightarrow{N_a}$

$\xleftarrow{N_b, [H_k(N_a, N_b)]_1^m}$

**Prover** (secret  $k$ )

Compute  $H_k(N_a, N_b)$

**Start of fast phase**

for  $i = 1$  to  $n$

Start Clock

$\xrightarrow{C_i \in_R \{0,1\}}$

$R_i := \text{node}(C_1 \dots C_i)$

Stop Clock

$\xleftarrow{R_i}$

**End of fast phase**

Check correctness of  
 $R_i$ 's and  $\Delta t_i \leq \Delta t_{\max}$

# Success Probability w.r.t. Mafia Fraud

$$\begin{aligned}\Pr(\tilde{R}^n = R^n) &= \sum_{i=1}^n \Pr(\tilde{R}^n = R^n | t = i) \Pr(t = i) \\ &\quad + \Pr(\tilde{R}^n = R^n | C^n = 0^n) \Pr(C^n = 0^n) \\ &= \sum_{i=1}^n 2^{-(n-i+1)} 2^{-i} + 2^{-n} \\ &= 2^{-n} (n/2 + 1) .\end{aligned}$$

# False Acceptance Rate

- A FAR of 0.01% can be reached with a single tree of depth 17, which requires 32 Kbytes of memory.
- A FAR of 0.01% can also be obtained by using two trees each of depth 9. This decreases the needed memory down to 256 bytes (0.25 Kbytes).

# Conclusion

- The first protocol that requires no signature and with a FAR less than  $(3/4)^n$ .
- Are such protocols practicable?
- Which parameters can be modified?
- No practical solution today (except NXP Mifare Plus).