Distance Bounding for RFID

Prof. Gildas Avoine
Université catholique de Louvain, Belgium
Information Security Group

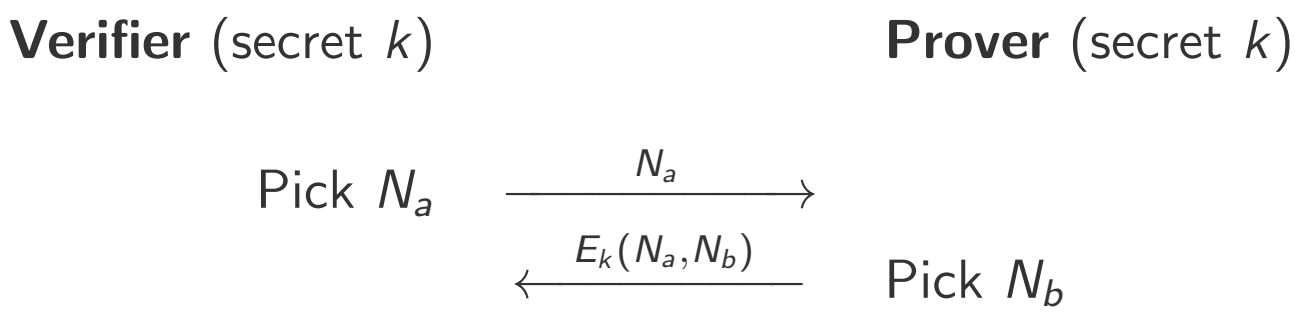
SUMMARY

- Relay Attacks
- Distance Bounding Protocols
- Discussion

RELAY ATTACKS

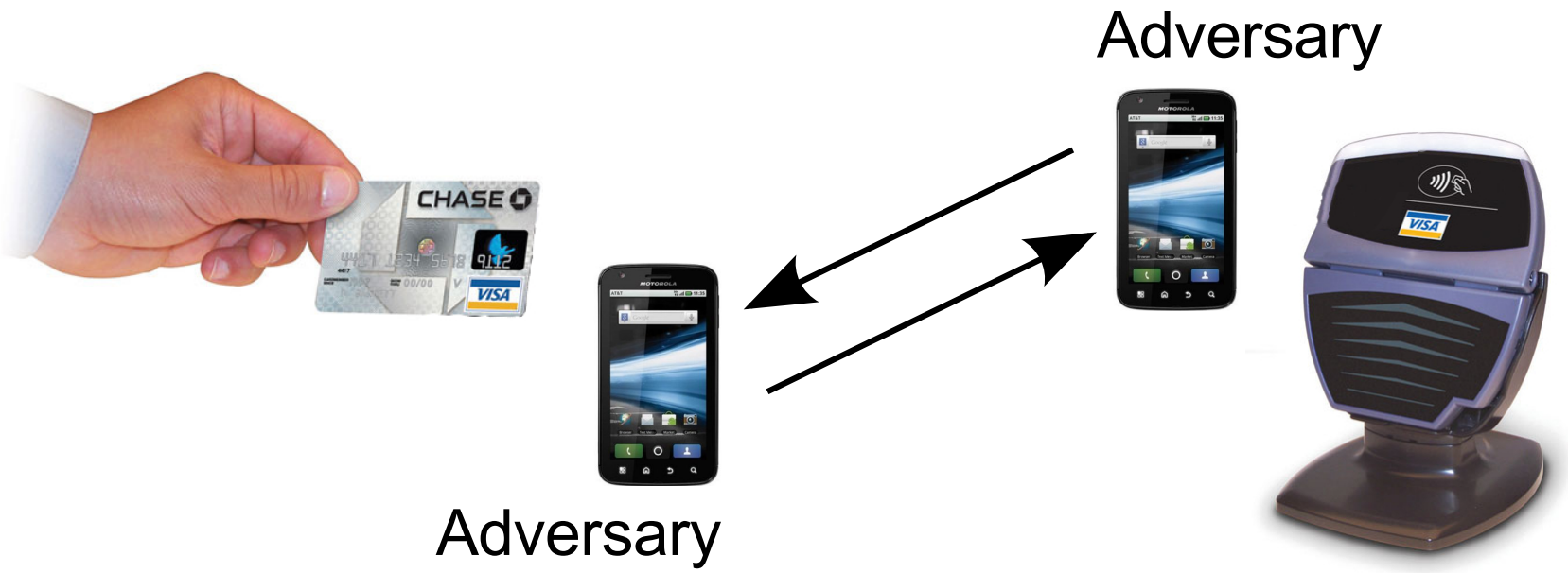
- Relay Attacks
- Distance Bounding Protocols
- Discussion

Variant of ISO 9798-2 Protocol 3



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

Relay Attack



Definition (Relay Attack)

A relay attack is a form of man-in-the-middle where the adversary manipulates the communication by only relaying the verbatim messages between two parties.

Practicability
Examples

- Radio link over 50 meters (G. Hancke [4]).
- Implementation included in libNFC (PN53x readers).

- Attacks by Francillon, Danev, Čapkun (ETHZ) against passive keyless entry and start systems used in modern cars [6].
  - 10 systems tested: no one resisted!

(a) Loop antenna placed next to the door handle.

(b) Starting the engine using the relay.

DISTANCE BOUNDING PROTOCOLS

- Relay Attacks
- Distance Bounding Protocols
- Discussion

Protocol Aims in General Framework [5]

Definition (Distance Bounding)

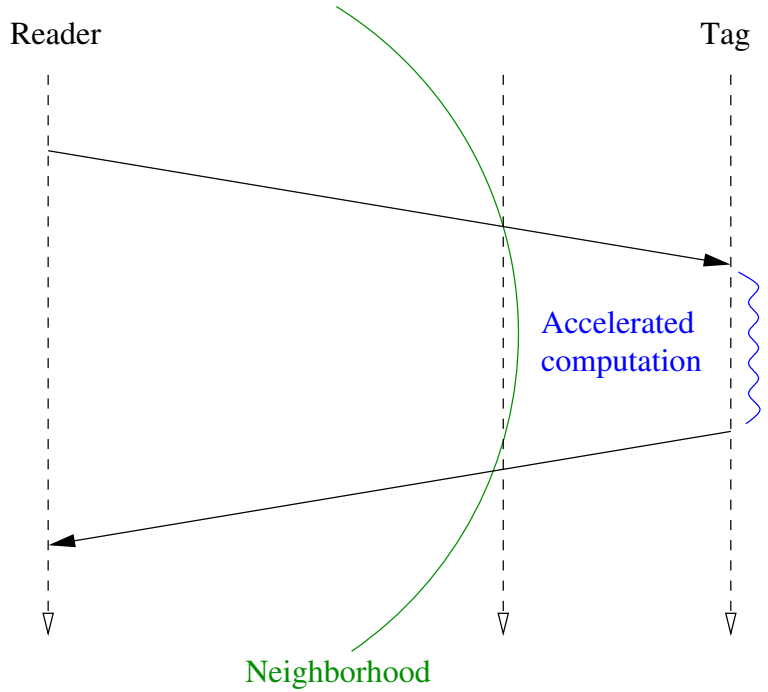
A distance bounding is a process whereby one party is assured:

1. Of the identity of a second party,
2. That the latter is present in the neighborhood of the verifying party, at some point in the protocol.

Distance bounding does not avoid relay attacks.

Distance Bounding Based on the Speed of Light

- Measure the round-trip-time (RTT) of a given message.
  - Provide a bound on the distance.
  - Idea introduced by Beth and Desmedt [2].



- Msg must be authenticated
- Auth. is time-consuming

Hancke and Kuhn's Protocol [3]
First RFID-focused Distance Bounding Protocol

Reader (secret K)		**Tag** (secret K)
Pick a random N_a	$\xrightarrow{N_a}$	
	$\xleftarrow{N_b}$	Pick a random N_b

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

Start of fast bit exchange

for $i = 1$ to n

Pick $C_i \in_R \{0,1\}$		
Start Clock	$\xrightarrow{C_i}$	
		$R_i = \begin{cases} v_i^0, \text{ if } C_i = 0 \\ v_i^1, \text{ if } C_i = 1 \end{cases}$
Stop Clock	$\xleftarrow{R_i}$	

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

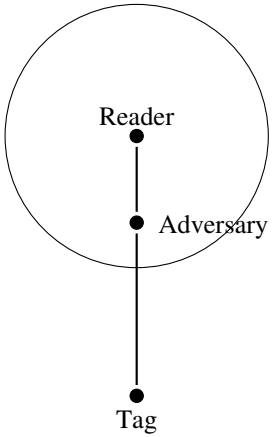
Check: correctness of R_i

End of fast bit exchange

Mafia and Distance Frauds

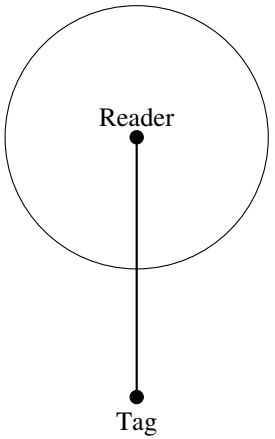
Definition (Mafia Fraud)

A mafia fraud [1] is an attack where an adversary defeats a distance bounding protocol using a man-in-the-middle (MITM) between the reader and an honest tag located outside the neighborhood.



Definition (Distance Fraud)

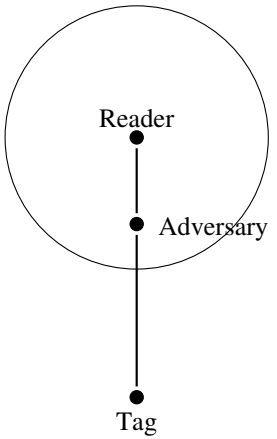
Given a distance bounding protocol, a distance fraud is an attack where a dishonest and lonely prover purports to be in the neighborhood of the verifier.



Terrorist Fraud

Definition (Terrorist Fraud)

A terrorist fraud is an attack where an adversary defeats a distance bounding protocol using a man-in-the-middle (MITM) between the reader and a dishonest tag located outside of the neighborhood, such that the latter actively helps the adversary to maximize her attack success probability, without giving to her any advantage for future attacks.



Hancke and Kuhn's Protocol

Reader
(secret K)

Pick a random N_a

$\xrightarrow{N_a}$

$\xleftarrow{N_b}$

Tag
(secret K)

Pick a random N_b

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

Start of fast bit exchange
for $i = 1$ to n

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

$\xrightarrow{C_i}$

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

$\xleftarrow{R_i}$

Stop Clock

Check: $\triangle t_i \leq t_{max}$
Check: correctness of R_i

End of fast bit exchange

Question

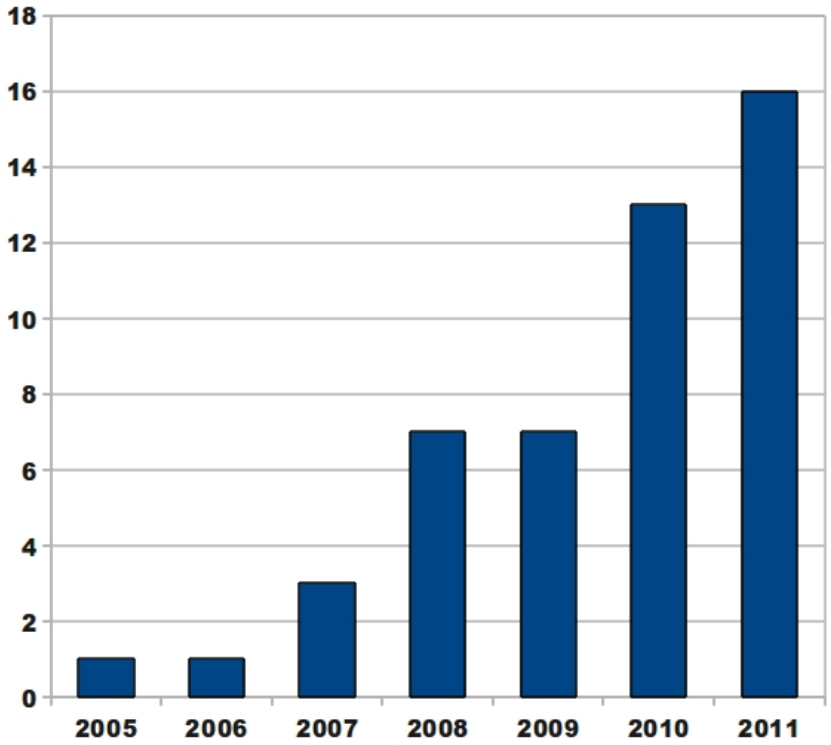
1. Mafia fraud: $\left(\frac{3}{4}\right)^n$
2. Terrorist fraud: 1
3. Distance fraud: $\left(\frac{3}{4}\right)^n$

DISCUSSION

- Relay Attacks
- Distance Bounding Protocols
- Discussion

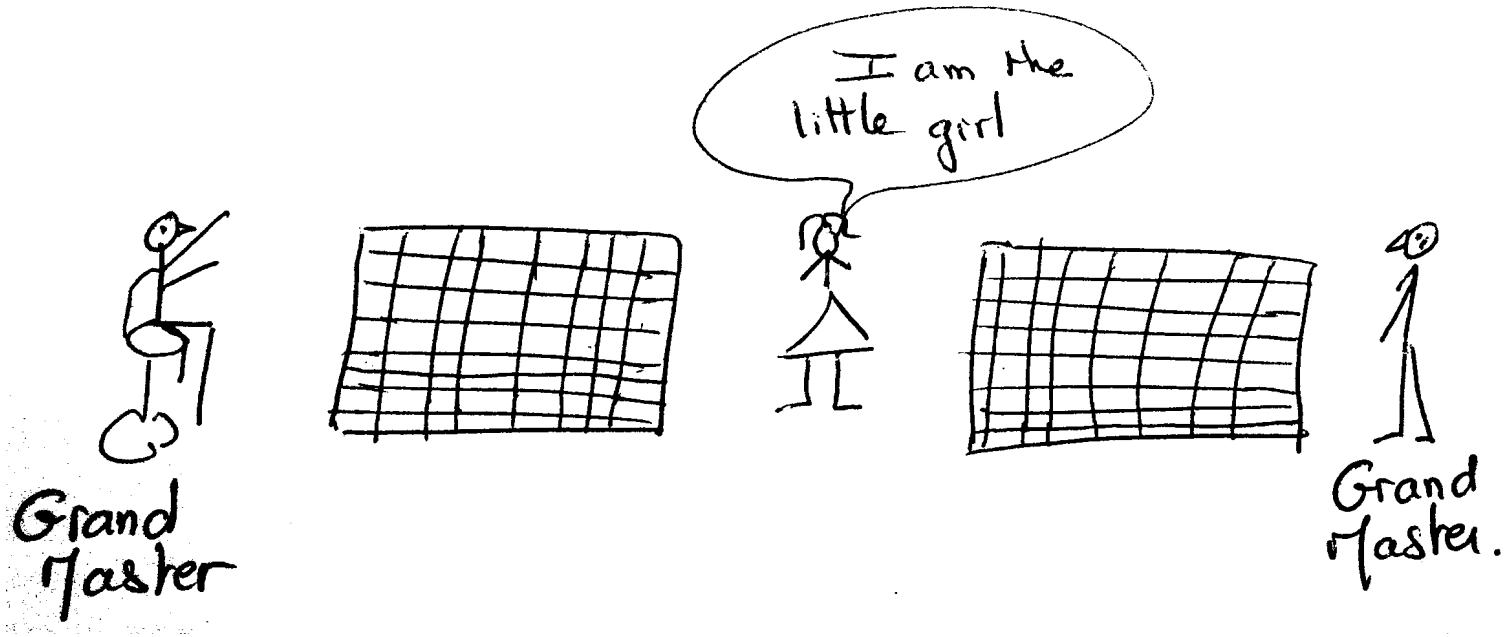
An Active Research Field in RFID?

- Is distance bounding an active research field in RFID?



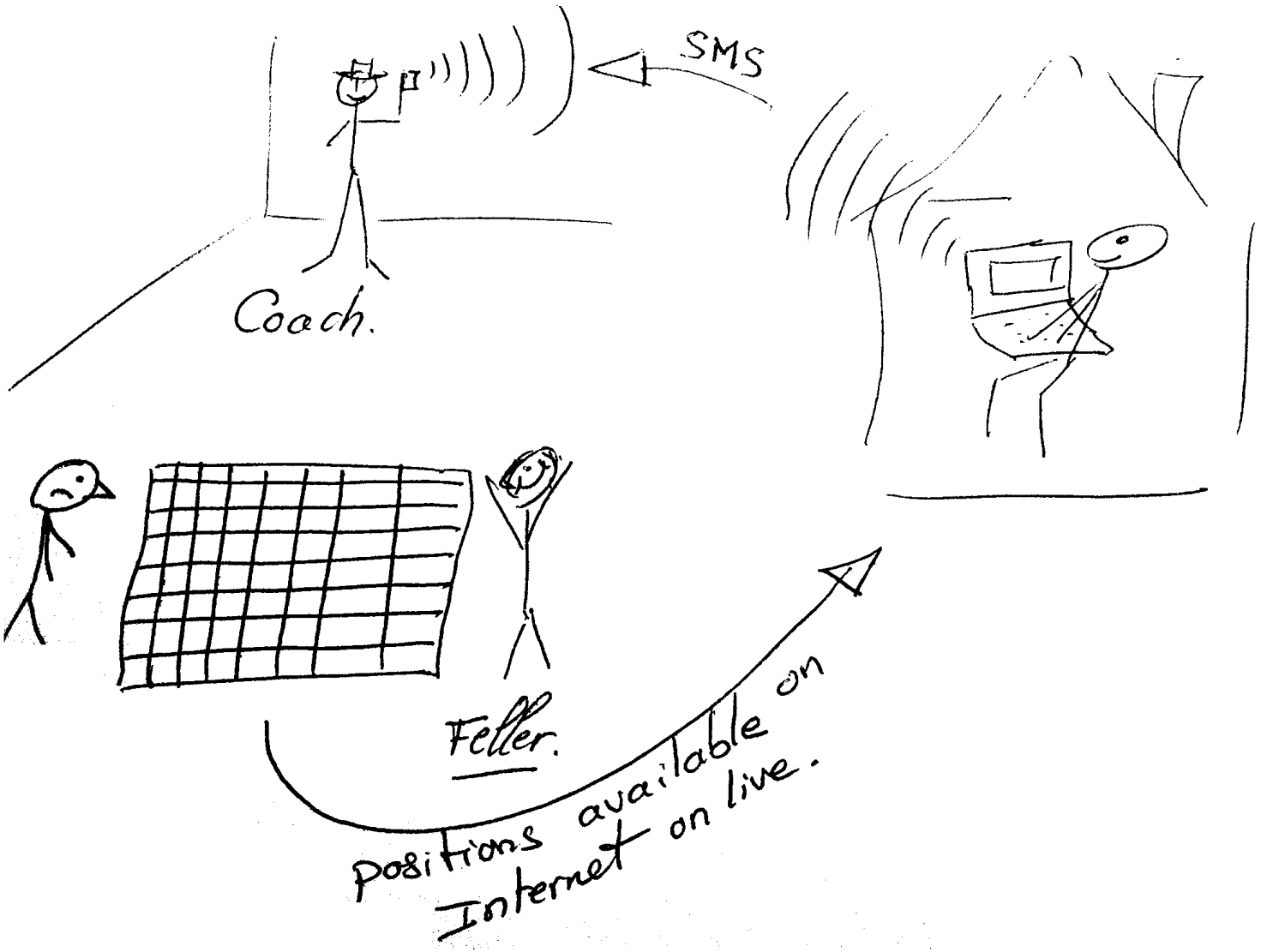
Relay in Other Domains?

- Are relay attacks only meaningful in the RFID context?
  - No! But RFID increases the risk.
- Chess grand master problem (Conway 1976)



Relay Attacks in Chess (Chess Olympiad 2010)

- French player Sébastien Feller during the Olympiad in Russia.



Distance Bounding too RFID-oriented

- Is research on distance bounding too RFID-oriented?
  - Probably yes.
- No cryptographic operation performed during the fast phase.
- Restrictive assumption: 1-bit challenges and responses
- Avoid a final signature.
- Which is the best protocol without the 2 last assumptions?

Current Research Activities

- Are there existing models/frameworks?

Definition

In a black-box model, the prover cannot observe or tamper with the execution of the algorithm.

Definition

In a white-box model, the prover has full access to the implementation of the algorithm and a complete control over the execution environment.

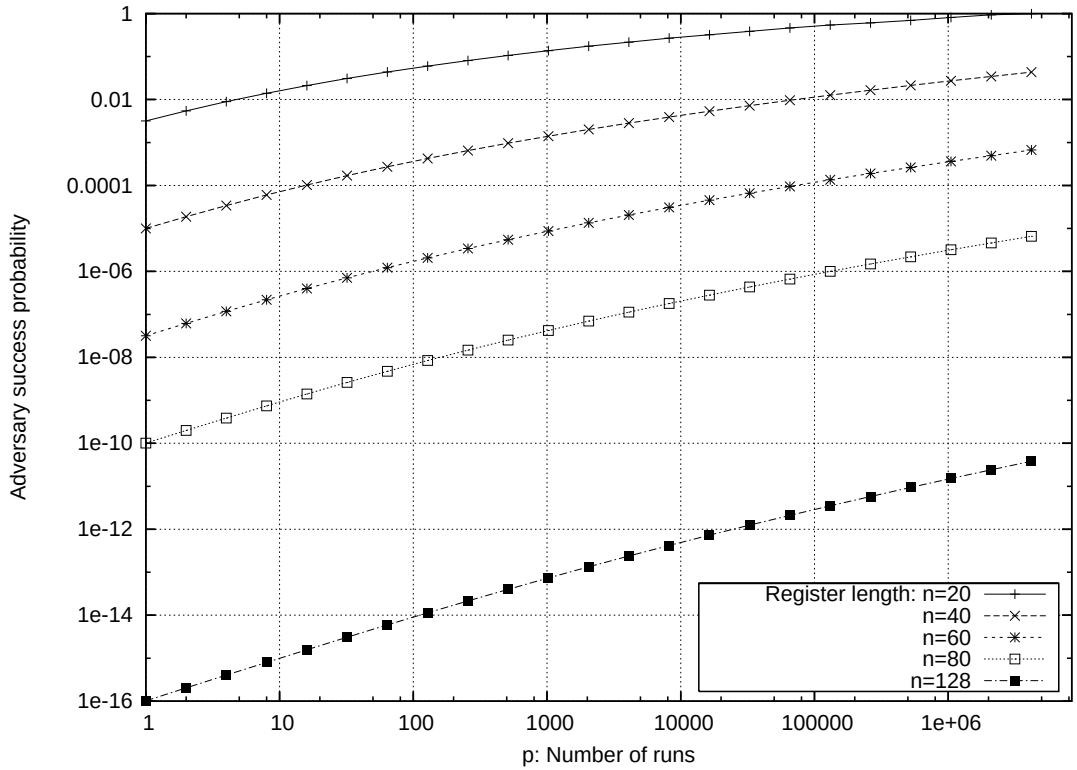
Definition (Pre-ask strategy)

The adversary relays the first slow phase. She then executes the fast phase with the prover before the verifier starts the fast phase. Afterward, she performs the fast phase with the legitimate verifier.

Theoretical model

- Are there some other attack scenarios?

- In the white-box model, restricting the computation capabilities of the prover within one protocol execution is required.



Hancke and Kuhn's Protocol

Reader (secret K)		**Tag** (secret K)
Pick a random N_a	$\xrightarrow{N_a}$	
	$\xleftarrow{N_b}$	Pick a random N_b

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

Start of fast bit exchange

for $i = 1$ to n

Pick $C_i \in_R \{0,1\}$		
Start Clock	$\xrightarrow{C_i}$	
		$R_i = \begin{cases} v_i^0, \text{ if } C_i = 0 \\ v_i^1, \text{ if } C_i = 1 \end{cases}$
Stop Clock	$\xleftarrow{R_i}$	

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

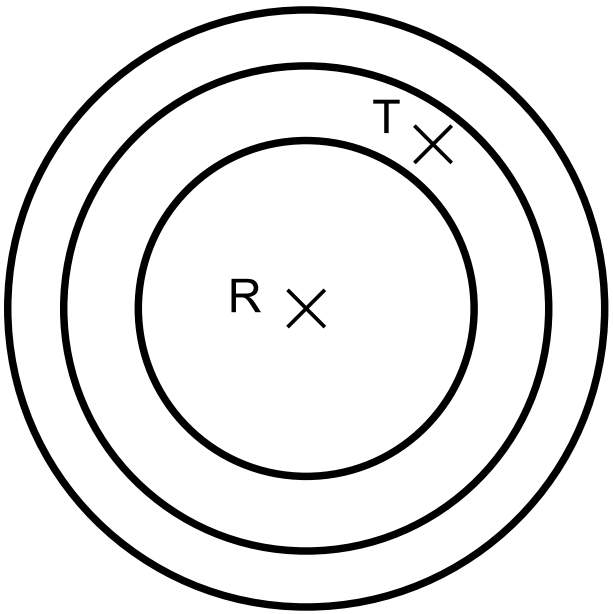
Check: correctness of R_i

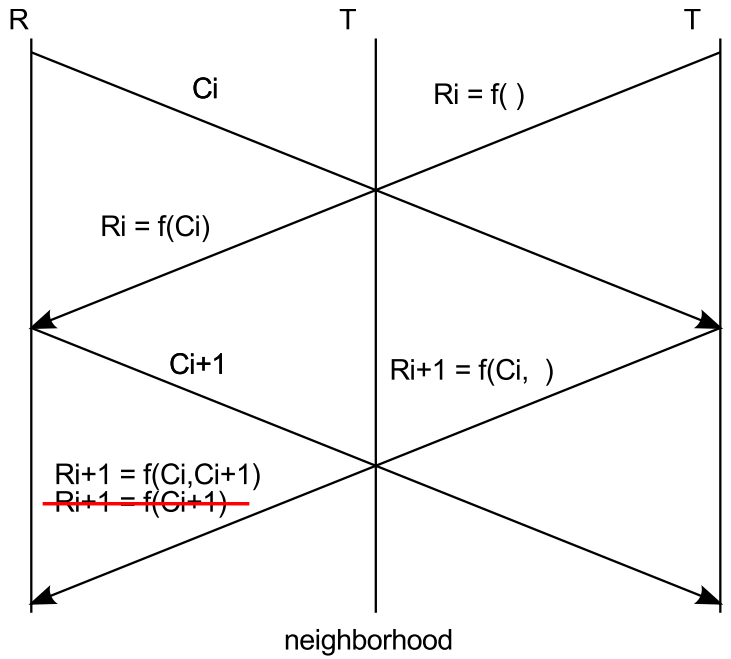
End of fast bit exchange

Question

1. Mafia fraud: $\left(\frac{3}{4}\right)^n$
2. Terrorist fraud: 1
3. Distance fraud: $\left(\frac{3}{4}\right)^n$

- In some distance bounding protocols, each response bit depends on some previous challenges during the fast phase.
- Receiving the previous challenges depends on how far the prover is away from the verifier.





Pretty Poor Proofs

- Proofs are "given an attack scenario".

Assumptions realistic

- Are there other questionable assumptions?
- Propagation delays are much shorter than processing times.
- Adversary also induces some delays.
- Thwarting adversaries using commercial readers.
- Consider a new distance?

Suggested Directions

- Theory is not mature yet.
- Do not introduce tons of new protocols.
- Be less RFID-focused.
- Provide less scenario-oriented proofs.
- Think about a new distance.

Further Reading

[1] Y. Desmedt, C. Goutier, and S. Bengio. Special Uses and Abuses of the Fiat-Shamir Passport Protocol. CRYPTO'87.

[2] T. Beth and Y. Desmedt. Identification Tokens - or: Solving the Chess Grandmaster Problem. CRYPTO '90.

[3] G. Hancke and M. Kuhn. An RFID Distance Bounding Protocol. SecureComm 2005.

[4] G. Hancke. Practical Attacks on Proximity Identification Systems. IEEE Symposium on Security and Privacy, 2006.

[5] G. Avoine, M. Bingöl, S. Kardas, C. Lauradoux, and B. Martin. A Framework for Analyzing RFID Distance Bounding Protocols. Journal of Computer Security, 2010.

[6] A. Francillon, B. Danev, and S. Čapkun. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. Network and Distributed System Security Symposium, 2011.