Relay Attacks and Distance Bounding Protocols

Gildas Avoine
Université catholique de Louvain, Belgium

Workshop on Cryptography for the Internet of Things

November 20 – 21, 2012, Antwerp, Belgium

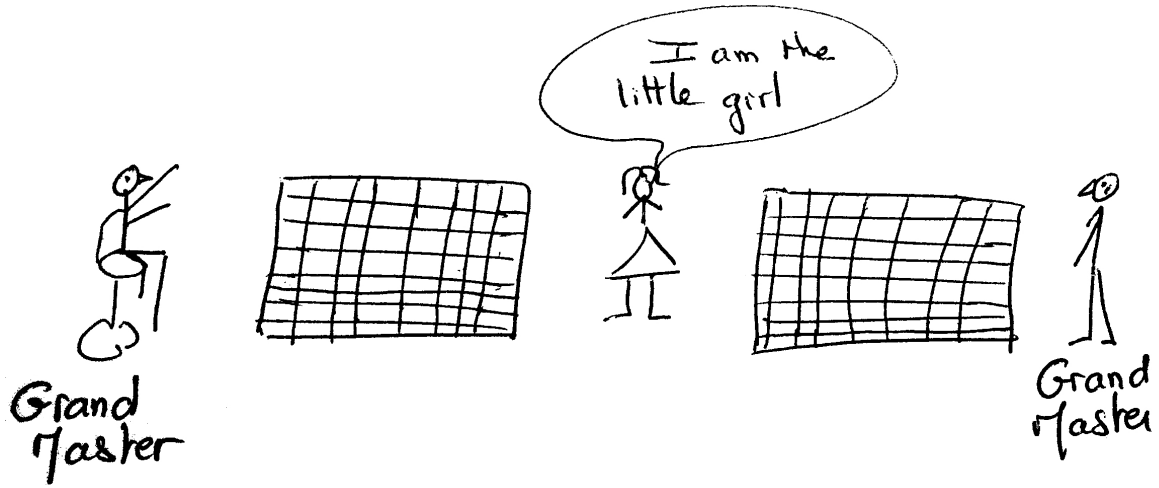
SUMMARY

- Relay Attacks
- Distance Bounding
- Distance Bounding Protocols
- Discussion

RELAY ATTACKS

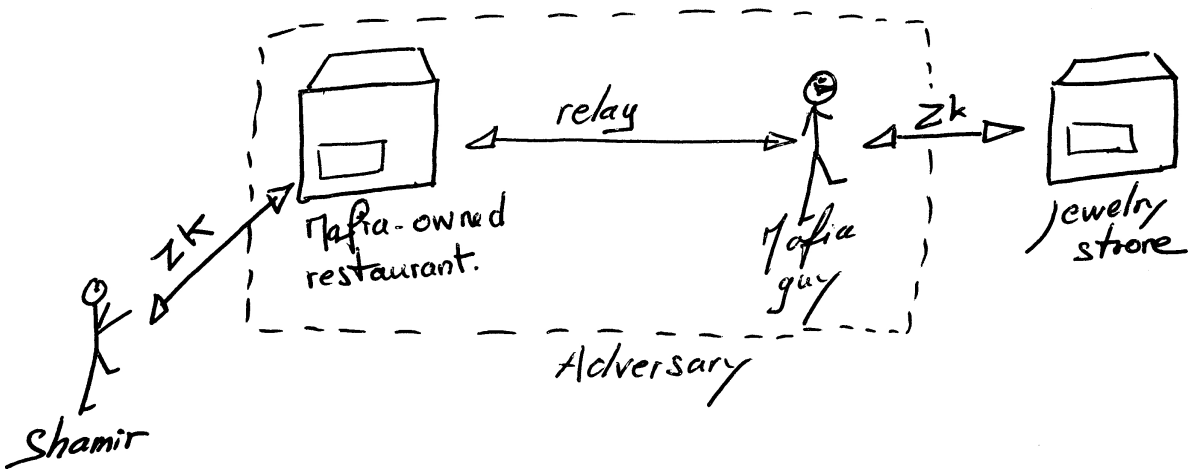
- Relay Attacks
- Distance Bounding
- Distance Bounding Protocols
- Discussion

- Chess Grand master problem (Conway 1976)



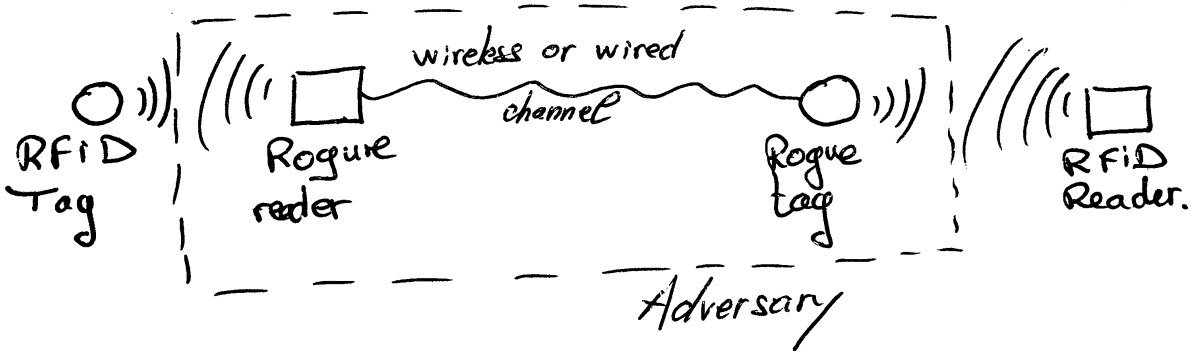
J. H. Conway. On Numbers and Games. Number 6 in London Mathematical Society Monographs, 1976.

- Feige-Fiat-Shamir ZK Protocol (1987)
- Shamir: "I can go to a Mafia-owned store a million successive times and they still will not be able to misrepresent themselves as me." (Gleick quoting Shamir, 1987)
- Desmedt, Goutier, Bengio (1987): Mafia fraud



Desmedt, Goutier, and Bengio. Special Uses and Abuses of the Fiat-Shamir Passport Protocol. CRYPTO'87

- Radio link over 50 meters (Hancke 2006).



Hancke. Practical Attacks on Proximity Identification Systems. IEEE Symposium on Security and Privacy, 2006

- Attacks by Francillon, Danev, Čapkun against passive car keyless entry and ignition systems (2011).

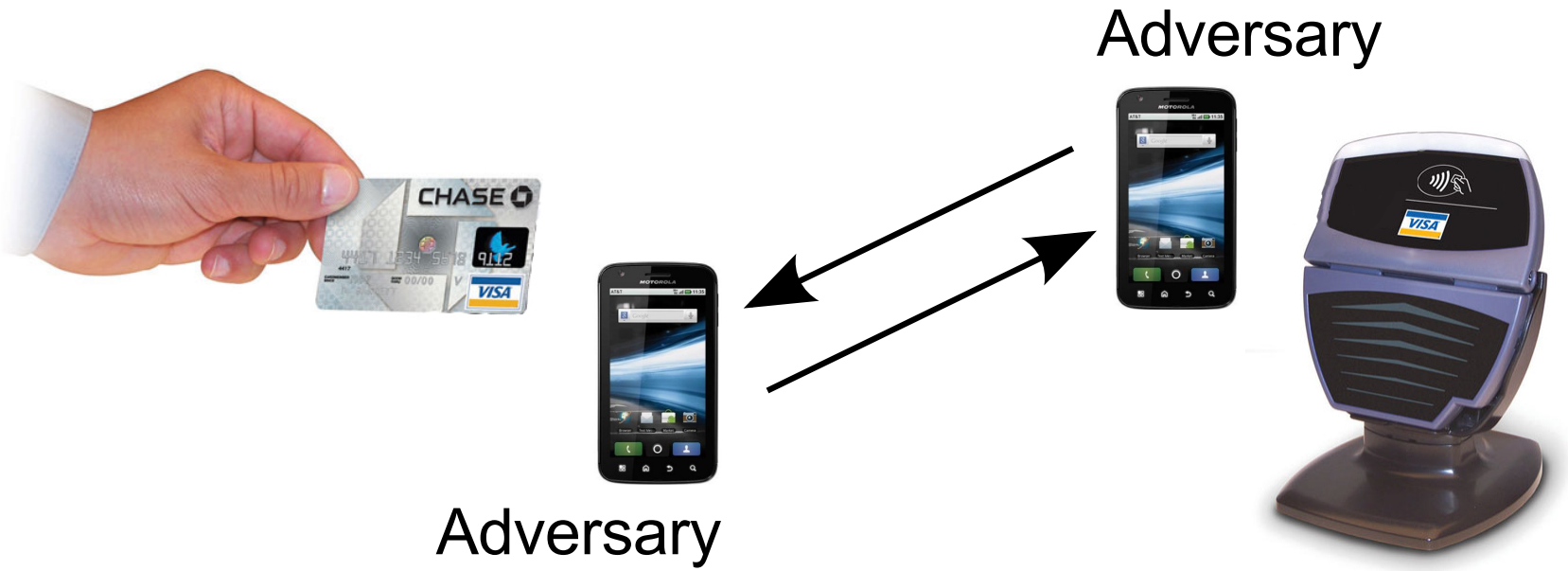
(a) Loop antenna placed next to the door handle.

(b) Starting the engine using the relay.

Francillon, Danev, and Čapkun. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. Network and Distributed System Security Symposium, 2011

Today and Tomorrow

- Implementation included in libNFC (PN53x readers).

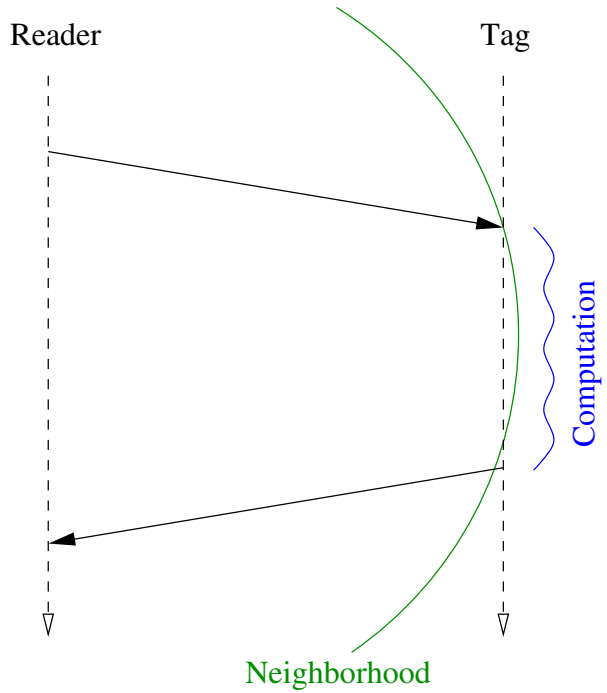


DISTANCE BOUNDING

- Relay Attacks
- Distance Bounding
- Distance Bounding Protocols
- Discussion

Distance Bounding Based on the Speed of Light

- Measure the round-trip-time (RTT) of an auth. message
  - Provide a bound on the distance.
  - Idea introduced by Beth and Desmedt (1990).



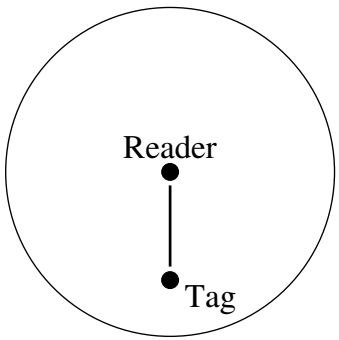
Beth and Desmedt. Identification Tokens - or: Solving the Chess Grandmaster Problem. CRYPTO'90.

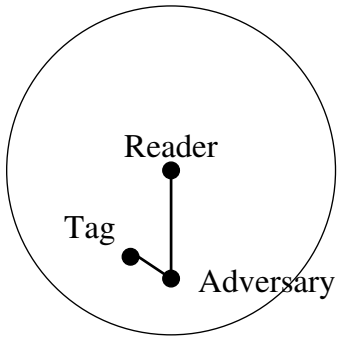
Distance Bounding

Definition (Avoine et al. 2011)

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.

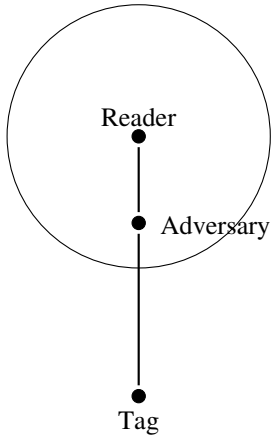
A Framework for Analyzing RFID Distance Bounding Protocols, 2011.

Avoine, Bingöl, Kardas, Lauradoux, and Martin.

Mafia and Terrorist Frauds

Definition (Mafia Fraud)

A mafia fraud 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.



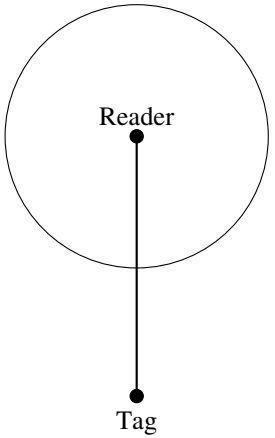
Definition (Terrorist Fraud)

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.

Distance Fraud

Definition (Distance Fraud)

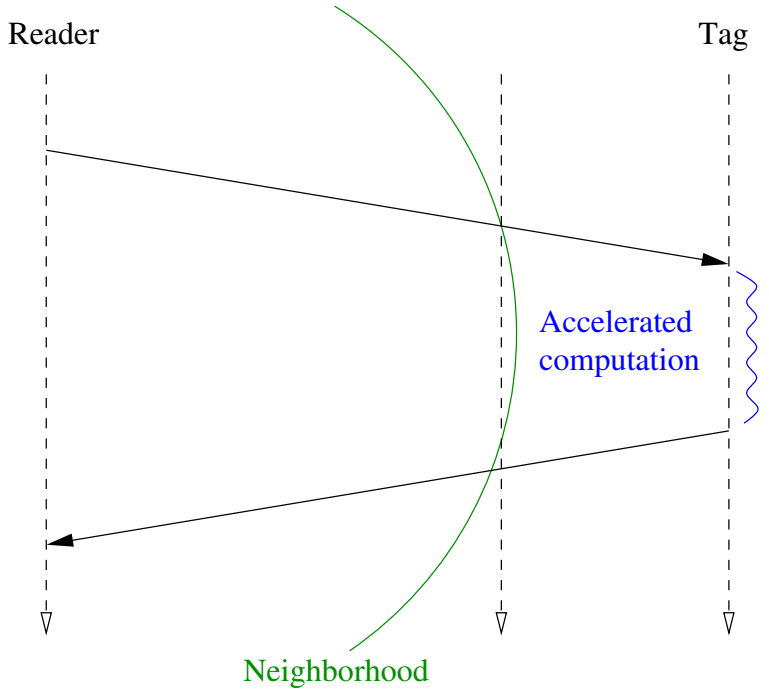
Given a distance bounding protocol, a distance fraud is an attack where a dishonest and lonely prover purports to be in the neighborhood of the verifier.



Real Life

- ISO 14443 already includes a timeout.
- Mifare Plus has a distance bounding protocol.

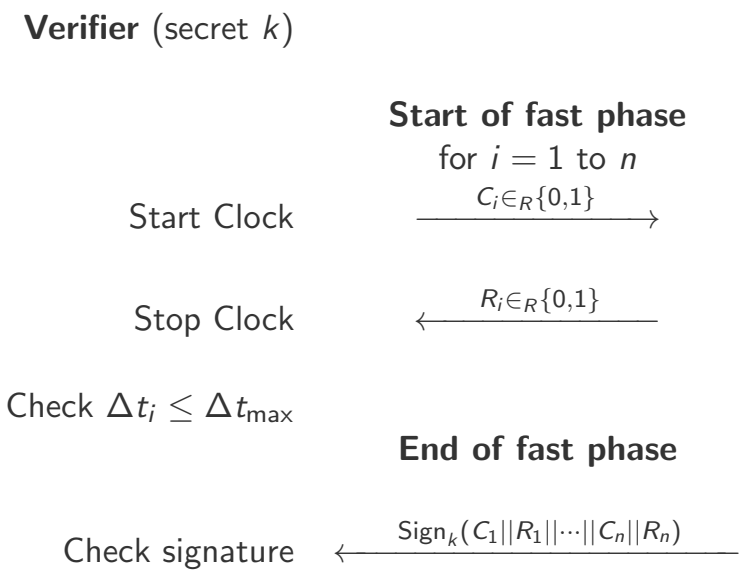
Distance Bounding Based on the Speed of Light



DISTANCE BOUNDING PROTOCOLS

- Relay Attacks
- Distance Bounding
- Distance Bounding Protocols
- Discussion

Brands and Chaum's Protocol (1993)



Question

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

Brands and Chaum, Distance-Bounding Protocols, EUROCRYPT'93.

Hancke and Kuhn's Protocol (2005)

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

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

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: $\left(\frac{3}{4}\right)^n$

Hancke and Kuhn. An RFID Distance Bounding Protocol. SecureComm 2005.

DISCUSSION

- Relay Attacks
- Distance Bounding
- Distance Bounding Protocols
- Discussion

Current Issues

- Improving the security w.r.t. the three frauds.
- Propagation delays are much shorter than processing times.
- Filling the gap between theory and practice.
- Defining clear adversary's capabilities.
- Provably secure distance-bounding protocols: Serge Vaudenay's talk.

Relay Attack in Chess (Chess Olympiad 2010)