A Primer on Relay Attacks and Distance-bounding Protocols

Gildas Avoine

Univ Rennes, INSA Rennes, CNRS
Institut Universitaire de France

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES RENNES

IUF

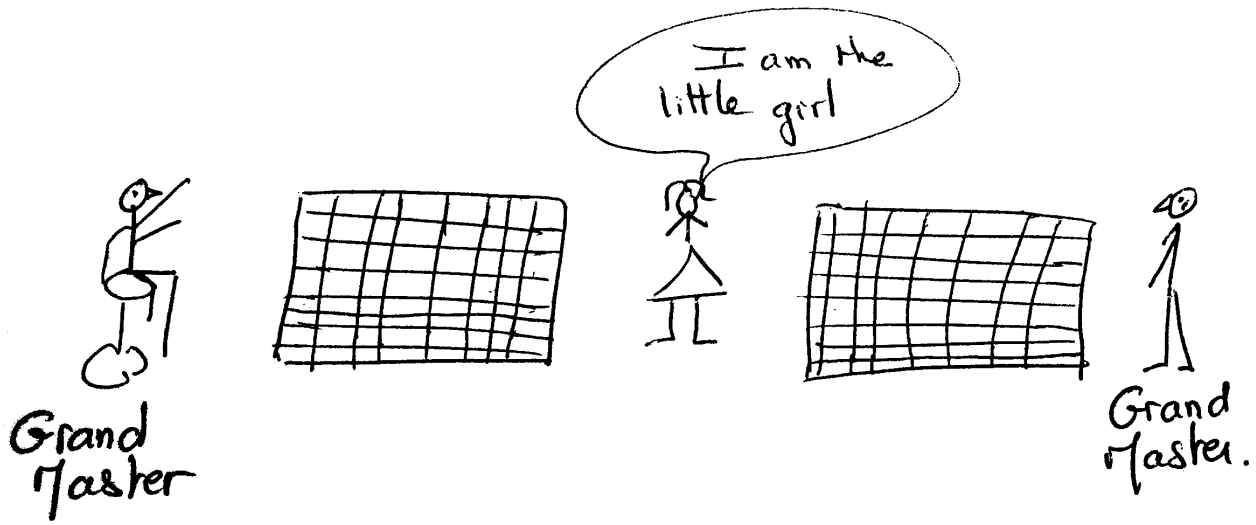
SUMMARY

- Relay Attacks
- Distance Bounding Protocols
- From Theory to Practice
- Conclusion

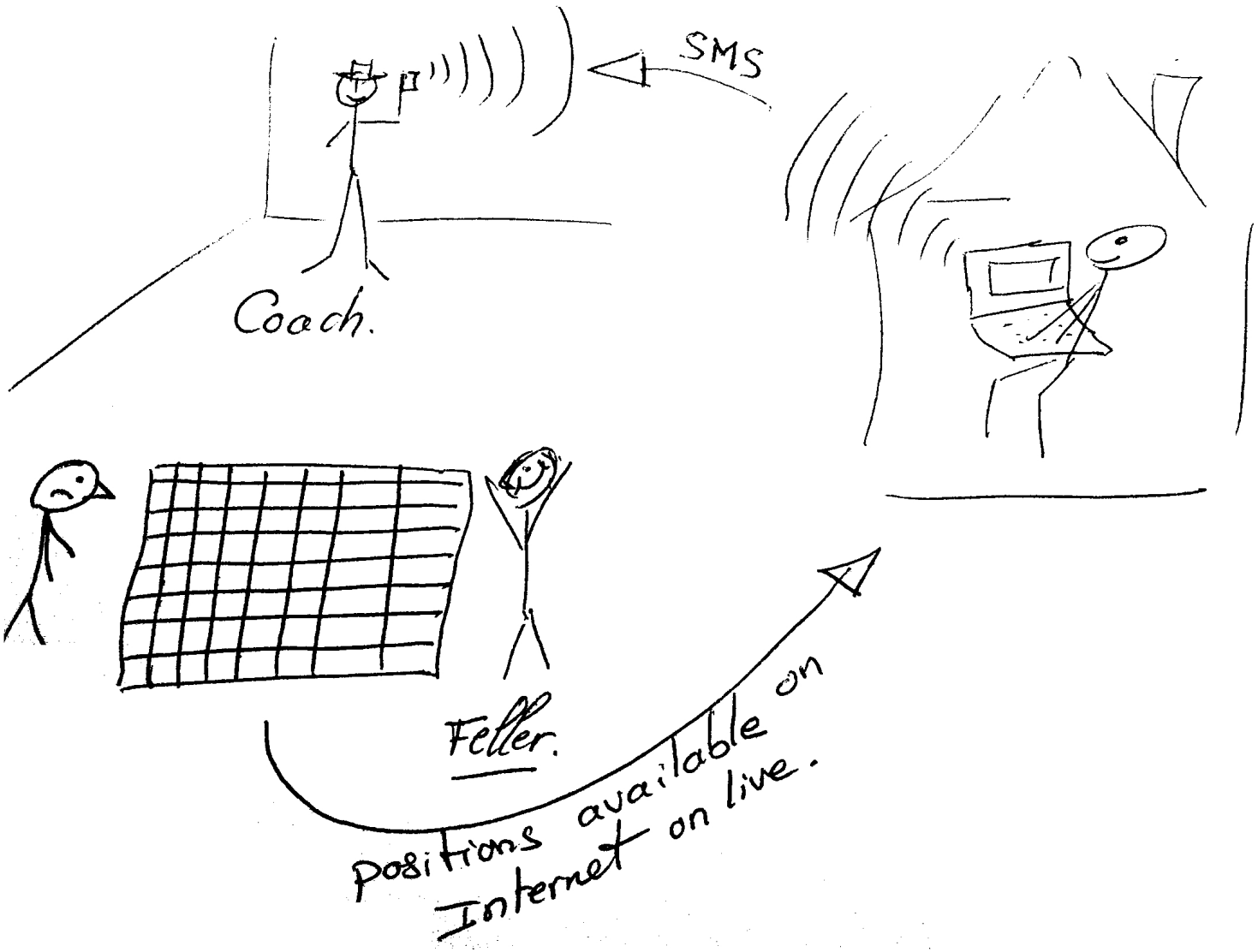
RELAY ATTACKS

- Relay Attacks
- Distance Bounding Protocols
- From Theory to Practice
- Conclusion

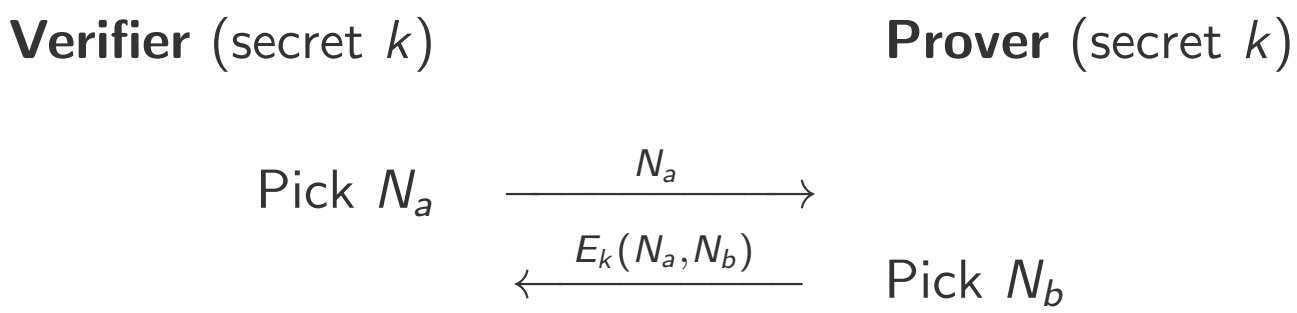
Chess Grandmaster Problem (Conway 1976)



Cheat During Chess Games (Chess Olympiad 2010)

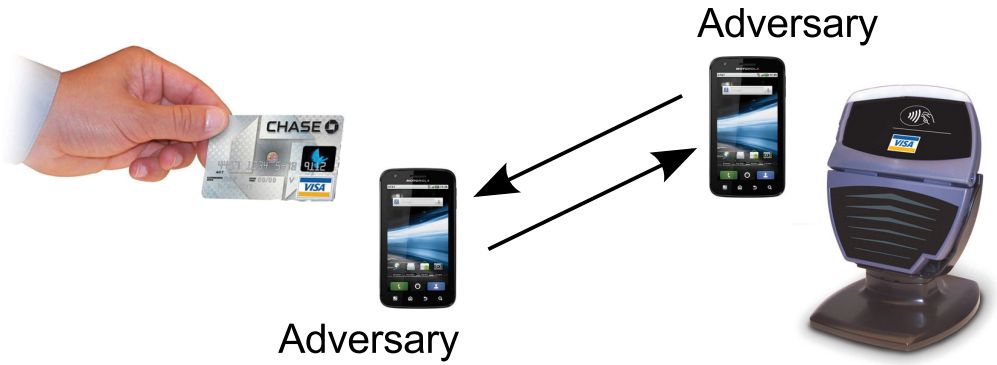


ISO 9798-2 Protocol 3 (Variant)

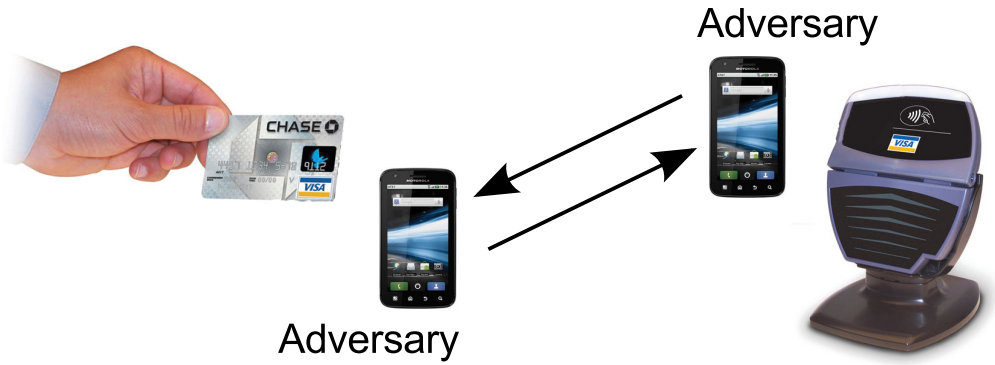


Protocol secure under common assumptions on E, k, N_a, and N_b.

Relay Attack



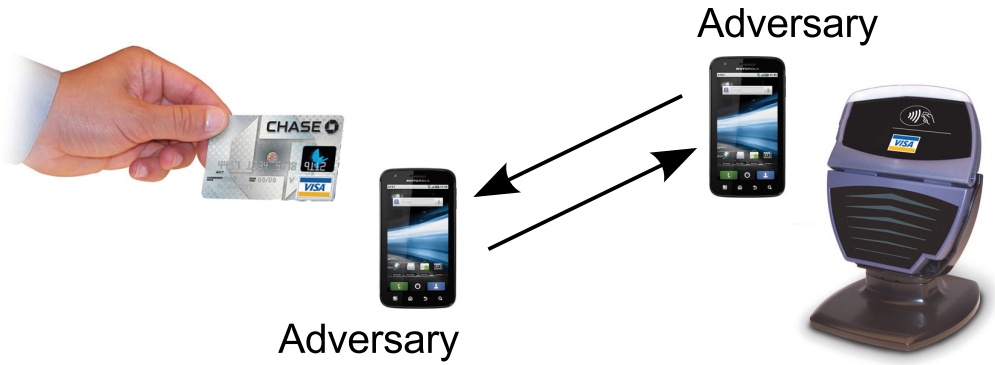
Relay Attack



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.

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.

Comment

Desmedt, Goutier, and Bengio [Desmedt et al. 1988] extended this concept to security protocols in 1987, with an attack on the Fiat-Shamir protocol [Fiat and Shamir 1986; Feige et al. 1987].

Experimental Results

- Radio link over 50 meters (G. Hancke, IEEE SSP 2006).
- Attacks by Francillon, Danev, Čapkun (ETHZ) against keyless entry and start systems used in modern cars (NDSSS 2011).

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

(b) Starting the engine using the relay.

- Implementation in libNFC. Implementations for smartphones.

Off-the-Shelf Devices

One person with the ***Q-key*** scanner stands near the key owners (*f. e. at the hotel reception*). A second person is located near the vehicle with the ***Q-Key*** transmitter (*f. e. in the basement car park).* The ***Q-key*** system now bypasses the large distance between the key owner and his vehicle in the basement car park. Both the keyless control unit in the vehicle, as well the transponder within the car key is lead to believe in a regular process (*regular process: key is located directly at the vehicle*).

Scenarios

- Payment (e.g., in the lockers of a swimming pool)
- Access control
- Digital right management (DRM)

DISTANCE BOUNDING PROTOCOLS

- Relay Attacks
- Distance Bounding Protocols
- From Theory to Practice
- Conclusion

Objective of Distance Bounding Protocols

Definition (Distance Bounding)

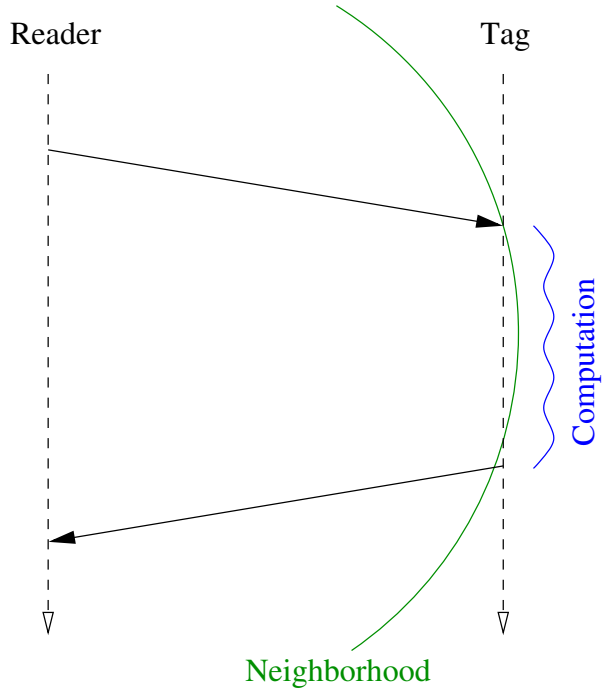
A distance bounding is a process whereby one party is assured:

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

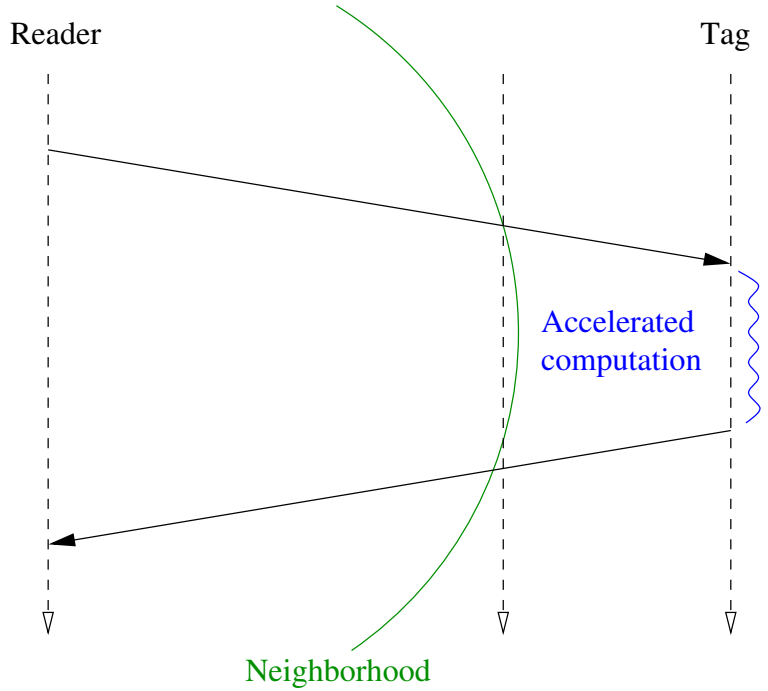
- Earliest distance bounding protocol: Brands and Chaum in 1993, based on an idea from Beth and Desmedt, 1990.
- Measure the round-trip-time (RTT) of a given message.



- Lightweight operations during RTT measurement.
- 1-bit challenges/responses.

Distance Bounding Based on the Speed of Light

- Earliest distance bounding protocol: Brands and Chaum in 1993, based on an idea from Beth and Desmedt, 1990.
- Measure the round-trip-time (RTT) of a given message.



- Lightweight operations during RTT measurement.
- 1-bit challenges/responses.

Hancke and Kuhn's Protocol (SecureComm 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

FROM THEORY TO PRACTICE

- Relay Attacks
- Distance Bounding Protocols
- From Theory to Practice
- Conclusion

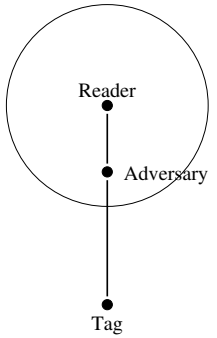
Attributes

- Resistance to frauds.
- Memory consumption.
- Number of crypto op.
- Final slow phase.
- Single-bit messages.
- Resilient to noisy channels.
- Security proofs.
- Mutual authentication.
- Mutual distance bounding.
- ...

Mafia and Distance Frauds

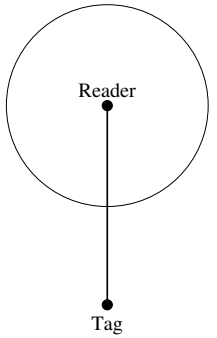
Definition (Mafia Fraud)

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.



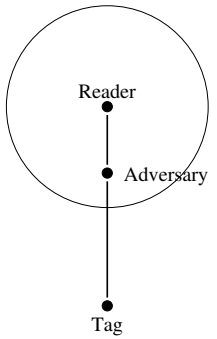
Definition (Distance Fraud)

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

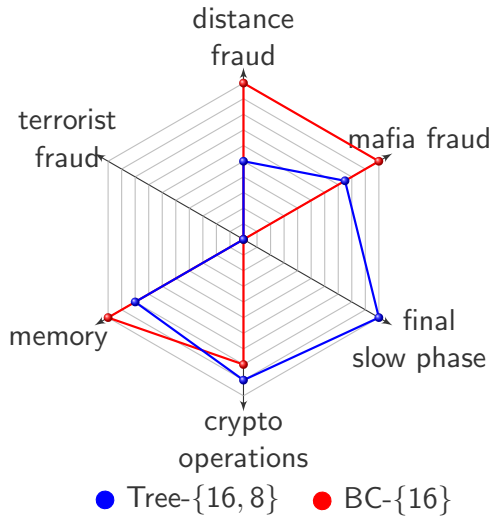


Definition (Terrorist Fraud)

A terrorist fraud is an attack where an adversary defeats a distance bounding protocol using a man-in-the-middle 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.



Spider Charts for Two Protocol Instances

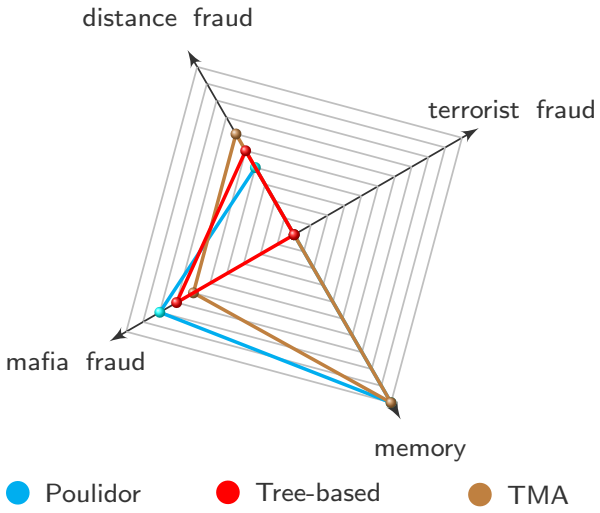


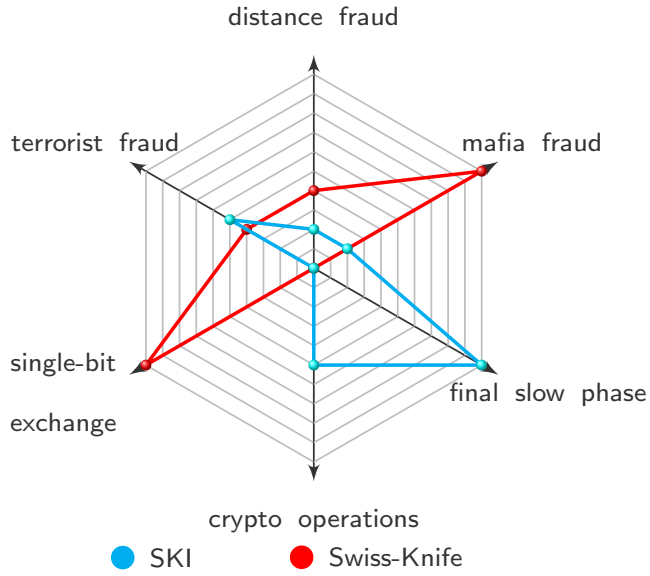
Joined work with Rolando Trujillo and Sjouke Mauw

Candidates

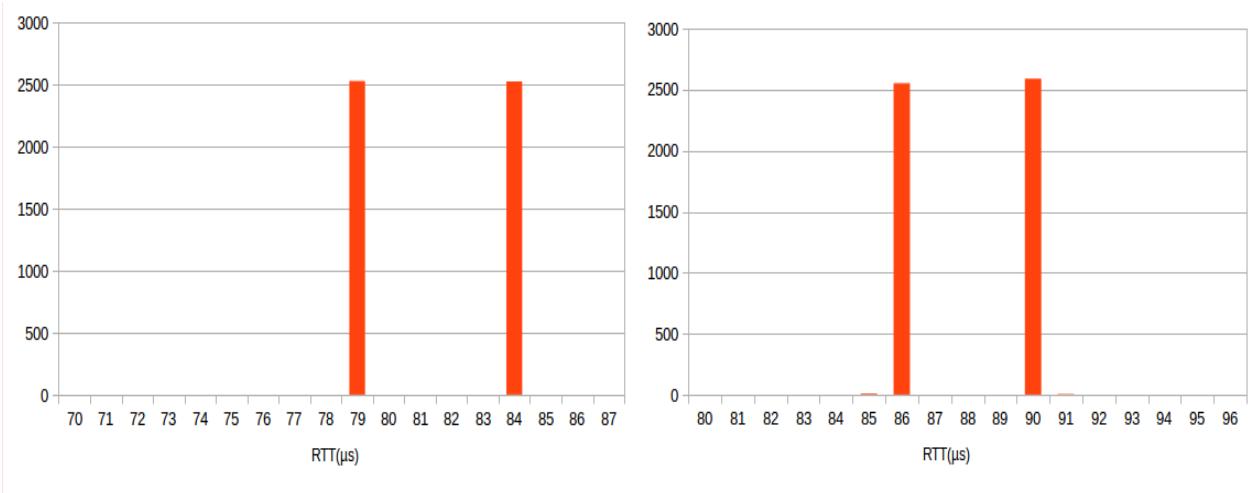
Protocol Instance	Parameter values
BC-$\{n\}$	$n \in \{1, \cdots, 128\}$
MAD-$\{n\}$	$n \in \{1, \cdots, 128\}$
BB-$\{n\}$	$n \in \{1, \cdots, 128\}$
HK-$\{n\}$	$n \in \{1, \cdots, 128\}$
MP-$\{n, p_f\}$	$n \in \{1, \cdots, 128\}$, $p_f \in \{0, 0.05, 0.01, \cdots, 1\}$
Swiss-Knife-$\{n\}$	$n \in \{1, \cdots, 128\}$
Tree-based-$\{n, \ell\}$	$n \in \{1, \cdots, 128\}$, $\ell \in \{1, 2, \cdots, 32\}$
Poulidor-$\{n\}$	$n \in \{1, \cdots, 128\}$
RC-$\{n\}$	$n \in \{1, \cdots, 128\}$
YKHL-$\{n\}$	$n \in \{1, \cdots, 128\}$
KA-$\{n, p_d\}$	$n \in \{1, \cdots, 128\}$, $p_d \in \{0, 0.05, 0.01, \cdots, 1\}$
SKI-$\{n, t\}$	$n \in \{1, \cdots, 128\}$, $t \in \{2, 3, \cdots, 32\}$
TMA-$\{n\}$	$n \in \{1, \cdots, 128\}$

Non-Dominated Protocols





Implemented Protocol: Measured round-trip time



Joined work with Rokia Lamrani Allaoui and Cristina Onete

Fastest Attacks

- Off-the-shelf tools: $\approx$ 10 milliseconds
- Tested distance bounding protocol: RTT $\approx$ 90 microseconds
- Thevenon et al.'s attack: $\approx$ 2 microseconds
- Francillon et al.'s attack: $\approx$ 100 nanoseconds

CONCLUSION

- Relay Attacks
- Distance Bounding Protocols
- From Theory to Practice
- Conclusion

Conclusion

- Practical DB-protocols mitigate the relay attacks.
- Attacks are still possible, though.
- Few devices implement DB-protocols
- No real-life application use a DB-protocol ???
- Still room for improvement: less computation, constant time, other frauds, proofs,...
- Practical implementations are needed.