Relay Attacks and Distance Bounding Protocols in RFID Environments

Prof. Gildas Avoine

Université catholique de Louvain, Belgium

Information Security Group

SUMMARY

- RFID Background
- Relay Attacks
- Countermeasures and Evolved Frauds
- Protocols
- Analysis Framework
- Conclusion and Further Reading

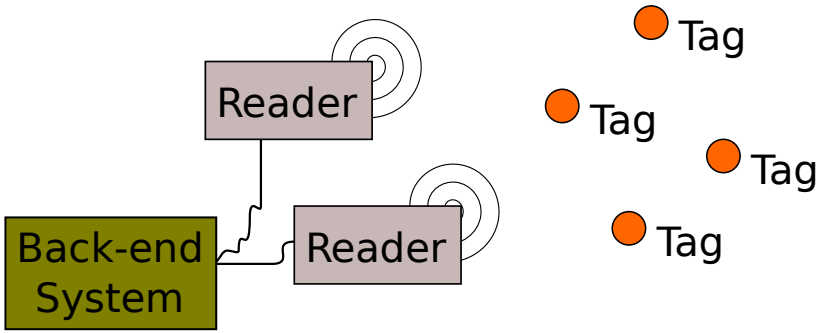
RFID BACKGROUND

- RFID Background
- Relay Attacks
- Countermeasures and Evolved Frauds
- Protocols
- Analysis Framework
- Conclusion and Further Reading

Architecture

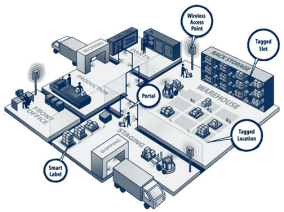
Definition (RFID)

[RFID] means the use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a tag through a variety of modulation and encoding schemes to uniquely read the identity of a radio frequency tag or other data stored on it.



Basic RFID

- Supply chain tracking.
  - Track boxes, palettes, etc.



www.aeroid.co.uk

- Libraries.
  - Improve book borrowing and inventories.

www.rfid-library.com

- Pet identification.
  - Replace tattoos by electronic ones.
  - ISO11784, ISO11785.

www.flickr.com

- Localisation.
  - Children in amusement parks, Elderly people.
  - Counting cattle.

www.safetzone.com

Evolved RFID

- Building access control.
  - Eg. UCL, MIT.
- Automobile ignition key.
  - Eg. TI DST, Keeloq.
- Public transportation.
  - Eg. Brussels, Boston, Paris, ..., Thalys.
- Payment.
  - Eg. Visa, Baja Beach Club.
- Electronic documents.
  - Eg. ePassports.
- Loyalty cards.

Credit: G. Avoine

Credit: G. Avoine

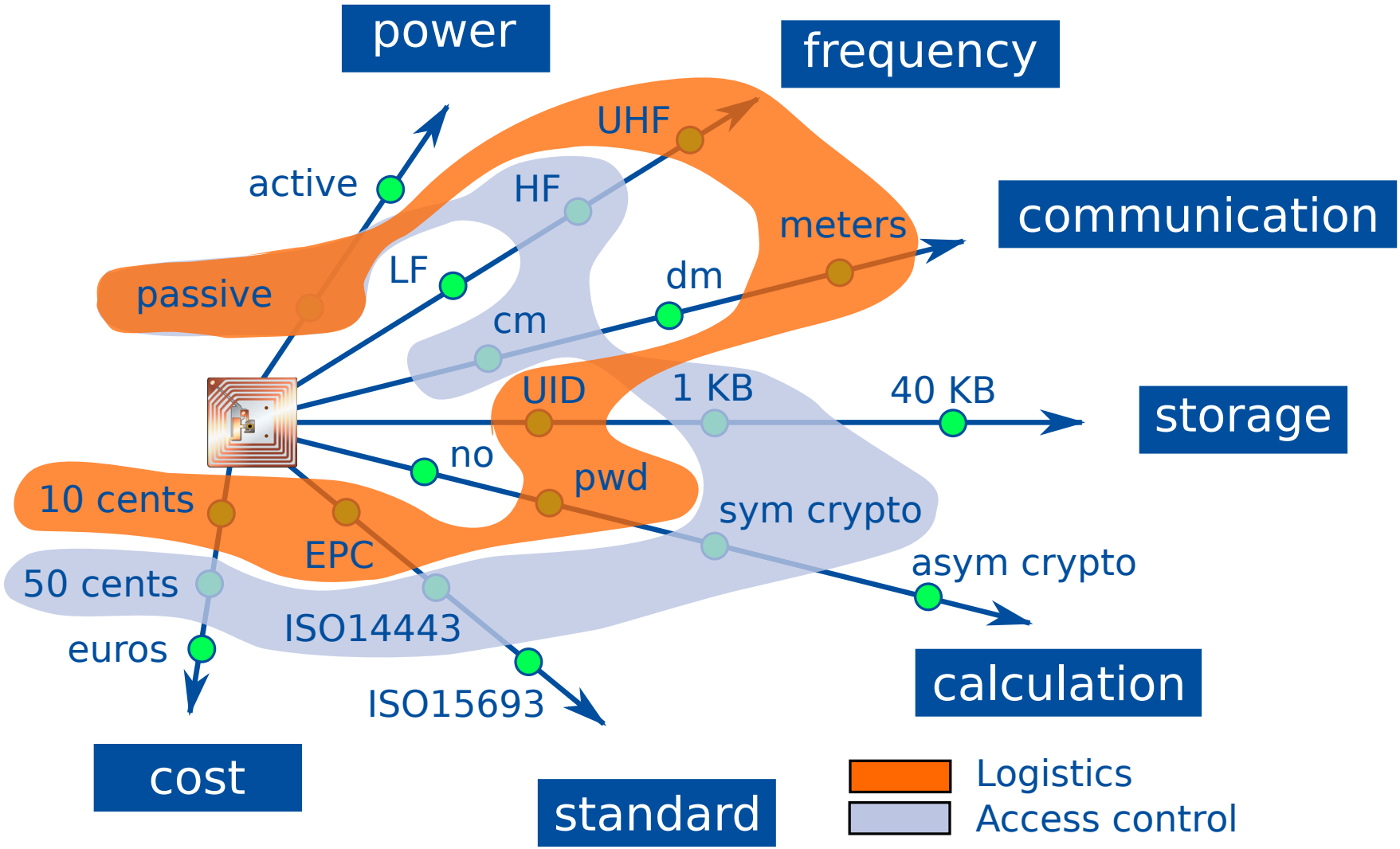
www.carthiefstoppers.com

www.brusselnieuws.be

blogs.e-rockford.com

www.bajabeach.es

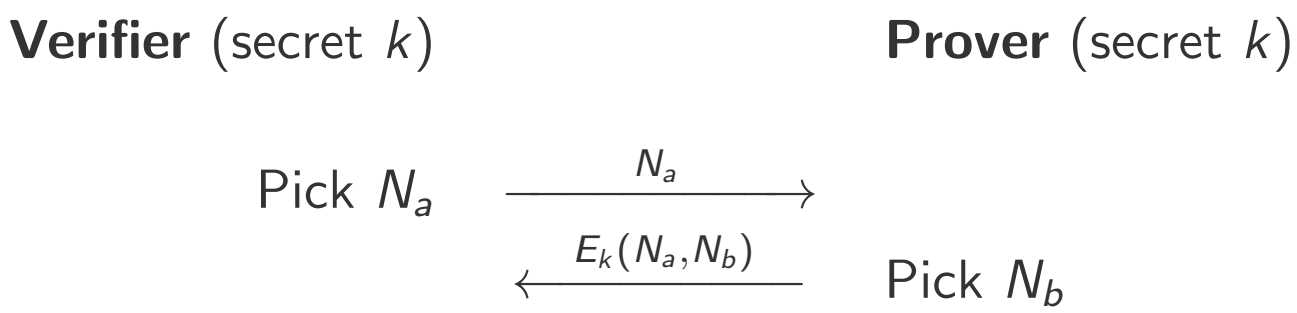
Tag Characteristics



RELAY ATTACKS

- RFID Background
- Relay Attacks
- Countermeasures and Evolved Frauds
- Protocols
- Analysis Framework
- Conclusion and Further Reading

Variant of ISO 9798-2 Protocol 3



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

Relay Attack

Verifier

Adversary ◄·····► Adversary

10000 km

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.

- Reader starts a timer when sending a message.
  - To avoid semi-open connections.
  - The timer is not tight.
- Example: ISO 14443 "Proximity Cards".
  - Used in most secure applications.
  - Standard on the low-layers (physical, collision-avoidance).
  - Default timer is around 5 ms.

- Radio link over 50 meters (G. Hancke 05).
- With some ACR122 (A. Laurie 09).
- With NFC cell phones or over Internet (libNFC).

COUNTERMEASURES AND EVOLVED FRAUDS

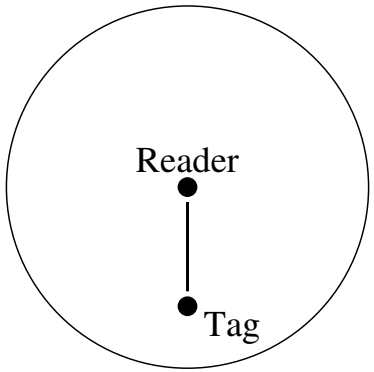
- RFID Background
- Relay Attacks
- Countermeasures and Evolved Frauds
- Protocols
- Analysis Framework
- Conclusion and Further Reading

Protocol Aims in General Framework

Definition (Distance Checking)

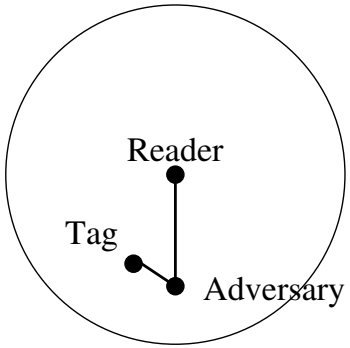
A distance bounding is a process whereby one party is assured:

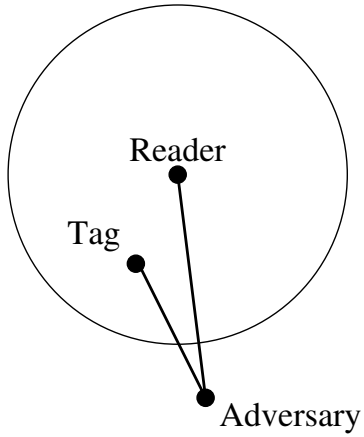
1. Of the identity of a second party,
2. That the latter is present in the neighborhood of the verifying party, at some point in the protocol.



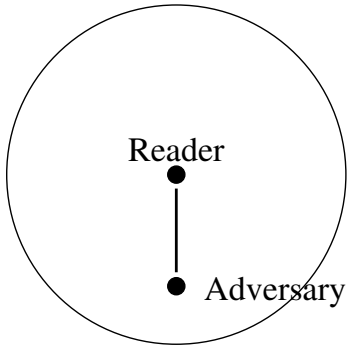
Distance bounding does not avoid relay attacks.

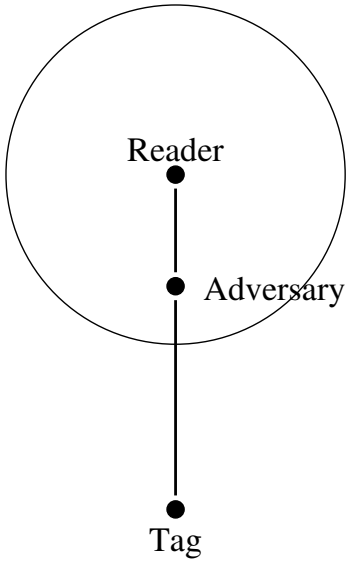
No Fraud

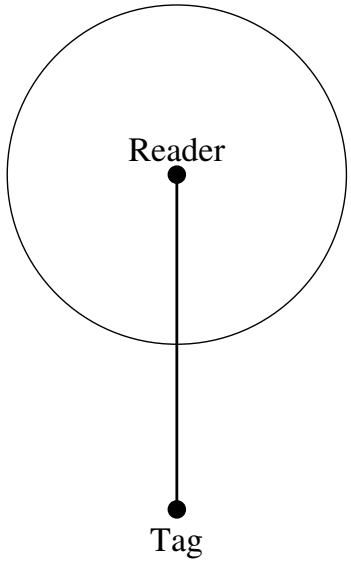


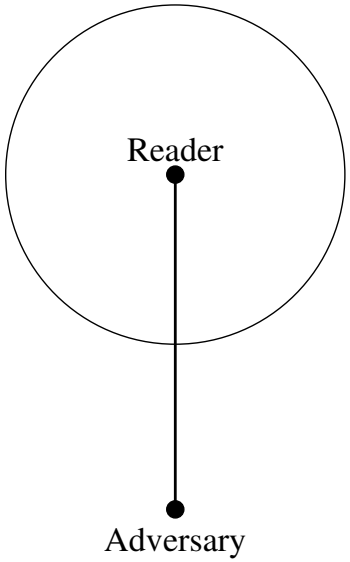


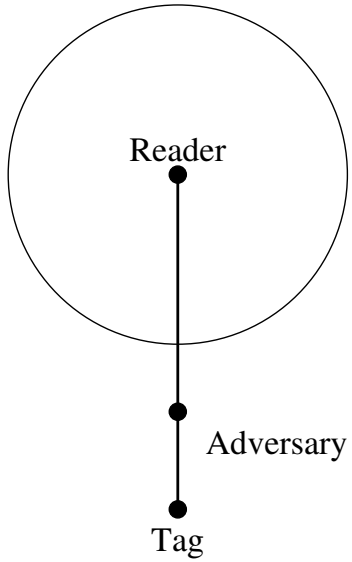
Fraud


Reader
Adversary


Reader
Adversary
Tag


Reader
Tag


Reader
Adversary

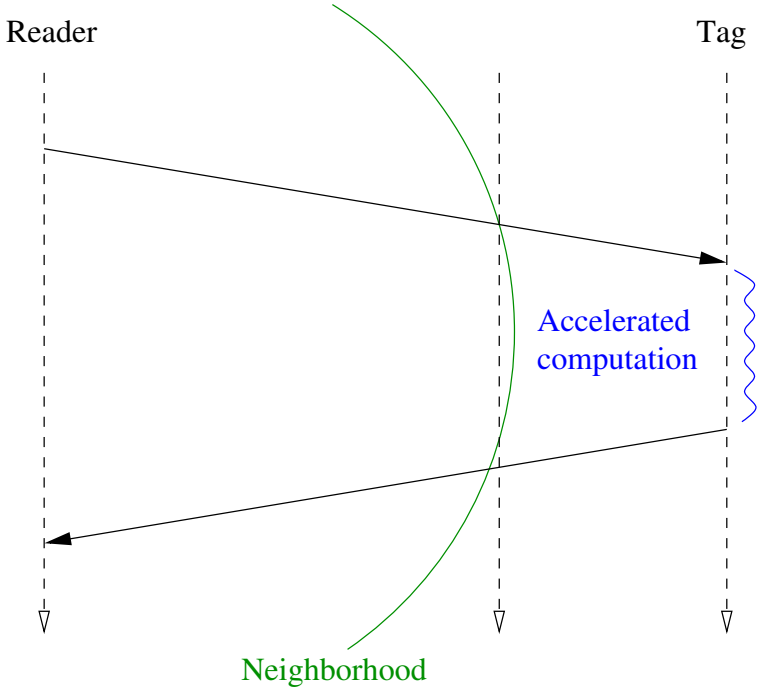

Reader
Adversary
Tag

Measuring the Distance

- Global Positioning System (GPS).
- Received Signal Strength (RSS).
- Round Trip Time (RTT).

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 [Crypto90].



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

Simplified Hancke and Kuhn's Protocol
Description

Reader (secret K)		**Tag** (secret K)
Pick a random N_a	$\xrightarrow{N_a}$	
		$h(K, N_a) = \begin{cases} v^0 = & 1\,1\,0\,1\,1\,0\,0\,0\,1\,0 \\ v^1 = & 0\,1\,1\,1\,1\,0\,0\,1\,0\,0 \end{cases}$
	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

Adversary's success probability (relay attack): 0.

Mafia Fraud

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.

- 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).
- A.k.a., relay attack, chess grandmaster, wormhole problem, passive man-in-the-middle, middleman attack...

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.

Example

Home confinement is a legal measure by which a person is confined by the authorities to his residence. With such a measure where travels are restricted, a distance attack is definitely relevant, in order to allow the person under monitoring to leave his residence without being detected.

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.

Example

The terrorist attack also makes sense in the case of home confinement because the arrested person may benefit from the help of an accomplice who stays close to the monitoring system while the person under control is away. In such a case, a terrorist fraud is needed because the ankle bracelet cannot be removed except by the authorities.

PROTOCOLS

- RFID Background
- Relay Attacks
- Countermeasures and Evolved Frauds
- Protocols
- Analysis Framework
- Conclusion and Further Reading

Theoretical Protocols

- Brands and Chaum (Eurocrypt 1993)
- Hancke and Kuhn (SecureComm 2005)
- Munilla, Ortiz, and Peinado (RFIDsec 2006)
- Reid, Neito, Tang, and Senadji (ASIACCS 2007)
- Singelée and Preneeld (ESAS 2007)
- Tu and Piramuthu (EURASIP RFID Technologie 2007)
- Munilla and Peinado (Wireless Com. and Mobile Comp. 2008)
- Kim, Avoine, Koeune, Standaert, and Pereira (ICISC 2008)
- Nikov and Vauclair (eprint 2008)
- Avoine and Tchamkerten (ISC 2009)
- Kim and Avoine (CANS 2009)
- Peris-Lopez, Hernandez-Castro, *et al.* (arXiv.org 2009)
- Avoine, Floerkemeier, and Martin (Indocrypt 2009)
- ...

HANCKE AND KUHN'S PROTOCOL (2005)

Simplified Hancke and Kuhn's Protocol
Description

Reader (secret K)		**Tag** (secret K)
Pick a random N_a	$\xrightarrow{N_a}$	
		$h(K, N_a) = \begin{cases} v^0 = & 1\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 0 \\ v^1 = & 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0 \end{cases}$
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

Success probability in the following cases:

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

Hancke and Kuhn's Protocol
Description

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

Simplified Hancke and Kuhn's Protocol
Analysis

Question

Success probability in the following cases:

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

ANALYSIS FRAMEWORK

- RFID Background
- Relay Attacks
- Countermeasures and Evolved Frauds
- Protocols
- Analysis Framework
- Conclusion and Further Reading

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. She can also finally relay the final slow phase, if any.

Definition (Post-ask strategy)

The adversary relays the first slow phase. She then executes the fast phase with the verifier without asking the prover. Then, she queries the prover with the correct challenges received during the fast phase. Finally, she relays the final slow phase.

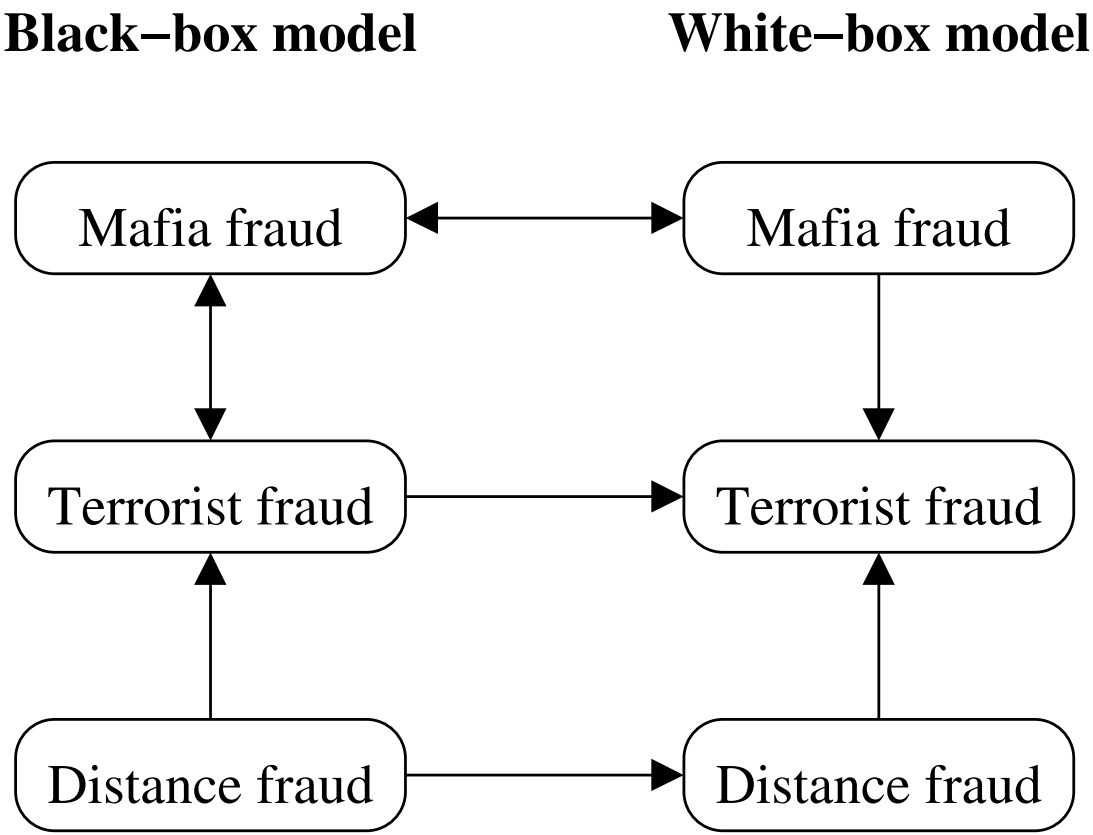
Definition (Black-box model)

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

Definition (White-box model)

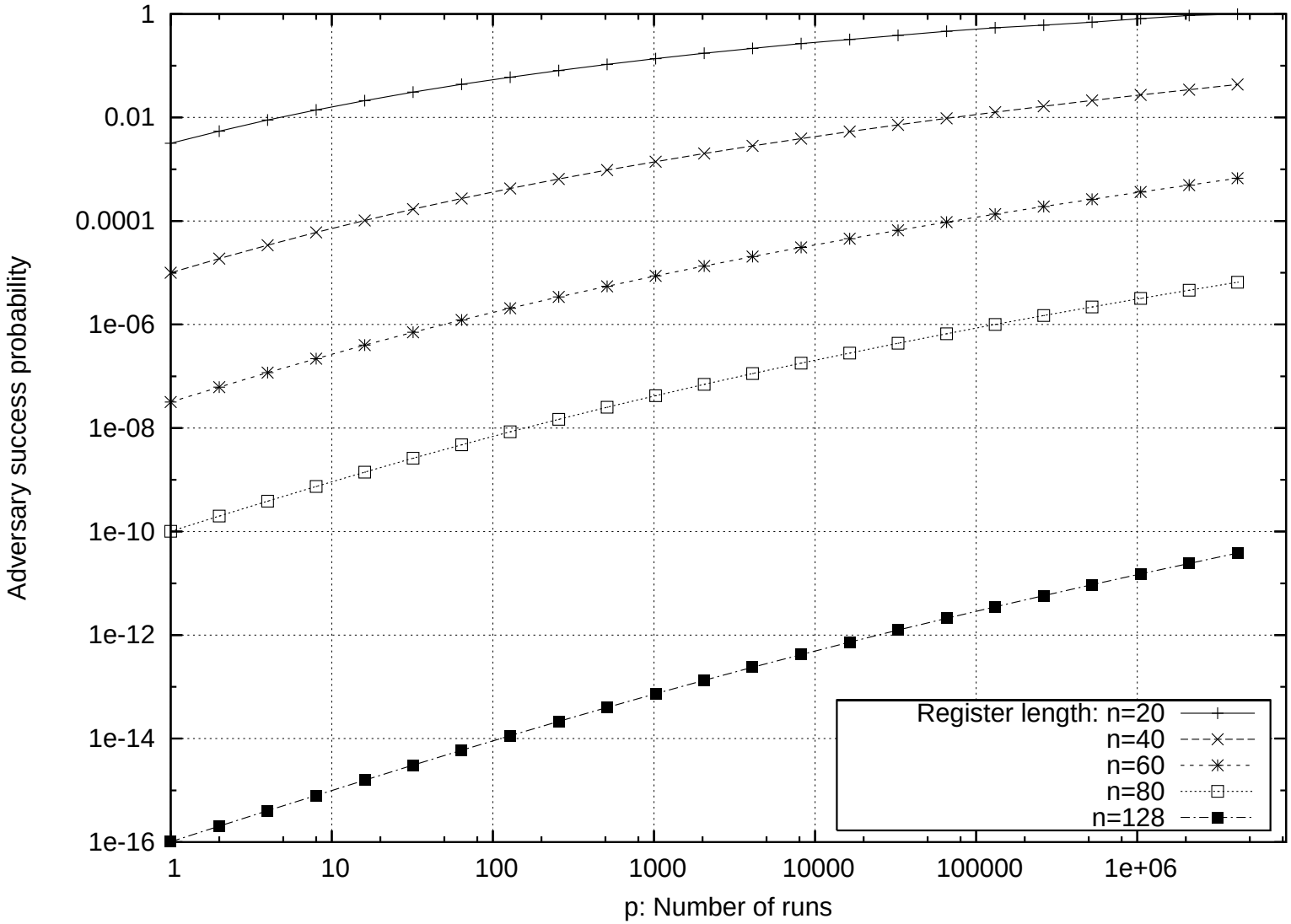
In a white-box model, the prover has full access to the implementation of the algorithm and a complete control over the execution environment.

Relations Between the Frauds and the Models



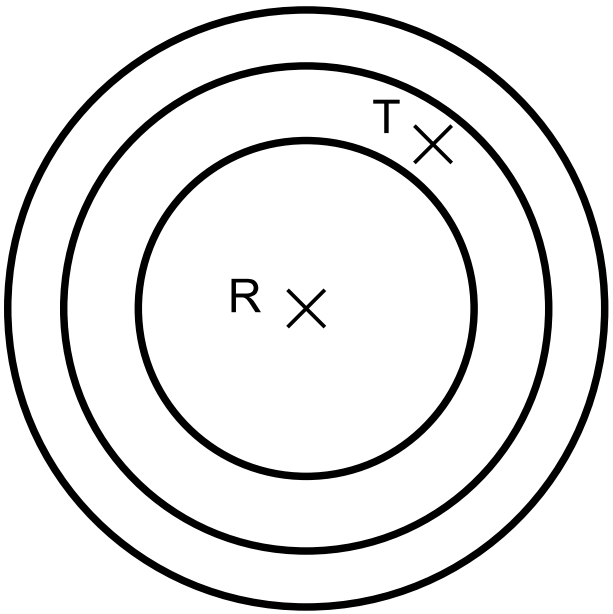
- In the white-box model, restricting the computation capabilities of the prover within one protocol execution is required.
- This computation bound should be provided by the designers of distance bounding protocols and the security analysis should be based on it.

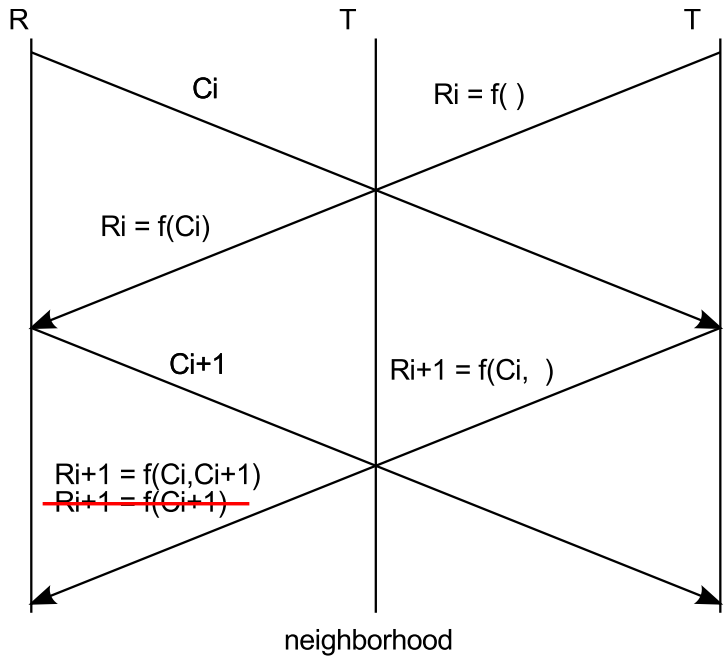
Prover Model
Computing Capabilities of the Prover - Example: HK



Prover Model – Circle Analysis
Distance Between Verifier and Prover

- 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.





CONCLUSION AND FURTHER READING

- RFID Background
- Relay Attacks
- Countermeasures and Evolved Frauds
- Protocols
- Analysis Framework
- Conclusion and Further Reading

- Goal is to decrease the adversary's success probabilities.
  - Resistance to noise.
  - Avoid a final signature.
  - Separate authentication and distance checking.
  - ...
- Theory is far beyond practice.
  - First protocols analyzed with a pedestrian appraoch.
  - What is designed in theory is perhaps not practical.

- Relay attacks are practicable.
- Distance bounding not implemented in commercial products.
  - Propagation delays are much shorter than processing times.
  - The considered time are nanoseconds.
  - What is the practical radius of the neighborhood?
  - Why sending only one bit?
- Mifare Plus contains a kind of distance bounding protocol.
- Mitigating the problem is perhaps enough.
  - Adversary also induces some delays.
  - Thwarting adversaries using commercial readers.
  - Avoiding long-distance attacks.

Further Reading

- Y. Desmedt, C. Goutier, and S. Bengio. Special Uses and Abuses of the Fiat-Shamir Passport Protocol. In CRYPTO'87, vol. 293 of LNCS, pp 21–39, Aug. 1988. Springer.
- S. Brands and D. Chaum. Distance-Bounding Protocols. In EUROCRYPT'93, vol. 765 of LNCS, pp 344–359, May 1993. Springer.
- G. Hancke and M. Kuhn. An RFID Distance Bounding Protocol. In SecureComm 2005, Sep. 2005. IEEE.
- G. Avoine, M. Bingöl, S. Kardas, C. Lauradoux, and B. Martin. A Framework for Analyzing RFID Distance Bounding Protocols. Journal of Computer Security, 2010.