

Distance Bounding: A Countermeasure to Relay Attacks?

Gildas Avoine

UCL/GSI, Belgium

<http://sites.uclouvain.be/security/>

BCRYPT Workshop on RFID Security – February 5th, 2010

Work presented here is partly issued from collaborations with Muhammed Ali **Bingöl**, Christian **Floerkemeier**, Chong-Hee **Kim**, Cédric **Lauradoux**, Benjamin **Martin**, Süleyman **Kardaş**, and Aslan **Tchamkerten**.

- Mise en Bouche.
- Relay Attacks.
- Distance Bounding.
- Hancke and Khun's Protocol.
- Why are there so many Protocols?
- Where do we go?

MISE EN BOUCHE

■ Supply chain tracking.

- Track boxes, palettes, ...



■ Pet identification.

- Replace common tattoos by electronic ones

■ Access control.

- Building, Public transportation.

■ Payment.

- SpeedPass, PayPass,



■ Electronic documents.

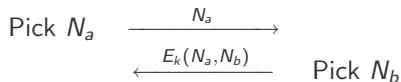
- ePassports, ...



Variant of ISO 9798-2 Protocol 3

Verifier (secret k)

Prover (secret k)



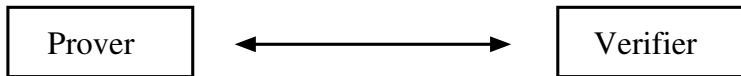
Protocol **secure** under common assumptions on E , k , N_a , and N_b .

Security Particularities of RFID Systems

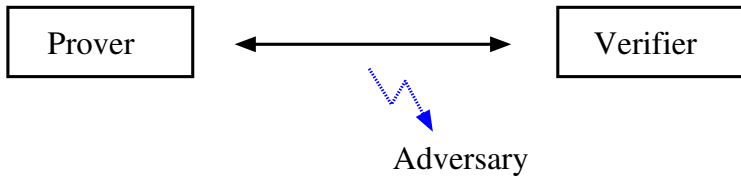
- **Wireless** communication.
 - Easy access to the channel.
- Tags answer **without agreement** of their holders.
 - Implicit agreement = being in the reader's field.
- **Low capabilities** of the tags.
 - Lightweight cryptography, no internal clock.

RELAY ATTACKS

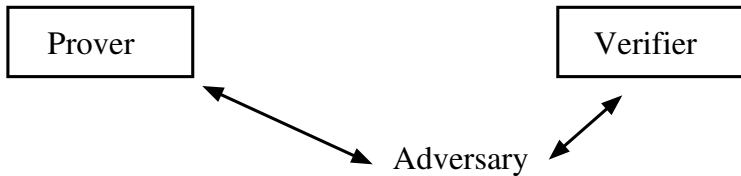
Relay Attack



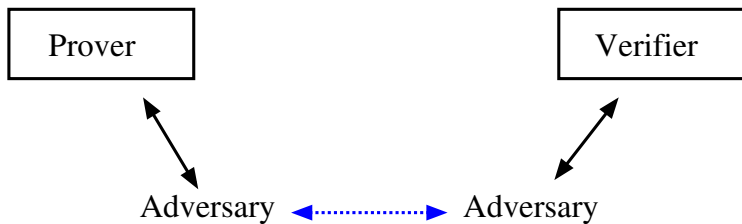
Relay Attack



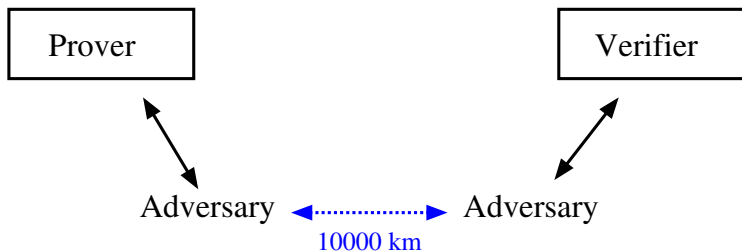
Relay Attack



Relay Attack



Relay Attack



Relay Attack



Relay Attack



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

Do-ability of the Relay Attack

- Successful attacks.
 - Radio link over **50 meters** (G. Hancke 05).
 - With some **ACR122** (A. Laurie 09).

Do-ability of the Relay Attack

- Successful attacks.
 - Radio link over **50 meters** (G. Hancke 05).
 - With some **ACR122** (A. Laurie 09).
- Reader starts a **timer** when sending a message.
 - To avoid **semi-open** connections.

Do-ability of the Relay Attack

- Successful attacks.
 - Radio link over **50 meters** (G. Hancke 05).
 - With some **ACR122** (A. Laurie 09).
- 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**.

Do-ability of the Relay Attack

- Successful attacks.
 - Radio link over **50 meters** (G. Hancke 05).
 - With some **ACR122** (A. Laurie 09).
- 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

Protocol Aims in General Framework

Definition (Authentication)

An **authentication** is a process whereby one party is assured 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 evidence is acquired). [Handbook of Crypto]

Definition (Distance Checking)

A **distance checking** is a process whereby one party is assured that a given property on its distance to a second party involved in a protocol is satisfied at some point in the protocol.

The area where the property is satisfied is called the **neighborhood** of the verifying party.

Definition (Distance Bounding)

A **distance bounding** is a process that consists of an **authentication** combined with a **distance-checking**, where the considered property is an upper-bound on the distance between the two parties.

- Distance bounding does not avoid relay attacks.
- Distance bounding check that the **distance** property between the verifier and the **claimed** prover is verified.
- Proximity check.
- A Distance bounding protocol P is secure if and only if: For all instance of P , P succeeds $\Rightarrow V$ authenticated T and the latter is in V 's neighborhood.
- In **practical RFID** systems, distance bounding thwarts the relay attack.

Definition (Distance Bounding)

A **distance bounding** is a process that consists of an **authentication** combined with a **distance-checking**, where the considered property is an upper-bound on the distance between the two parties.

- Distance bounding does not avoid relay attacks.
- Distance bounding check that the **distance** property between the verifier and the **claimed** prover is verified.
- Proximity check.
- A Distance bounding protocol P is secure if and only if: For all instance of P , P succeeds $\Rightarrow V$ authenticated T and the latter is in V 's neighborhood.
- In **practical RFID** systems, distance bounding thwarts the relay attack.

Definition (Distance Bounding)

A **distance bounding** is a process that consists of an **authentication** combined with a **distance-checking**, where the considered property is an upper-bound on the distance between the two parties.

- Distance bounding does not avoid relay attacks.
- Distance bounding check that the **distance** property between the verifier and the **claimed** prover is verified.
- Proximity check.
- A Distance bounding protocol P is secure if and only if: For all instance of P , P succeeds $\Rightarrow V$ authenticated T and the latter is in V 's neighborhood.
- In **practical RFID** systems, distance bounding thwarts the relay attack.

Definition (Distance Bounding)

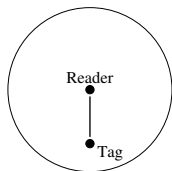
A **distance bounding** is a process that consists of an **authentication** combined with a **distance-checking**, where the considered property is an upper-bound on the distance between the two parties.

- Distance bounding does not avoid relay attacks.
- Distance bounding check that the **distance** property between the verifier and the **claimed** prover is verified.
- Proximity check.
- A Distance bounding protocol P is secure if and only if: For all instance of P , P succeeds $\Rightarrow V$ authenticated T and the latter is in V 's neighborhood.
- In **practical RFID** systems, distance bounding thwarts the relay attack.

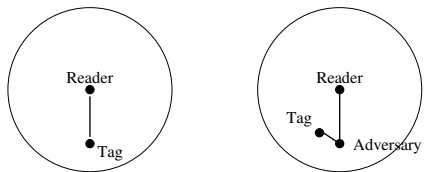
Definition (Distance Bounding)

A **distance bounding** is a process that consists of an **authentication** combined with a **distance-checking**, where the considered property is an upper-bound on the distance between the two parties.

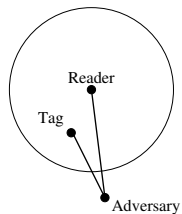
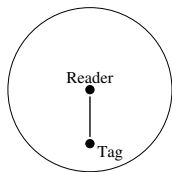
- Distance bounding does not avoid relay attacks.
- Distance bounding check that the **distance** property between the verifier and the **claimed** prover is verified.
- Proximity check.
- A Distance bounding protocol P is secure if and only if: For all instance of P , P succeeds $\Rightarrow V$ authenticated T and the latter is in V 's neighborhood.
- In **practical RFID** systems, distance bounding thwarts the relay attack.



No Fraud

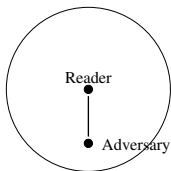


No Fraud

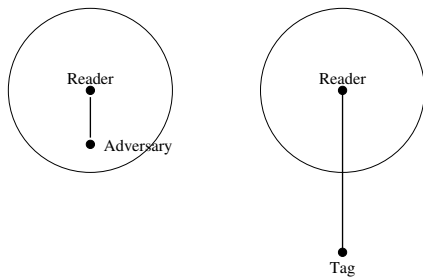


From Attack to Fraud

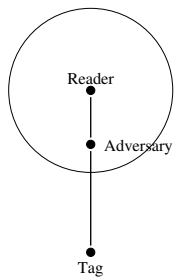
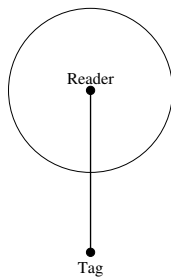
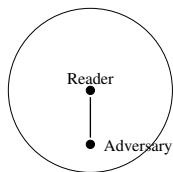
From Attack to Fraud



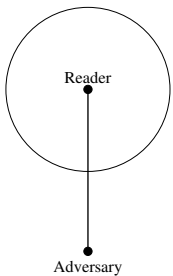
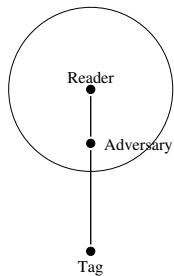
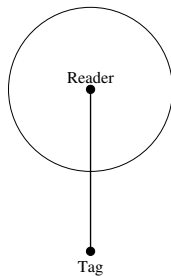
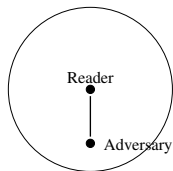
From Attack to Fraud



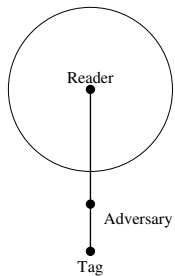
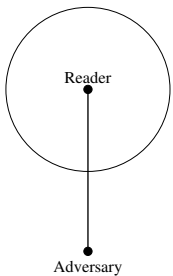
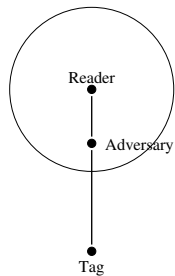
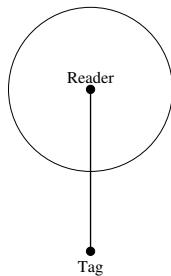
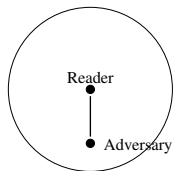
From Attack to Fraud



From Attack to Fraud

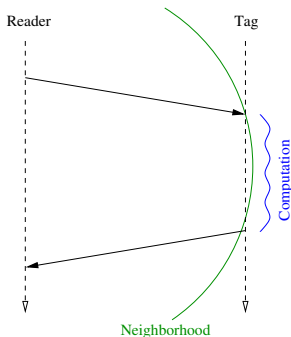


From Attack to Fraud



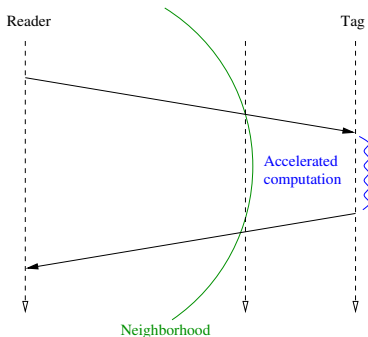
Distance Bounding Based on the Speed of Light

- Measure the **round-trip-time** (RTT) of a given message.
 - Provide a bound on the distance (proximity check).
 - Idea introduced by Beth and Desmedt [Crypto90].



Distance Bounding Based on the Speed of Light

- Measure the **round-trip-time** (RTT) of a given message.
 - Provide a bound on the distance (proximity check).
 - Idea introduced by Beth and Desmedt [Crypto90].



- 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

Hancke and Kuhn's Protocol

Reader
(secret K)

Pick a random N_a



Tag
(secret K)

Pick a random N_b

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

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

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



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

Stop Clock



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

End of fast bit exchange

Adversary's Success Probabilities

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

Adversary's Success Probabilities

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

Adversary's Success Probabilities

- Mafia Fraud: $(\frac{3}{4})^n$.
- Terrorist Fraud: 1
- Distance Fraud: $(\frac{3}{4})^n$.

**WHY ARE THERE SO MANY
PROTOCOLS?**

Why so Many Protocols?

- Goal is to decrease the adversary's success probabilities.
- Goal is to add new features.

Goal is to add new features

- Resistance to noise.
- Avoid a final signature.
- Separate authentication and distance checking.
- And probably more. . .

Decrease Adversary Success Probability

- Trade-off prob. vs computation complexity.
- Trade-off prob. vs memory (eg. Avoine-Tchamkerten).
- Trade-off prob. vs symbol size (bits) (eg. Munilla-Peinado).
- Trade-off mafia fraud vs distance fraud (eg. Kim-Avoine).
- And probably more. . .

WHERE DO WE GO?

Goal is to add new features

- *“I believe this puts an end to RFID distance bounding protocol”* (anonymous reviewer).
- Not the end of the story, just the beginning!

Goal is to add new features

- *“I believe this puts an end to RFID distance bounding protocol”* (anonymous reviewer).
- Not the end of the story, just the beginning!

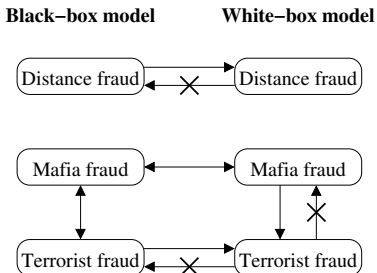
- Are distance bounding protocols **practicable**?
- Can we reach a unified **framework**?
- Which **parameters** can be modified?

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



- An **arrow** from A to B (scenario,model) means: if there exists an attack in A that succeeds with probability p_A , then there exists an attack in B that succeeds with probability p_B s.t. $p_B \geq p_A$.
- A **crossed out arrow** means that the implication is false.

Adversary Strategies

- **No-ask strategy.** The adversary does not interact with the prover during the attack.
- **Pre-ask strategy.** The adversary queries the prover before he starts the fast phase with the legitimate verifier.
- **Post-ask strategy.** The adversary queries the prover after the verifier stops the fast phase. This strategy only makes sense if a final slow phase exists.

The parameters

- What is the practical radius of the neighborhood?
- Why sending only one bit?
- Is it more expensive to send $1 \times n$ bits than $n \times 1$ bit?
- Shall noise really taken into account?
- And many many other practical questions...

CONCLUSION

- Distance Bounding: a Countermeasure to Relay Attacks?
- Unified framework needed.
- Move to practice.

Come-back to the Title of the Talk

- Distance Bounding: a Countermeasure to Relay Attacks?
- Unified framework needed.
- Move to practice.

- Distance Bounding: a Countermeasure to Relay Attacks?
- Unified framework needed.
- Move to practice.

- RFID Security and Privacy **Lounge**:
 - <http://sites.uclouvain.be/security/>
- RFID Security and Privacy **Training Week**:
 - <http://sites.uclouvain.be/security/rfidtraining.html>