Chapter 4

Implementation of a Countermeasure to Relay Attacks for Contactless HF Systems

Pierre-Henri Thevenon and Olivier Savry

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/53393

1. Introduction

Nowadays, HF contactless technologies following the ISO 14443 standard are extensively used worldwide. Critical applications like access control or payment require high security guarantees. However, contactless channels are less secure and offer more opportunities for any kind of intrusion than other ways of communication; e.g. eavesdropping and contactless card activation using false reader [1, 2, 3, 11]. Among the attacks on the physical layer, relay attack is the most dangerous because of its simplicity, its impact and its insensitivity to cryptographic protections. It consists in setting up an unauthorized communication between two devices out of their operating range [4, 6]. On Figure 1, two attackers are able to create a link between the reader and the contactless card without the agreement of the owner. A relay is composed of two elements: a first one close to the reader and called proxy, a second one close to the card and called mole. These two elements communicate together by a wired or a wireless link

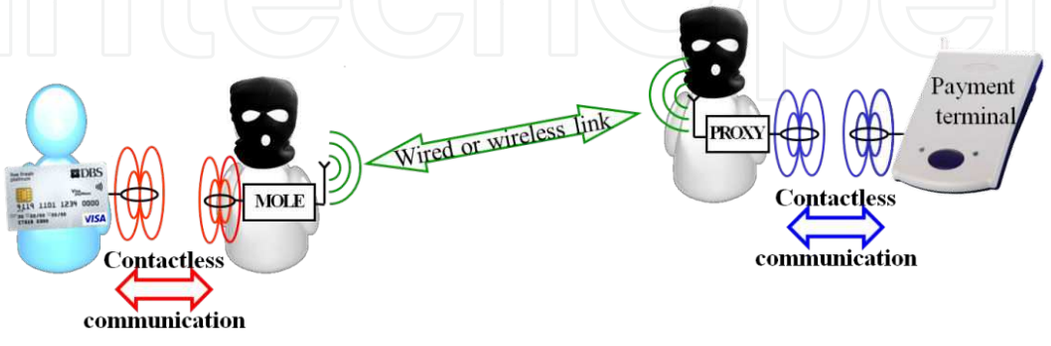

Figure 1. Relay scenario in a queue

A relay attack is thoroughly transparent for current contactless systems and cryptographic protocols. A possible countermeasure is the distance bounding protocol which can add an upper bound for the distance between the two communicating devices.

In this chapter, we will first assess the potential of relay attacks by implementing them and by keeping in mind the concern of introducing a delay as low as possible. Indeed, this time remains the only detectable feature of such an attack and the existing countermeasures rely on its accurate assessment.

The delay constraint guides us towards the development of three kinds of relay: a wired passive relay, a relay based on a wireless super-heterodyne system and a wireless relay with a complete demodulation of the signal. Our experimental results show that those cheap devices introduce really low delay from 300 ns to 2 μs jeopardizing the use of current distance bounding protocols. A more adapted solution will then be implemented and addressed in the second part of the document. It modifies the stage of the distance bounding protocol which uses the physical layer to carry out a delay assessment with a correlation in the reader between the received signal and the expected one. Finally, a security analysis will be performed and improvements will be discussed.

2. Relay attacks

2.1. Related work

The relay attack is based on the Grand Master Chess problem described by Conway in 1976. The latter shows how a person, who does not know the rules of this game, could win against one of two grand masters by challenging them in a same play. The relay attack is just an extension of this problem applied to the security field. By relaying information between a reader and a card outside the reader field, an attacker can circumvent the authentication protocol. This attack needs two devices: a mole and a proxy. The mole pretends to be the true reader and exchange data with the proxy which pretends to be the true card.

The larger the distance between the different elements is, the more efficient is the relay. Typical maximum distances between the reader and the proxy or between the mole and the card are roughly 50 cm. The distance between the mole and the proxy is not limited; it just depends on the chosen technology [5].

By using a relay, an attacker can transmit requests and answers between an honest reader and an honest card separated by 50 metres [6]. Many communication channels can be used to link the mole and the proxy like GSM, WIFI or Ethernet [8]. The delay, introduced by such a relay is more than 15 μs. At the physical layer, this attack is the most dangerous for many reasons:

- The card is activated and transmits information when it is powered, without the agreement of the victim. Anyone can be a victim because the attacker has just to be close enough to control your card like in a crowd.

http://dx.doi.org/10.5772/53393

- The attack occurs on the physical layer i.e. the relay transmits coded bits without knowledge about the frame significance. The ISO9798 standard presents an authentication protocol to prove that the contactless devices involved in the communication share the same secret key. For eavesdropping or skimming attacks, the use of this kind of protocol limits the risks. For the relays attacks, knowing the key is not necessary. Actually, a relay does not neither modify the information of the frame nor has to know its meaning. It just transmits the data. The encrypted data are transmitted as plain text.
- Contactless standards such as standard ISO14443 impose timing constraints in order to synchronize data sent by many cards at the same time, especially during the anti-collision protocol. However, these constraints are not enforced by the majority of cards [9]. These requirements would complicate the relay attack if they were really applied. Another weakness of the standard is the time delay between the reader request and the card answer. These time delay is not only such long but also expandable by the card and consequently by an attacker.

2.2. Presentation of relay attacks

The delay in current relays is mainly due to the use of components such as microcontrollers or RFID chips. This kind of components is used for the reconstruction of the decoded signals. So, the original signal becomes compatible with other protocols, like Wifi or GSM, used in the wireless communication between the mole and the proxy. All these signal processes lead to the addition of delays in the relay. They can be considerably lowered by the only use of analog components. Attack scenarios with wired relays must then be considered because they can induce very low delays. Moreover, this kind of relays is simple to realize, with few cheap components. Even if they seem to be unlikely, they can be effective in a queue for example or if they are hidden in the environment.

2.2.1. Passive wired relay

Fig. 2 depicts a simple design of a relay which introduces a very low delay close to a period of the carrier 13.56 MHz. This relay does not require an amplifier or other active components. The coaxial cable between the two antennas can be longer than 20m. Such a system is very low cost; the attacker needs a piece of PCB, few components for the matching and a coaxial wire. Overall cost is a few dollars at most. We claim that wired relays are the simplest and fastest relays by design and as a consequence, they should challenge the approaches of countermeasures which only parry the largest delays.

2.2.2. Relay based on a wireless super heterodyne system

This relay, shown on fig. 3, is quite similar to the relay attack developed by Hancke because it is not restricted by a wired link. Contrary to Hancke's relay, our wireless relay does not use digital components like microcontrollers or RFID chips to process the signal. The delay induced by this relay should be shorter. To do so, the reader signal of frequency fc is mixed with another signal of frequency F, generated by a local oscillator. It results a signal of frequency fc+F, easier

Figure 2. Potential use of a wired relay

to amplify and to send further. A PLL is used as a local oscillator to have the same frequency in the modulation and demodulation circuit.

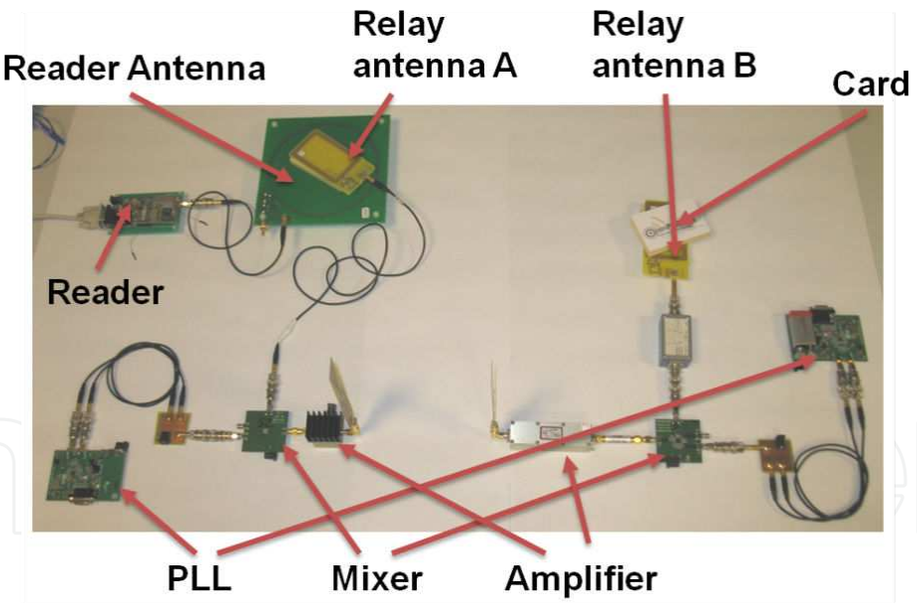

Figure 3. Forward wireless relay

2.2.3. Relay with demodulation of the signal

We have developed a more advanced relay (Fig. 4) close to those realized by Hancke or Kasper.. To realize a relay which demodulates the signal is more complex for an attacker, because it must have a perfect knowledge of the contactless standards. Our system is compliant with the

http://dx.doi.org/10.5772/53393

ISO14443-A standard to be compared with literature relays. However, it can be adapted to a different contactless standard such as ISO15693 or ISO14443-B.

The proxy is mainly based on thus developed by Carluccio et al. [7]. This electronic card can be divided into two subsystems: one for demodulation and decoding of the reader signal and one for the load modulation of the card.

The Mole is based on a reader developed in our laboratory. This device has a RF front-end RF which allows amplitude modulation and demodulation. The heart of the mole is a FPGA which separates the phase of emission and reception phase. The proxy signal is processed by the FPGA of the mole; it is coded in modified Miller and modulated in OOK. The HF signal is then amplified and injected in the antenna. The victim's card understands the request of our Mole as a frame from a standard reader and answers by modulating its load. This signal is firstly processed by an analog system and then sampled, demodulated and decoded by the FPGA.

The proxy and the mole communicate together through a wireless system. We have used chips used in the video/audio wireless transmission systems since they allow a sufficient bit rate of 212kbits/s.

The datasheet of video transmission systems provides a theoretical distance operation of 100 metres. In practice, problems of propagation in a building must be taken into account but this distance is sufficient to realize the attack in a shop. Based on experiments realized with the relay, we have obtained a maximum distance of 10 cm between the card and the mole but also between the proxy and the reader.

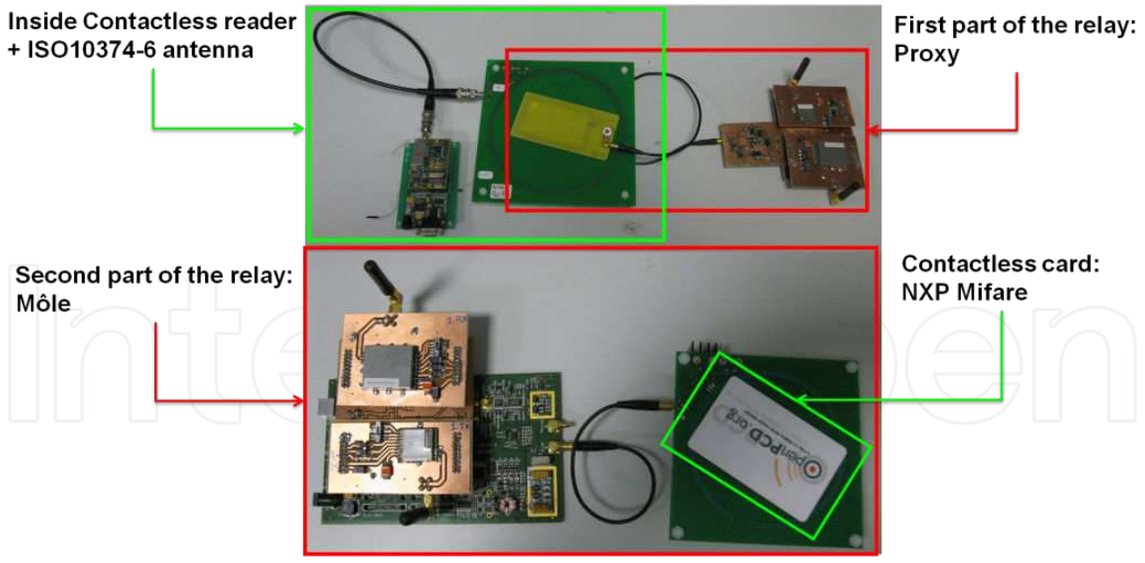

Figure 4. Relay with demodulation of the signal

2.3. Experiments on introduced delay

This experiment is performed to measure the introduced delays of the different relays. To do so, a reader sends a fixed sequence through a relay. With an oscilloscope, this sequence is

recorded directly on two calibration coils located close to the two relay antennas. This sequence is a signal modulated in amplitude with a subcarrier at 848 kHz. The cross-correlation of the two recorded signals allows the computation of the temporal shift between them. In this experiment, we assume that the delay is the same for the forward and the backward channel so the results are the double of the value which is computed.

Fig. 5 gives an overview of the computed delays. Each type of relay is characterized by a temporal distribution. The delay introduced by the relay can be used to detect the presence of a relay. Wireless relays and wired relays have roughly the same delays because the mix of the signals is very fast in the case of the wireless relay. The relay with demodulation introduces a delay 7 times inferior to Hancke's relay.

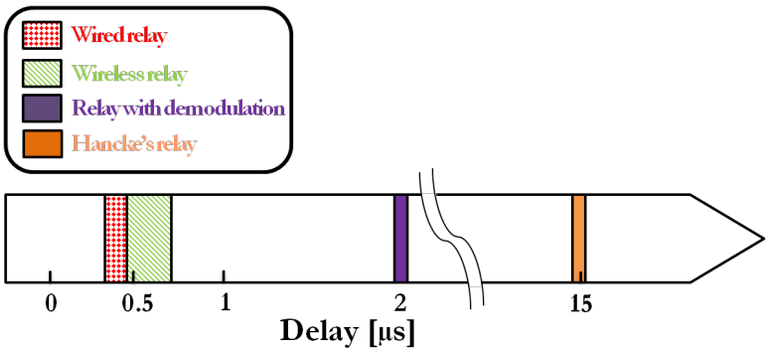

Figure 5. Measured delays

3. Countermeasures

In this part, we first describe the main existing relay detection systems and have a critical look to these solutions. Then, a new protocol based on the correlation, is described and implemented on a real contactless system.

3.1. Existent countermeasures and weaknesses

As mentioned before, design of a suitable countermeasure against relay attacks is a veritable challenge. This is partially because cryptography has no effect on it. Currently, there are few methods to detect relay attacks: distance bounding protocols, countermeasures based on timing measurements or physical structures implying the denial of service of the card.

3.1.1. Distance bounding protocols

In 2003, Hancke et al. have presented the first distance bounding protocol designed for contactless systems [11]; it is based on Brands and Chaums description [10]. Since then, many others distance bounding protocols have been published to improve the security of the scheme.

http://dx.doi.org/10.5772/53393

However, if they have been designed to use the physical layer of the system, they never have been implemented and tested in the HF band.

Distance bounding protocols are used to detect additional delays introduced by a relay during a transaction between two devices. This kind of protocol is often divided into three stages. In such a protocol, the card, named prover, must convince the reader, named verifier, that they are close to each other. During the first stage, the verifier and the prover exchange encrypted sequences, used during the second stage. While, the second stage consists of a timed exchange between the prover and the verifier, in order to verify the card's location. This analysis is made by measuring the time between the request of the verifier and the response of the prover. The last stage is an authentication and verification. The verifier computes and checks the measured times to define the location of the prover and analyses the prover answers to verify its honesty.

The reliability of such protocols depends mainly on the physical layer; the communication channel during the exchange stage affects the accuracy of the propagation time measurements. However, Hancke et al. and recently Rasmussen et al. are the only authors who gave a number of indications related to the protocol implementation at the physical layer level [13]. Other authors claim the merits of their distance bounding protocols such as cost, complexity, reliability but none of them has treated the problem of the protocol implementation for a contactless system.

Such discussions and analysis may be proposed before further works on these protocols.

Distance measurements based on the use of electromagnetic and acoustic waves are used in many applications such as radars. The distance resolution is inversely proportional to the bandwidth; this relation shows one of the weaknesses of distance bounding protocols implemented on a contactless or UWB communication channel:

These two communication channels use electromagnetic waves which have celerity close to the speed of light. In a contactless system, the distance between the verifier and the prover is smaller than 10 cm. Propagation time is then smaller than 300 ps. The first assumption of distance bounding protocol is that the processing time of the signal is assumed to be much smaller than the propagation time of the signal transmitted between the two parts, so smaller than 300 ps.

- HF communication channel: For a contactless system with a bandwidth of 848 kHz, the spatial resolution is around 350 m. Such resolution is too weak to measure a distance between two communicating entities. Moreover, establishing time in HF antennas, processing time for modulation and demodulation take too much time to measure small delays
- UWB communication channel: The bandwidth of a UWB system is equal to 20-25% of its central frequency. The spatial resolution is then close to 1.6 m for a 1GHz UWB system. Such resolution is suitable to detect any kind of relays. However, UWB implementation on an HF contactless system is complex. Hardware constraints are required such as the modification of all RF front-end: add of electrical antennas and specific modulation and demodulation systems.

To summarize, distance bounding protocols are really difficult to implement since the use of the UWB adds cost and complexity. By using HF communication channel, the propagation time remains difficult to isolate because it can be small compared to the processing time. To consider the constraints imposed by the physical layer of HF contactless systems is a priority for developers of algorithms against relay attacks

3.1.2. Solutions based on time measurements

Reid et al. have proposed a solution allowing the measurement of the time duration between the end of the request and the start of the reply [9]. For that, the authors have identified two reference points which represent the state change of the system. In theory, this system can measure average delays of 300 ns; this resolution is 50 times smaller than the delay introduced by Hancke's relay. This counter-measure can be accurate enough to avoid relay attack. However, some problems remain:

- The card does not always reply at the same time;
- No protocol authentication are implemented;
- The signal processing can increase the duration of the delay;
- The attacker can act on the relay to disturb the counter measure.

Munilla et al. have proposed a protocol based on the ISO14443-A standard [10]. In this solution, the reader measures the delay between its request and the card answer. It computes the number of carrier periods between the end of its synchronization bit and the time when the carrier becomes stable after the card response. The authors concluded that their protocol can be used to detect simple relay attacks which induced delays lower than 1 μs. However, this resolution is inefficient against distance fraud attack. Moreover, this countermeasure imposes the modification of standards and of the physical layer. In this solution, the carrier is switched off regularly so the card cannot be powered during this time.

3.1.3. Solution based on the denial of service

The literature provides some examples of solutions that enable the card's holder to disable their card temporarily [1, 18]. The easier solution is a wallet made of metallic sheets, which acts as a faraday cell. Reference [17] presents physical structures which enable the card's holder to turn off their card by separating the chip and the antenna.

3.2. Our solution

This part describes a new protocol compliant with contactless standards which authenticates the two communicating parties. A first implementation of this countermeasure on a real contactless system demonstrates its reliability.

http://dx.doi.org/10.5772/53393

3.2.1. The proposed scheme

The main objective of this countermeasure is to detect relay attacks by measuring the delay introduced by them by using the correlation method.

The first assumption of our protocol is not based on the propagation time but on the complete delay between a triggering pulse of the reader and the answer of the card received by the reader. This delay is different when a relay is inserted between the reader and the card. For an easier understanding of the solution, we suppose that the forward and backward times induced by the relay are the same to make the explanations easier. In this solution, a recorded sequence is correlated with the same sequence sent by the card. The solution is based on an authentication of the card and the measurement of delay induced by a potential relay, as shown in the fig. 6 and the fig. 7. Our protocol is similar to the distance bounding one; it could be divided into three stages: initialization, time measurement and verification.

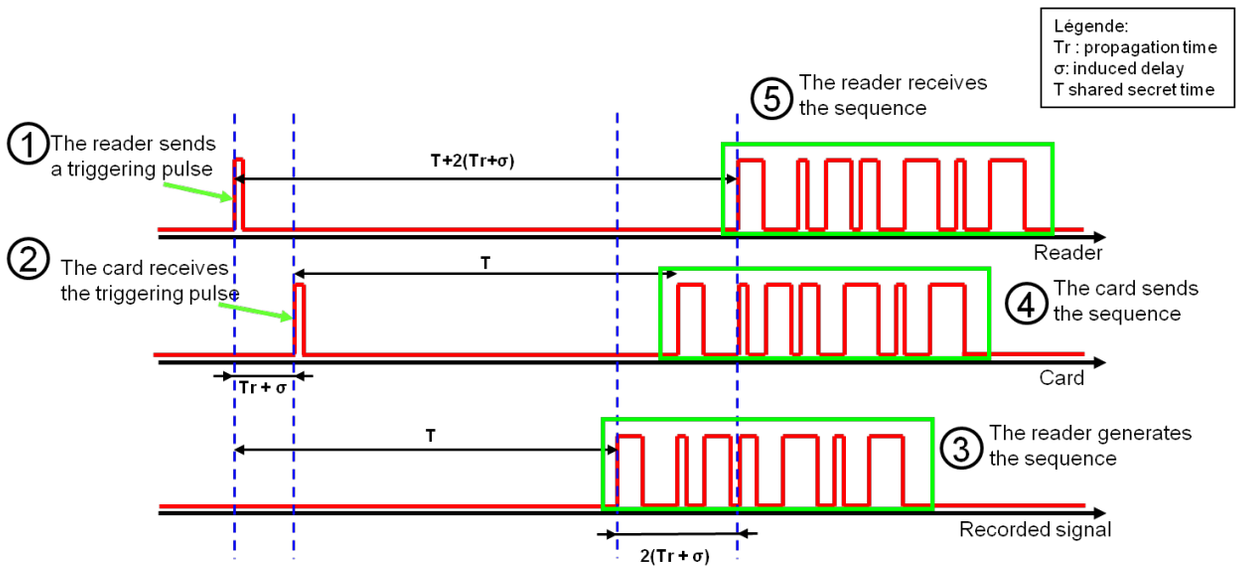

Figure 6. Time measurement stage in the proposed protocol

The first part of our protocol starts by the sending of a nonce from the reader to the card. The reader and the card use any validated symmetric lightweight cryptographic algorithm E, a shared key k and an exchanged random number to calculate T, the waiting time before the sending of the card answer and S, the sequence send by the card and synthesized in the reader. Hence, the computation of T and S by the reader and the card allows the authentication of the card. The first objective of our solution is to detect the relay so there is no mutual authentication in this protocol. However, few modifications of our protocol are possible to have this option.

After the exchange of the random sequence, the second stage starts (fig. 6). A random number of clock cycles after the end of the request frame, the reader modulates briefly its field to create a synchronization pulse. This pulse is received by the card with a delay function of the propagation time Tr and the delay induced by the uplink relay σ. It acts as a start point of the protocol for the reader and the card. Once the triggering pulse is received, the card has to send

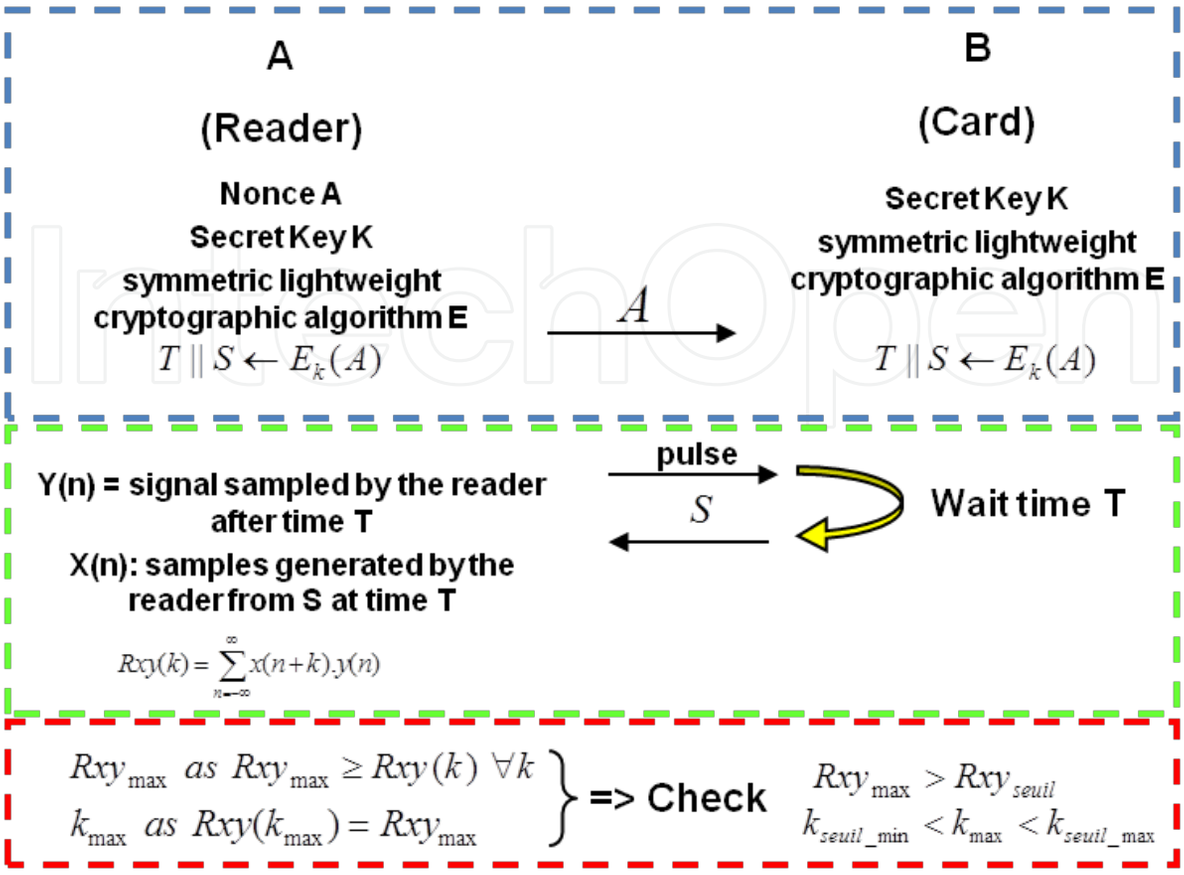

Figure 7. The proposed protocol consists of three stages. The first stage calculates two pseudorandom numbers, using a symmetric cryptographic algorithm and a secret key k and an exchanged nonce. The second stage is time critical as the card has to answer one of the generated pseudorandom sequences, a time T after a synchronization pulse. The third is the verification of the relay presence

the sequence S after a time duration T measured from the synchronization start by using its load modulation. The time duration between the reader request and the card answer is usually sufficient to send this sequence. The reader received the sequence S with a delay from its sent synchronization. This delay depends strongly on the delays introduced by the uplink and downlink relay. A time T after its synchronization pulse, the reader synthesizes the sequence S as it was sent by the card but without any delay. The received sequence S from the card is sampled by the reader after a time T from the triggering pulse to synchronize the samples Y(n) from the card answer and the sample X(n) from the synthesized sequence of the reader.

During the verification stage, the reader correlates the two recorded sequences X(n) and Y(n) to determine the delay between the two sequences. The index corresponding to the maximum value of the correlation is the number of samples of the delay. This number and the maximum correlation value are used to determinate the presence of a relay in the reader field.

http://dx.doi.org/10.5772/53393

3.2.2. Experiments and results

This part presents the first results of correlation based on our solution implementation. The solution is implemented on an "open" reader and contactless card that we developed, illustrated in fig. 8.

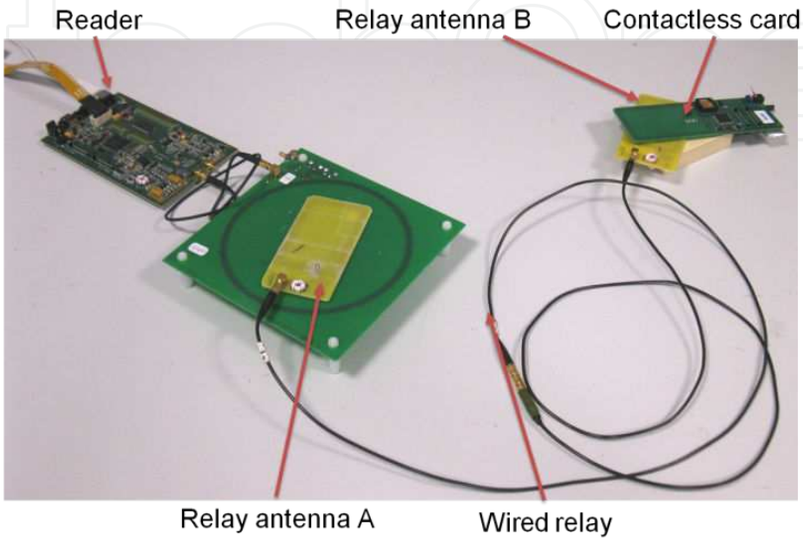

Figure 8. Experimental setup with an open reader and an open card in the presence of a wired relay.

The objective of our experiment is to demonstrate that the computed delay depends on the relay. We perform our four scenarios: one without relay, the others with the three relays studied previously.

Based on 2000 delay values taken in presence or not of a relay and for different distance between antennas, we compute the distribution of these four cases.

This first implementation of a cryptographic protocol based on the physical layer gives interesting results. The chart on fig. 9 shows three different histograms: one for each implemented relay (the wired relay and the fastest wireless relay) and one in the case without relay. These first results prove the efficiency of our solution since it is able to detect a relay with the help of the maximum delays occurred in a classical contactless system. Only relay designed by us are tested but we assume that delay induced by these relay are close to the theoretical minimal delay induced by the most critical relay. Then, we can claim that our solution can detect the most existed relay attacks.

3.3. Discussion

The objective of this discussion is the analysis of the security and the privacy of this solution.

Card cloning and replay attacks with a false card could not be authenticated by the reader and the threat will be detected. In fact, the card must compute two random binary sequences during the first stage of our protocol. The result of this computation is checked during the second

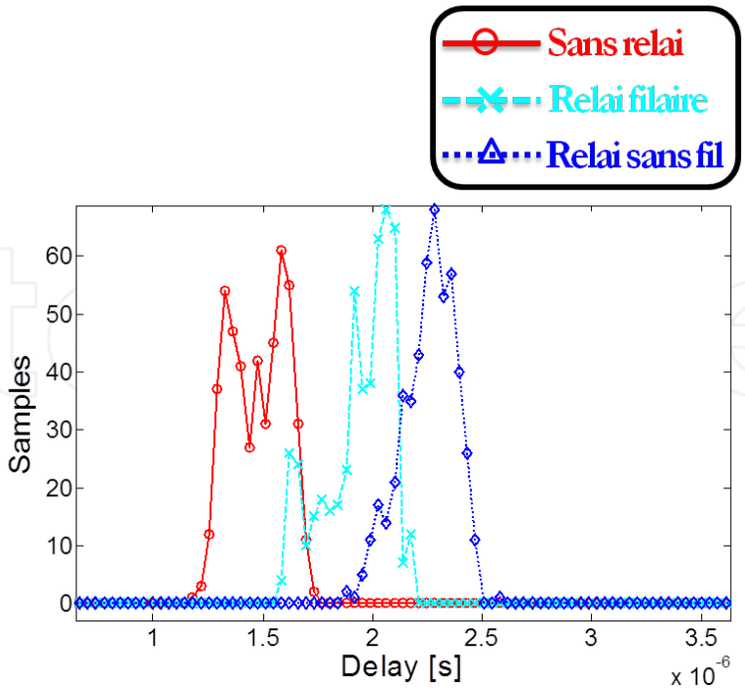

Figure 9. Delay distribution with our solution for each case (with one of the two most critical relays or without relays) for different distance between antennas.

stage. A false card could not send the correct sequence at the correct time to the reader because they depend on the knowledge of the secret key k.

In the case of distance bounding protocols, the security is analyzed by exposing the protocol to three different attacks. Our solution can be exposed to the same attacks to detect possible weaknesses.

3.3.1. Distance fraud

The scenario of this first attack requires a true reader, named verifier, and a false contactless card, named prover. The prover must convince the verifier they are close to each other when it is outside the communicating range. Firstly, this attack is only theoretical in the domain of contactless systems since no author implements this attack. Thus, the prover authenticates the card during the challenge; a corrupted card will be detected (see above). The detection of distance fraud attacks depends on the delays introduced by a modified card.

3.3.2. Mafia fraud

In the mafia fraud attack, the attacker does not perform any cryptographic operations based on the security protocol, and only forwards the challenges and the responses between the honest prover and the honest verifier: it is the standard relay attack.To convince the verifier and the prover they are close to each other, the relay can speed up the clock of the carrier to improve the response time of the prover answer [14]. The received signal will be compressed and the correlation value will be weaker so this attack will be detected. In the same way, the

http://dx.doi.org/10.5772/53393

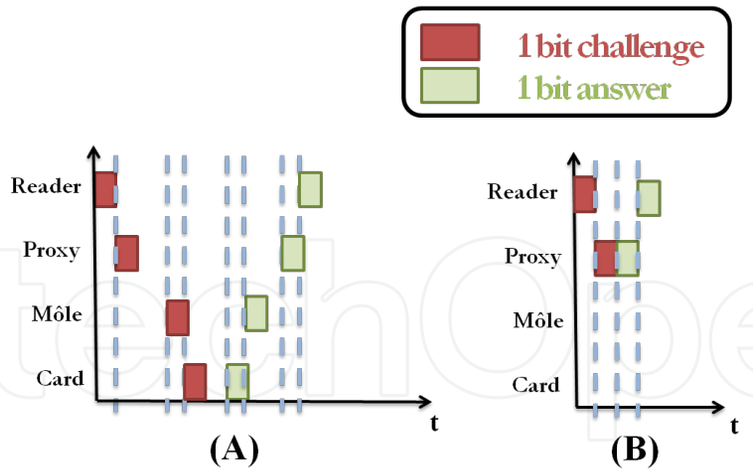

Figure 10. Noisy environment (A) classical case (B) Case with the anticipation of the answer

relay can not anticipate the synchronization pulse of the card because the pulse position in the time is random. Our protocol is resistant to the mafia fraud.

3.3.3. Terrorist fraud

This attack is similar to the previous one, the only difference is that the contactless card and the relay cooperate to mislead the reader. This attack is possible if the protocol does not guarantee a link between the authentication part and the timed challenge part. In our case, the answer of the card and the time between the pulse and this answer are deduced by the cryptographic key during the authentication part. Our solution is resistant to terrorist fraud.

3.4. Physical attacks

The main objective of this article is to prove the reliability of a solution based on the HF physical layer. We assume that the authentication protocol can be improved based on the literature. However, our solution must be resistant to such physical attacks.

3.4.1. Noisy environment

Distance bounding protocols are usually based on the use of an Ultra Wideband modulation. This modulation is sensitive to noise because its spectral power density is weak. In the case of a noisy channel, the attacker can anticipate the bits sent by the card to reduce the value of the delay measured by the reader. The answer of the card is just one bit; the attacker has a fifty-fifty chance to discover the real value. Then the reader can believe these errors are due to the noisy environment since they are introduced by the attacker. Then the reader concludes that the card is closer than it is and it does not detect the relay (fig. 10).

In our solution, the use of the HF physical layer which is less sensitive to noise and a length of many bits for the sequence S circumvent the anticipation of the sequence by the relay.

3.4.2. Timing attacks

The clock of the card is linked to the carrier frequency of the device which is powered it. This attack, described by Hancke [14], allows an attacker to speed up the clock and then the processes computed by the card to reduce the secret time T of our protocol. Then, the relay transmits the card answer earlier and the relay is not detected (fig. 11). In [16], the authors show that few solutions allow the limitation of the clock increase such as low-pass filters or internal clock. With this kind of solutions implemented on the card, an attacker can absorb 2-3 ns by clock cycle (73.74 ns). To realize such attacks, the attacker has to use a complex relay which demodulates the signal. This kind of systems introduces delays of few µs. Then this attack is not possible if the secret time T between the reader request and the card answer is lower than a determined threshold. This threshold must be inferior to the necessary time to compensate the delay introduced by the processing times of the relay.

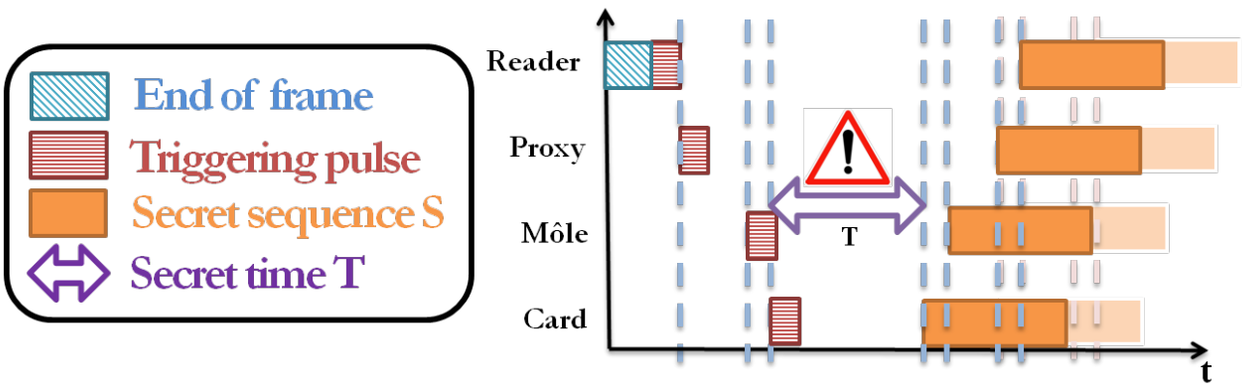

Figure 11. Timing attacks

3.4.3. Anticipation of the synchronisation pulse

The anticipation of the pulse by the relay is a weakness of this kind of protocols because our pulse does not contain a challenge. The relay does not have to wait the pulse and can anticipate and send it earlier. This solution cancels the delay introduced by the forward processing times of the relay (fig. 12). A first solution is to send the pulse just after the end of frame of the reader. Then, the attacker can just cancel the delay introduced by the forward relay. Secondly, our system can use multi level modulation to encrypt the pulse. This modulation can be in amplitude or phase. The value of the secret time T and the secret sequence S can be linked to the value of the modulation level.

Then, this solution limits the anticipation of the pulse since the answer of the card is function of the modulation of the reader.

3.5. Countermeasure improvement

The accuracy and the reliability of our solution can be enhanced:

http://dx.doi.org/10.5772/53393

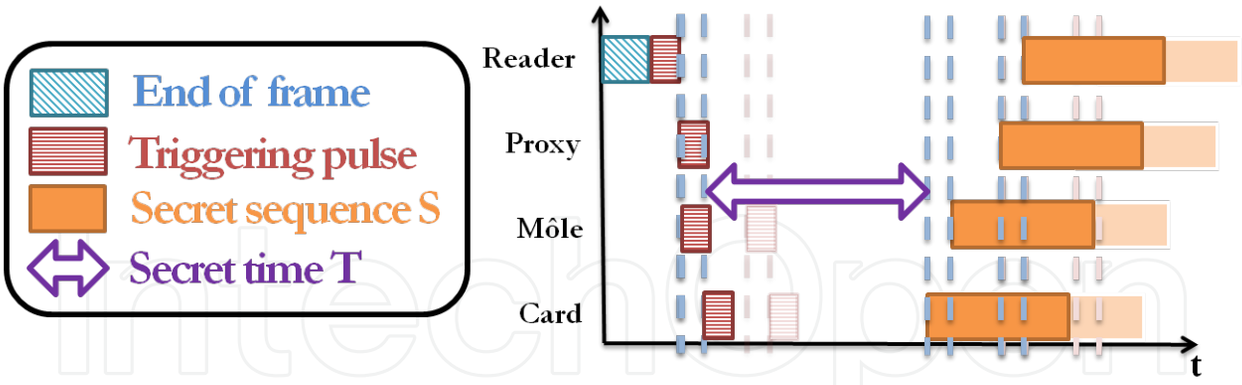

Figure 12. Anticipation of the synchronisation pulse

3.5.1. Pulse detection

An important improvement concerns the detection of our reference point; the accuracy is mainly due to the triggering pulse identification. It is currently realized using a binary signal, this signal results of the demodulation of the RFID signal. We do not control this demodulation but we suppose that it adds a shifting delay to our total delay. We have to develop a system which can detect a pulse with a fixed delay to reduce delay accuracy significantly. The improvement of the accuracy and the rapidity of the pulse detection can be made by using phase modulation only for the pulse. This solution has been implemented on the previously used contactless reader and a new contactless card able to decode a signal modulated in phase. Our approach, c.f. B.1?, was tested with the new parameters for the pulse emission and reception. The results are described on fig. 13. The delay distribution for the case without relay and the case wired relay show an important improvement. Indeed, the two histograms are significantly different; the introduced delay becomes more important with the presence of the wired relay. This experiment shows that all relay attacks can be detected efficiently using the phase modulation for the synchronization pulse. However, this improvement implies the modification of the existing Radio-Frequency front-end equipment.

3.5.2. M-sequences

M-sequences present many properties which can improve the accuracy and the sequence generation of our solution. An M-sequence is a pseudo random sequence generated in most cases by linear feedback shift register and is used in many cryptographic applications. Two properties of M-sequences are of interest: randomness and correlation properties. The sequence is composed of pulses with variable width multiple of the minimal period. The autocorrelation of this kind of signals is an approximation of a Kronecker delta function. Such functions present an important peak when there is no delay between the signals is null which is easy to detect in the case of an implementation.

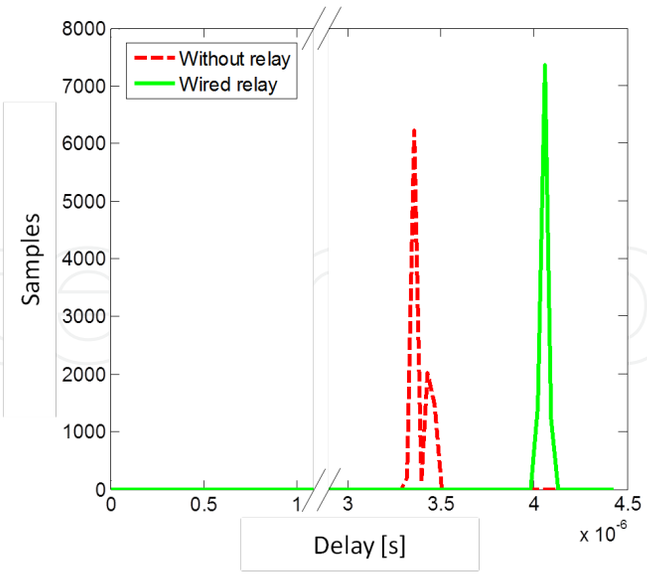

Figure 13. Delay distribution with our solution for the case without relay and in the case with a wired relay for different distance between antennas.

3.5.3. Correlation on PM (Phase Modulation) signals

In the case of NFC use in smartphones for critical application, we can suppose that the target (corresponding to the contactless card) uses active mode to answer to the initiator (the reader in our solution).

Then, the target can modulate its signal by varying the instantaneous phase of the carrier signal. The phase modulation can be more complex for implementation but more accurate in terms of correlation. In fact, the signal received and recorded by the initiator must be in phase with the generated one. There are fewer problems with establishing times in antennas because there is no subcarrier, c.f. II.C.2. The obtained accuracy depends on the phase modulation but we can think that we can detect delays close to half of a carrier. Such improvements imply modifications of standards.

4. Conclusion

The relay attack is an attack on physical layer which should be seriously considered because it can be easily implemented and used in a lot of applications. Moreover, the increasingly use of NFC technology, especially in phone applications, opens new opportunities for intruders. Nowadays, contactless readers are unable to detect a relay. This attack does not modify the signal, nor disturb the transaction and induce delays close to a few periods of the signal carrier. Additionally, cryptography, which is the best solution for most threats, cannot detect this attack.

http://dx.doi.org/10.5772/53393

The first objective of our work was to realize relay attacks with the shortest delays. Within this chapter, we have presented three different solutions to overcome this problem. Experiment results show that the designed wired relay is the most critical relay in terms of the introduced time delay. Our work shows that with two simple antennas and a wire, an attacker can relay data between a reader and a card with delays close to 300 ns, i.e. 50 times shorter than Hancke's relay attack. Today, no countermeasure is able to detect this kind of relays.

The second objective was to develop a new solution to detect such delays with maximum certainty. This countermeasure uses correlation between two sequences to compute the delay introduced by the relay. This will be used to determine the presence of a relay in the reader's field. For the first time, a solution was implemented on a contactless system and the results are interesting. A contactless system does not require additional hardware resources to use our protocol which allows accuracy close to 300 ns. This solution respects the contactless standards and does not disturb the communication between the reader and the card since the protocol can run during the response time of the card. Apart from the most critical relay, namely wired relay, which is not detected in few rare cases, all kind of relays are detected with our counter-measure. However, we developed another solution that detects all kind of relays attacks by improving the accuracy of our contactless system. However, the latter requires a modification of the RF front end.

Author details

Pierre-Henri Thevenon and Olivier Savry

Léti, Minatec, CEA Grenoble, France

References

[1] Juels A. RFID security and privacy: A research survey, IEEE Journal on Selected Areas in Communications, Vol. 24, Issue 2, p381–394; 2006.

[2] Weis S., Sarma S., Rivest R., Engels D. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, proceedings of the International Conference on Security in Pervasive Computing, Vol. 2802, p454-469, SPC 2003; 2003.

[3] Hancke G.: Practical attacks on proximity identification systems, IEEE Symposium on Security and Privacy, p328-333; 2006.

[4] Hancke G., Mayes K., Markantonakis K. Confidence in Smart Token Proximity: Relay Attacks Revisited, Elsevier Computers & Security, Vol. 28, Issue 7, p615-627; 2009.

[5] Lishoy F., Hancke G. P., Mayes K., Markantonakis K. Practical NFC Peer-to-Peer Relay Attack using Mobile Phones, Workshop on RFID Security, RFIDSec'10, 7-9 June 2010, Istanbul, Turkey; 2010.

[6] Hancke G. A Practical Relay Attack on ISO 14443 Proximity Cards, Manuscript; 2005.

[7] Carluccio D., Kasper T., Paar C. Implementation details of a multipurpose ISO 14443 RFID-tool, Workshop on RFID Security, RFIDsec'06, 12-14 July 2006, Graz, Austria; 2006.

[8] Kfir Z., Wool A. Picking virtual pockets using relay attacks on contactless smartcard systems, SecureComm 2005, 5-9 September 2005, Athens, Greece; 2005.

[9] Hlavac M., Rosa T. A Note on the Relay Attacks on e-passports: The Case of Czech e-passports, IACR ePrint; 2007.

[10] Brands S., Chaum D. Distance Bounding Protocols, Advances in Cryptology, p344–359, Workshop on the Theory and Application of Cryptographic Techniques, EUROCYPT'93, May 23-27, 1993, Lofthus, Norway; 1993.

[11] Hancke G. Eavesdropping Attacks on High-Frequency RFID Tokens, Workshop on RFID Security, RFIDSec'08, Budapest, Hungary; 2008.

[12] G. Hancke, M. Kuhn, An RFID distance bounding protocol, SecureComm 2005, 5-9 September 2005, Athens, Greece; 2005.

[13] Rasmussen K. B., Capkun S. Realization of RF Distance Bounding, 19th USENIX Security Symposium, USENIX'10, 11-13 August 2010, Washington, DC, USA; 2010.

[14] Hancke G., Kuhn M. Attacks on Time-of-Flight Distance Bounding Channels: roceedings of the first ACM Conference on Wireless Network Security, WiSec'08, p194–202, 31 March – 2 April 2008, New York, USA; 2008.

[15] Munilla J., Ortiz A., Peinado A. Distance Bounding Protocols with void-challenges for RFIDs, Workshop on RFID Security, RFIDsec'06, 12-14 July 2006, Graz, Austria; 2006.

[16] Reid J., Gonzalez Neito J., Tang T., Senadji B. Detecting Relay Attacks with Timing Based Protocols, ACM Symposium on Information, Computer and Communications Security, ASIACCS 2007, 20-22 March 2007, Singapore; 2007.

[17] Karjoth G., Moskowitz P. Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced, Workshop on Privacy in the Electronic Society, WPES'05, 7 November 2005, Alexandria, VA, USA; 2005.

[18] The off switch for "always on" mobile wireless devices, spychips, toll tags, RFID tags and technologies. www.mobilecloak.com (accessed 12 September 2012).

[19] DIFRwear's RFID Blocking Products. www.dirfwear.com (accessed 12 September 2012).