Proceedings of the 9th International Conference on Applied Informatics
Eger, Hungary, January 29–February 1, 2014. Vol. 2. pp. 177–184
doi: 10.14794/ICAI.9.2014.2.177

Relay attacks on HF RFID and NFC communications and defence against them*

Tamás Varga, Róbert Schulcz

{tvarga,rschulcz}@mik.bme.hu

Abstract

Relay attacks are attacks on systems' security involving a malicious third party interrupting communication between legitimate parties A and B. During a relay attack the malicious third party forwards messages between parties A and B without changing any of the messages thus relay attack can be interpreted as a special case of man-in-the-middle attacks. Its purpose is often eavesdropping on communication links but relay attack is also capable to change the chronology of events and extend the range of the communication link.

The relay attack against RFID or NFC communication links is often implemented to impersonate a device at a distant location.

In our work our goal is to discuss the general properties of attacks and specifically the relay attacks on RFID and NFC systems and to enumerate the relay attacks on RFID and NFC devices discussed in papers. Our work also contains thoughts of feasible defence techniques against the relay attacks.

1. HF RFID and NFC

HF in term HF RFID is the acronym for high frequency. HF RFID systems are mostly operating at the frequency of 13.56 MHz. Near Field Communication (NFC) devices share the operating frequency range with those technologies.

1.1. HF contactless smartcard systems

Speaking of HF RFID in this document we refer to the NFC related technologies discussed in standards ISO 14443 and JIS 6319-4. The logistics-related HF RFID systems such as ISO15693 systems are out of the scope of this document for they are not categorised as smartcards nor they implement advanced security features.

*This article was financed by the project TÁMOP-4.2.2.C-11/1/KONV-2012-0014 FutureRFID - Az RFID/NFC technológia továbbfejlesztési lehetőségei az “Internet of Things” koncepció mentén.

1.1.1. History of contactless smartcards

RFID devices were able to serve as security tokens since their early implementations, many of us have used RFID tokens to authenticate themselves at access control gates.

The eldest systems were designed with no or little security considerations in mind. One of the approaches was to use EM4001 cards as security tokens. EM4001 cards are low-frequency RFID cards with a typical reading distance of some centimetres. These devices are actually wireless WORM memory devices with absolutely no security on-board. The security of these access control systems laid solely on the security by obscurity principle.

As RFID systems became more common and technology advanced, a new class of devices, the contactless smartcards have approached the market. These devices had more than just memory on-board, they were equipped with low-power CPUs and basic operating systems. Being able to do some computations on-board, the possibility of embedding cryptographic operations onto the contactless device became possible.

1.1.2. Security of contactless smartcards

Contactless smart cards are microprocessor devices designed to support security protocols which exchange data with their reader counterpart by radio data reception and transmission.

Their ancestors are wired smartcards such as the USIM cards in cell phones.

As the demand for contactless smartcards and their popularity have risen, many problems regarding the security of these devices emerged. For low market price and low-power operation, smartcard manufacturers try to keep things simple. Smartcards on the market are based on a couple of thousands of gates, so these devices are very much resource-limited. This resource-limited nature of the technology led to solutions like the NXP MIFARE Classic line of devices. NXP created a custom stream cipher for the MIFARE Classic cards which could have been implemented in about 400 NAND gate equivalents. The algorithm itself was kept secret by NXP which was a warning itself. The cards have been introduced in 1994. In 2008 the Crypto-1 cipher has been broken by reverse-engineering [1].

Being compromised a successor for MIFARE Classic security solutions was demanded. NXP have decided to go for well documented and widely used cryptographic algorithms with its DESFire family of cards such as DES, 3DES and AES (supported by e.g. MIFARE DESFire EV1).

The main problem of contactless smart card security are the conflicting requirements of secure algorithms, resource-limited hardware and low price of devices demanded by the market.

Manufacturers decided to go for compromises and create a wide range of products from low-cost low-security devices to high-cost complex devices which utilise complicated cryptographic algorithms.

1.2. NFC devices

NFC devices are often cellular phones or tablets with an NFC-enabled chip. NFC devices may act as RFID readers or tags, or they can even change roles in a communication process.

1.2.1. Security solutions of NFC devices

NFC devices differ from contactless smartcards in many aspects. First of all, they have other peripherals such as key pads, screens, Internet connectivity hardware. There are many input and output devices available which can be utilised in a security protocol for PIN entry, fingerprint reading, one-time-password delivery etc. Second, they are much less resource-limited in computational power: nowadays smart phones have CPUs and GPUs as powerful as workstations' were some years ago.

The NFC-enabled smart devices are similar to contactless smartcards in the physical communication characteristics.

Some NFC devices use an embedded Secure Element (SE) for cryptographic operations. The Secure Element may be implemented in software or may be an actual wired smart card with an own operating system and software. If implemented on a smart card, a SE may be embedded into the USIM card of the NFC phone equipment or may be present as a separate hardware in the device. The SE concept is simple: the SE component communicates through the wireless interface, the NFC chip is only used as a modem, APDUs are processed and generated by the SE.

2. Attack types on NFC and contactless smartcards

In this section we discuss several attack possibilities against smartcards. Please note, that attacks against readers' and tags' security is discussed, a complete systems' secure or insecure nature may depend on other factors, such as network and business application security. [2]

2.1. Attacks against cryptographic algorithms

As security relies on protocols which employ cryptographic algorithms, smartcards may become vulnerable if these algorithms become proven inadequate. [2]

Using strong algorithms are the best manner to avoid this kind of attacks.

2.2. Eavesdropping

Because the data exchange between the communicating parties is wireless an eavesdropper with properly sensitive equipment may be able to receive and decode the communications from a distance. [2]

If the possibility of eavesdropping is taken into consideration while designing communication protocols and choosing cryptographic algorithms, the usefulness of eavesdropping can be rendered void. An eavesdropper may receive the ciphered data but cannot deduce any plaintext data.

2.3. Cloning

Cloning means that an adversary creates a replica of a security token for example by copying all the data from a smartcard to another card thus having a perfect clone of the legitimate smartcard. [2]

Cloning can be prevented by designing security protocols and hardware properly.

2.4. Traffic analysis

Traffic analysis means eavesdropping legitimate card communication or querying the card with prepared data not to gather plaintext data but to deduce some information about the characteristics of the communication, such as size of the data transferred, handshake protocols. This attack is often used combined with other methods. [2]

Successful traffic analysis can be prevented by designing proper communication protocols.

2.5. Side-channel attacks

Side-channel attacks are attacks when the smartcard's security is challenged by not only inspecting communication but by measuring or tampering with other factors specific to the hardware implementation of the cryptographic algorithm, such as timings, power consumption of the smartcard or ambient temperature. Inspecting the schematic of the tag IC is also considered a side-channel technique. [2] An example for side-channel attack is David Oswald and Christof Paar's attack on DESFire MF3ICD40 cards which was based on measuring the power consumption of the cards [3].

To strengthen tags against side-channel attacks it is necessary to care about the security as early as the design process of the integrated circuit and to audit the product before going into production considering the possibility of such attacks. Countermeasures may include redesigning algorithms, using random delays, randomising in-memory data or randomising execution order of algorithms where applicable [4].

2.6. DoS attacks

Denial of Service attacks are attacks which aim to render system components unusable. Methods include jamming the RF communication between the reader and the tag or placing a malicious tag next to a legitimate tag which does not play fair in the anti-collision phase of the communication thus making communication impossible because of successive collisions. Attacks using privacy and security features of the tags such as killing or locking tags with a random password are also considered DoS attacks. [2]

There is no real solution against jamming attacks because of the shared medium.

2.7. Replay attacks

Replay attacks are attacks when card- reader transactions are monitored and after one legitimate party is removed the communication is played back to the other party. [2]

Up-to-date challenge-response protocols are not vulnerable by these attacks.

2.8. Man-in-the-middle attacks

Man-in-the-middle attacks are attacks when two legitimate parties A and B try to communicate with each other and without being aware of they are both communicating with an adversary, C. C relays the messages between A and B with or without modifying the messages. If the data is not modified during the man-in-the-middle attack, a special case of MITM attack, a relay attack is performed.

MITM attacks with data tampering are preventable by using appropriate security protocols, such as digital signatures and signed certificates. Preventing relay attacks is a difficult or impossible task for existing smartcard infrastructures and requires unpleasant compromises for future deployments.

3. Relay attacks

Relay attack is a special type of man-in-the-middle attack when no data tampering is done by the adversary in the middle, he just relays the data between the legitimate parties.

3.1. Why are smartcard systems affected?

The basis of operation in current smartcard systems is that the contactless card and the reader authenticate each other by giving proof to each other of holding a shared secret. Because this process involves challenge- response protocols, an adversary may not know what a legitimate card or reader would answer to a specific challenge, so if a correct answer is got from a card or reader the other party assumes that he communicates with a legitimate card or reader and they are in a well-defined vicinity of each other. As during a relay attack legitimate parties communicate with each other, the shared secret is available to both parties, only the communication range is extended [5]. The relay devices may not conform to standards, so even the card – reader distances may be greater than usual [6].

3.2. Are relay attacks really dangerous?

The answer to this question is definitively a yes. A relay attack against a contactless smartcard system means that if the card is used as an access token or virtual wallet the attacker may access buildings, rooms or even real-world money with a pair of relay devices even without the knowledge of the legitimate card holder at a distant place.

See the following example: a man named John has an access card to pass the turnstiles at his office building, which he keeps in his wallet in his back pocket. On a crowded public transport vehicle an adversary Alan may get his reader device hidden in a bag to reading distance of the card. During this time his accomplice waits at the office building where John works and upon a signal from Alan (e.g.: text message, phone call, etc.) he places a rouge card device hidden in his purse to the turnstile's reader as John would with the original card. If the reader- card communication could be relayed wirelessly for example via a 3G GPRS channel, the adversary may entry to the building.

Using the NFC or HF RFID equipment in passports and electronic voting systems poses other dangers as well, like border crossings with fake passports or manipulation of votes during elections [7, 8, 9].

3.3. Types of relay attacks affecting NFC and HF RFID devices

Relay attacks on NFC and HF RFID equipment may be of several types depending on the communication layer which the attack takes place in.

3.3.1. Attack in the physical layer

A relay attack may be performed in the physical layer of the communication channel by RF components (modulators, demodulators, receivers, transmitters). This attack type is performed without revealing any data either ciphered or deciphered.

During an attack in the physical layer a mixer is used to extract the baseband signal from the RF signal of the initiator which is then mixed up to a suitable frequency for large distance transmission and transmitted over the air to the other party. There the baseband signal is recovered with an RF receiver and fed into an RF transmitter which communicates directly with the target device. The answer of the target is transmitted back to the initiator similarly.

The advantage of physical layer attacks is the small additional delay of the communication. Using just a wire or mixers, the delay may be under 1 μs [10].

3.3.2. APDU relaying

A relay attack may be performed by relaying the APDU frames transacted between the legitimate parties. This method means that the data is transmitted between the parties digitally on an arbitrary interface. Because the data transmission may be jittery, buffering may be required which implies longer delays introduced into the communication.

The delay is proportional to APDU length if the whole APDUs are stored in buffer and are transmitted as wholes [8].

A special case of APDU relaying is when the APDUs from an NFC device's built-in SE are relayed to another NFC device thus virtually cloning the Secure Element [11, 12].

3.4. Preventing relay attacks

Relay attacks pose the largest danger when a transaction can finish unnoticed. If multi-factor authentication schemes are used in a system, relay attacking a device without at least informing the target about a transaction being carried out is just simply impossible. Although rouge terminal equipment may pose further risks, the user is then informed that a transaction is in progress, he only sees invalid information about the transaction details.

3.4.1. Multi-factor authentication

Multi-factor authentication may mean a PIN code entry, using input/output devices on NFC equipment for authentication or just a switch on the card. Some research have been done on measuring environmental parameters to be used as a further authentication factor [13].

3.4.2. Possibilities without multi-factor authentication

Preventing relay attacks is not possible just by inspecting the data exchanged during APDU transactions. Prevention is only feasible by analysing the APDU transactions' timing parameters thus detecting the relay attack and hanging up communication afterwards.

The protocols which employ the principle above are named distance bounding protocols as the timing inspection's role is to find out an upper bound of distance between the reader and the target. Distance bounding protocols may usually be split up to three phases. In phase one, the setup phase, an initialisation is necessary for the parties to prepare for the second phase. The second phase is a rapid data exchange with strict timing constraints. The third phase is a verification when the verifier party evaluates the data gathered in the exchange phase [14].

As the distance bounding is based on the round-trip-time of bits, the timing needs to be very precise. The signal propagation speed equals the speed of the light, so a time error of a microsecond means 300 m distance error. The conventional HF or NFC radio transmission techniques are unable to fulfil such requirements, so asynchronous logic and separate RF channels are necessary to accomplish successful distance bounding [14].

On the smartcard market NXP announced cards with MIFARE proximity check technology like MIFARE Plus X and MIFARE DESFire EV2 in 2008 and 2013

[15, 16].

4. What can I do to prevent a fraud?

If not using a technology with distance check feature, an end user can take the following measures to limit the possibility of a relay attack fraud against his card: store your card in a shielded purse, so it's unusable till you pop it out of the purse and use your card only at trusted readers if possible!

References

[1] K. Nohl, D. Evans, Starbug and H. Plötz, "Reverse-Engineering a Cryptographic RFID Tag," 2008.

[2] A. Mitrokotsa, M. R. Rieback and A. S. Tanenbaum, Classification of RFID Attacks.

[3] D. Oswald and C. Paar, Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World, 2011.

[4] K. Markantonakis, M. Tunstall, G. Hancke, I. Askoxylakis and K. Mayes, "Attacking smart card systems: Theory and practice," 2009.

[5] G. Hancke, "A Practical Relay Attack on ISO 14443 Proximity Cards," 2005.

[6] Z. Kfir and A. Wool, "Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems," Tel Aviv University.

[7] Y. Oren and A. Wool, "Relay Attacks on RFID-Based Electronic Voting Systems".

[8] M. Weiss, "Performing Relay Attacks on ISO14443 Contactless Smart Cards using NFC Mobil Equipment," Der technischen Universität München, 2010.

[9] M. Hlavac and T. Rosa, "A Note on the Relay Attacks on e-passports".

[10] P.-H. Thevenon, O. Savry, S. Tedjini and R. Malherbi-Martins, "Attacks on the HF Physical Layer of Contactless and RFID Systems".

[11] M. Roland, "Applying Relay Attacks to Google Wallet," Zürich, 2013.

[12] M. Roland, "Relay Attacks on Secure Element-enabled Mobile Devices Virtual Pickpocketing Revisited".

[13] A. Czeskis, K. Koscher, J. R. Smith and T. Kohno, "RFIDs and Secret Handshakes: Defending Against Ghost-and-Leech Attacks and Unauthorized Reads with Context-Aware Communications".

[14] G. Hancke, Design of a secure distance-bounding channel for RFID.

[15] NXP, "mifare.net :: MIFARE Plus," [Online]. Available: `http://www.mifare.net/en/products/mifare-smartcard-ic-s/mifare-plus/`. [Accessed 15 04 2014].

[16] Wikipedia, "MIFARE - Wikipedia, the free encyclopedia," [Online]. Available: `http://en.wikipedia.org/wiki/MIFARE`. [Accessed 15 04 2014].