RFID Eavesdropping Using SDR Platforms

F. Le Roy, T. Quiniou, A. Mansour, R. Lababidi, and D. Le Jeune

Lab-STICC UMR CNRS 6285, ENSTA Bretagne,
2 rue François Verny, Brest, France
{frederic.le_roy,thierry.quiniou,ali.mansour
raafat.lababidi,denis.le_jeune}@ensta-bretagne.fr
http://www.ensta-bretagne.eu

Abstract. Radio Frequency Identification (RFID) devices have been recently introduced in several applications and services such as National Identification Cards, Passports, Credit Cards, etc. In this paper, we investigate the security of such devices by showing the possibility of conducting RFID eavesdropping using simple and common devices such as a Software Defined Radio platform. Generally classical RF attacks can be made on long range transmission protocols, however we extend the standard RF attacks to cover RFID communication protocols. In this manuscript, an off-line step-by-step analysis is developed to prove the feasibility of reversing a complete RFID protocol. A real-time implementation is also realized to highlight a real threat in the everyday life.

1 Introduction

Radio-Frequency Identification (RFID) is a contactless use of Radio-Frequency (RF) electromagnetic fields to transfer data between a reader and a RFID tag. Nowadays, RFID is widely used in access control systems, public transports and stock control. RFID can be implemented in different technologies, however the widely used one is described by the standard ISO14443 [1]. Using sophisticated and expensive equipment, previous work demonstrates the vulnerability of this technology. Indeed, interception, decoy or jamming hacks of the "RFID air interface" demonstrate the weakness of systems using contactless chips [2]. Many studies have shown that encryption algorithms or sophisticated protocols can not completely guarantee the communication security between a reader and a RFID tag [3][4][5].

To prevent harmful attacks on RFID devices, various vulnerabilities should be clearly identified [4][5]. Many references in the literature describe in details these security holes, for example: The relay attack on credit card presented in [6] or the Mifare classic cloning tag attack presented in [7]. Due to their big number of varieties, RFID attacks can not be easily classified. However, the wireless RFID attacks can be mainly divided into two classes:

- Passive attack: The attacker only intercepts the communication between a reader and a tag. Eavesdropping [8] or side-channel attacks (or side channel analysis) [9] are the most used passive attacks.
- Active attack: The attacker transmits radio signals in ordre to stimulate the tag. Activation or deactivation, skimming [10] emulation/spoofing [11] and relay [6] are often used to prove the insecurity of RFID.

In specific applications (such as digital distribution broadcast, similar to Google Play Store), smartphones can be used to carry out some attacks and therefore increase the threats of such attacks. However, Near Fiel Communication (NFC) chips implemented in smartphones make applications to become highly platform dependent. For example, applications running on new devices using NFC chip can't read classic tags (as Mifare classic tags); otherwise the NFC chip manufacturer should get the autorisation of NXP through the purchase of an additional license [12]. To be more efficient, a hacker should deploy a simple system that allows him to attack a large panel of applications independently of the target platform. To reach his goals, that attacker could develop his system using new technology called SDR (Software Defined Radio) along with development tools like gnuradio [13]. In fact, serval studies have recently shown that such devises can handle LTE applications [14], GPS [15][16] or AIS spoofing [18], and ADS-B eavesdropping [17]. SDR and gnuradio can be used to easily inject smart hijacking codes in the communication protocol of target devices.

2 Reverse engineering

In RFID passive applications, the reader generates a RF signal to activate the RFID tag who starts transmitting toward the reader its unique identifier code with useful data using a load modulation. In Near filed applications, when the distance between the reader and the device antennas becomes comparable to the carrier wavelength, an inductive coupling between the two antennas will exist. While in far filed applications, the two antennas are coupled using a radiative coupling. Different standards for RFID with respect to applications and distances are summarized in table 1.

Table 1: RFID working range

Band	Coupling	Distance	Applications
LF: 125-135 kHz	Inductive	$<$ 10 cm	Animal identification Factory collection
HF: 13.56 MHz (HF)	Inductive	0.3 - 3 m	Credit card Transportation card
UHF: 865-956 MHz	Radiative	$<$ 10 m	Remote control Tracking, International Article Number
MW:2.4 MHz; 5.8 GHz	Radiative	$>$ 15 m	Electronic toll

Most common cheap tags use Low or High Frequencies with inductive coupling. In this case, the reader (called Proximity Coupling Device (PCD)) establishes a magnetic coupling with the tag (called Proximity IC Card (PICC)) which enables us to power-up the passive tag and push this one to exchange data with the reader.

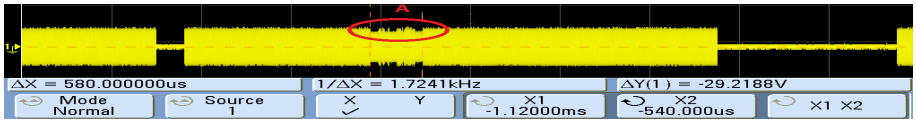
2.1 Attack context

In modern societies, connected objects are invading our everyday life. These smart relatively small sensors will be deployed in outrageous number and they will exchange data among themselves using new network technology such as the

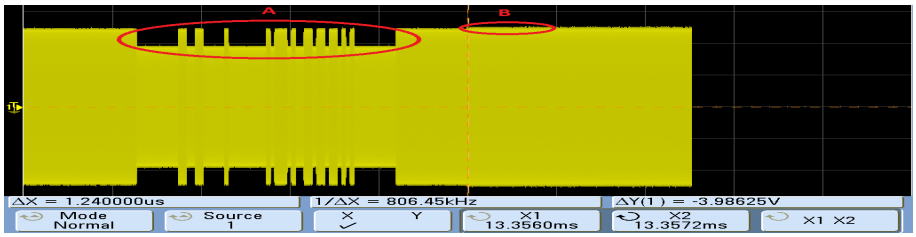
Internet of the Things (IoT). Some of them will use a RFID technology. To demonstrate the concept of an eavesdropping attack on a RFID tag, we targeted in our experience RFID toys[1]. The targeted PICC toys "Rabbits" can exchange data with a computer through a PCD device called "mirror". In the original application, PCD is used to identify a PICC and trigger specific applications (such as reading a weather forecast or playing music).

2.2 Temporal analysis

The signal shown in figure 1a was obtained without the presence of any tag. By making a zoom over the time axis, we can notice the existence of a simple carrier at $f_c = 13.56$ MHz which can be related to the RFID standard[2] ISO/IEC14443-2 [1]. According to that standard, PCD generates periodic scanning signals. Each scanning cycle can be divided into: an active simple carrier period (11.6ms) (a part of this time is shown in fig. 1a), a silence period of 300 μs, then the carrier is again activated before being periodically modulated during 580 μs (see the red circle A of figure 1a), after that the carrier will be again transmitted without any modulation and the cycle will be ended by another silence period of 1.8 ms.



(a) Without tag



(b) With tag

Fig. 1: Scope observations

After the modulation period A of the PCD (see figure 1b), a near PICC transmits its data by modulating the load of its antenna, see the red circle B of the same figure. The load modulation is generated using a subcarrier $f_{sub} = f_c/16 = 847.5kHz$, as it is given by the standard [1]. The bandpass signal generated by the tag is the sum of two band-pass signals at $f_c - f_{sub} = 12.713MHz$ and $f_c + f_{sub} = 14.408MHz$. We should mention the existante of two RFID standards ISO/IEC 14443-2 and ISO/IEC 15693 defined with two types of communication schemes, types A or B with the same acrrier frequancy $f_c = 13.6$

[1] For further details on the used toys, see `www.journaldulapin.com/tag/karotz`
[2] RFID and NFC standards are summarized in [5].

MHz and the same bit rate $D_b = 106kb/s$. Each standard use a specific modulation as illustrated in table 2. Type A uses On-off-keying (OOK). While type B uses an amplitude shift keying (ASK) modulation with an index of 10%. PICC modulates its data using a binary phase shift keying modulation (BPSK). Figures 1a and 1b show PCD → PICC transmission (in area A) using an ASK 10% and a subcarrier around 800 kHz, therefore so the used standard can be ISO/IEC 14443 (type B).

Table 2: RFID stabdard at 13.56 MHz

Standard	Type	Direction	Modulation	Line code	Subcarrier	Rate
14443	A	PCD → PICC PICC → PCD	ASK 100% ASK	Miller Manchester	no 847.5 kHz	106 kbps
	B	PCD → PICC PICC → PCD	ASK 10% BPSK	NRZ	no 847.5 kHz	
15693	Low	PCD → PICC PICC → PCD	ASK 100% or 10% ASK or FSK	8-PPM Manchester	no **423**/485 kHz	1.65 kbps 6.62 kbps
	Fast	PCD → PICC PICC → PCD	ASK 100% or 10% ASK or FSK	2-PPM Manchester	no **423**/485	26.5 kbps

3 Platform description

Our platform contents a RFID antenna, a Digital Video Broadcasting - Terrestrial (DVB-T) receiver, an upconverter and a computer with gnuradio [13]. Since we are using passive tags, the PICC signals are very weak, therefore a specific RFID antenna *DLP-FANT* was successfully introduced to eavesdrop PCD ↔ PICC communication. The DVB-T (R820T dongle from NooElec) is a common USB2 television tuner based on RTL2832u. Palosaari showed that this device can be used an a SDR platform. In our platform, we select the NooElec dongle. Using a chip Rafael Micro R820T, NooElec dongle can sample a radio signal from 24 MHz to 1766 MHz at 2.4 Msps over an USB2. It is worth metioning that the RTL2832u device can not handle the 13.56 MHz RFID frequency because it is out side its range. To solve that problem, a frequency converter (*Ham It Up v1.2* from NooElec) has been used to upconvert the signal at 125 MHz. In spite of the 10 dB conversion loss measured with a vectorial network analyzer, the upconvertor can receive a strong PCD signal and a correct PICC signal.

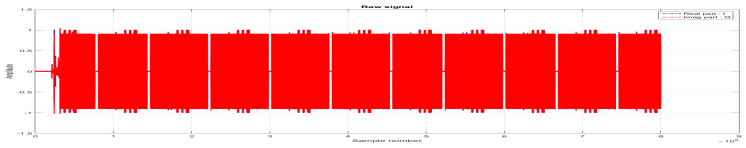


Fig. 2: Raw signal recorded with a GRC application

4 RFID eavesdropping: Signal recording

Using the platform described in the previous section and the graphical tool *GNU Radio Companion (GRC)* software (in GRC, DVB-T devices is given as a source

block), we recorded our signals. In our application, the central frequency has been set to the upper side band of PICC signal according to: $f_c + f_{sub} + f_{IF} = 13.56MHz + 847.5kHz + 125MHz = 139.4075MHz$. Figure 2 shows a cyclic PCD signal registered and processed later on using Matlab. The Upper peaks grouped by three are the BPSK signal replies by PICC to PCD.

5 PICC signal demodulation

The FFT of PICC transmited sighnal is shown in figure 3, where subcarrier is located at $f_{sub} = 847.6KHz$ with a BPSK bandwidth less than $\frac{D_{sym}}{2} = \frac{D_b}{2} = \frac{f_c/128 \approx 106kHz}{2} \approx 53kHz$.

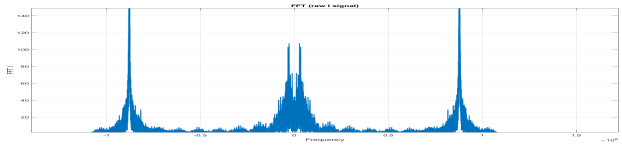


Fig. 3: FFT of the real part of PICC signal

An elementary time unit (ETU) which represents a symbol duration is defined as $ETU = 1/D_b = 9.44\mu s$. The sampling frequency f_s used for acquisition is 2.4 MHz. The number of samples per symbol is: $N_{samples/symbol} = f_s/D_b \approx 23$. This number of samples per symbol is very comfortable and we could reduce it in the future in order to reduce the computation time. A BPSK constellation represents two different phases spaced of π. Nevertheless, this constellation rotates currently during transmission because of effects of the propagation channel. The constellation of figure 4 contains the signal but the rotation creates a circle. To synchronize the signal a Costas loop is used [20]. After processing, we obtained the final binary information but with phase ambiguity. Actually, we are not able to predict if the π phase represent the '0' or the '1' symbol and we consequently have to compare the bit sequences as patterns. The binary data are illustrated in figure 4.

6 PCD signal demodulation

Records used for PCD demodulation are the same that the PICC demodulation because they always contain useful information. PCD transmits requests at PICC with a 10% ASK modulation signal. Figure 5 shows the ASK signal and the PICC response which have a higher amplitude because of the subcarrier load modulation.

Fast Fourier transform of the signal gives the frequency of the signal to processed in baseband. A frequency translation followed by a low pass filtering gives the signal illustrated in the figure 6.

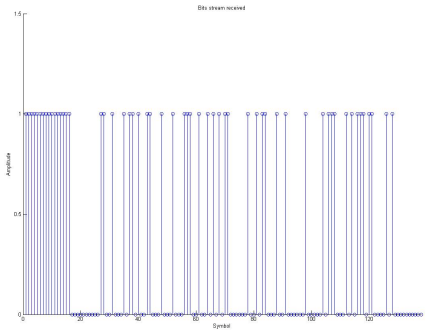


Fig. 4: Binary information of PICC

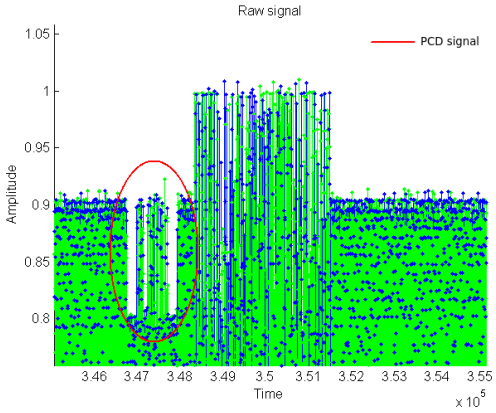


Fig. 5: Raw signal from PCD and PICC

A threshold applied on this signal gives us the binary data representing the necessary but sufficient information to understand and reverse the complete protocol.

7 Conclusion

In this article RFID eavesdropping between an RFID reader and a tag has been successfully implemented using a low-cost hardware and an open source software stack. Moreover, we have shown that the association of Python or Matlab with Qnuradio toolkit makes signal processing on physical radio signals very powerful and very easy to prototype. Using this raw material, the communication protocol between reader and tag can then be intercepted and analyzed by more sophisticated tools such as Wireshark: for example, association has been successfully done for GSM eavesdropping. In future work, it's expected to to see if more

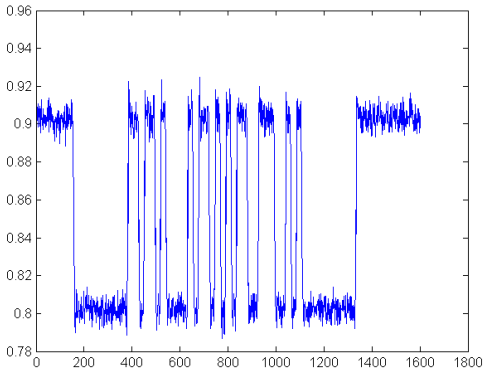


Fig. 6: PCD demodulated signal

complex RFID attacks can be performed on SDR platform. Some of our recent works shown that present studied codes used with R820T are easily portable to other SDR platforms. On the contrary of R820T, BladeRF or HackRF platforms has a transmit output usable for jamming. So, in future works, the feasibility of more advanced attacks such as skimming or emulation will be explored. In the software radio community, these kinds of attack are viewed as a smart waveform because antenna time, transceiver time and terminal time are different. Thus, absolute, relative and immediate time concepts are crucial to manage smart waveform. This coming work will focus in particular on a transceiver API currently available as a draft document at the WinnF.

References

1. Joint Technical Committee : ISO/IEC 14443-2 : Identification cards Contactless integrated circuit(s) cards Proximity cards Part 2: Radio frequency power and signal interface, ISO/IEC International Standard (2001)
2. Oren, Y., Schirman, D., Wool, A.: RFID jamming and attacks on Israeli e-voting, In: Smart Objects, Systems and Technologies, pp. 1–7. VDE, Munich (2012)
3. Thevenon, P.H.: Sécurisation de la couche physique des communications sans contact de type RFID et NFC. Phd thesis, Université de Grenoble (2011)
4. Di J., Thompson D.R.: Security for RFID tags. In: Tehranipoor, M., Wang, C. Introduction to Hardware Security and Trust. Springer, New York (2012)
5. Khoo, B., Harris, P., Husain S. A.: Security risk analysis of RFID technology: A RFID tag life cycle approach. In: Wireless Telecommunications Symposium, pp. 1–7. IEEE press, Prague (2009)
6. Lee, E.: NFC Hacking: The Easy Way. In: 20th DEFCON `https://www.defcon.org/html/links/dc-archives/dc-20-archive.html`, Las Vegas (2012)
7. Almeida, M.: Hacking Mifare Classic Cards. In: blackhat, `https://www.blackhat.com/sp-14/summit.html`, Sao Paulo (2014)

8. Hancke, G.: Eavesdropping attacks on high-frequency RFID tokens. In: 4th Workshop on RFID Security (RFIDSec), pp. 100–113, (2008)
9. Oren, Y., Shamir, A.: Remote Password Extraction from RFID Tags In: IEEE Transactions on Computers, vol. 56(9), 1292–1296 (2007)
10. Juels, A., Molnar, D., Wagner, D.: Security and Privacy Issues in E-passports. In: 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks, pp. 74–88. IEEE press, Athens (2005)
11. Winkler, M., Faseth, T., Arthaber, H., Magerl, G.: An UHF RFID tag emulator for precise emulation of the physical layer. In: Wireless Technology Conference (EuWIT), pp. 273–276, IEEE press, Paris (2010).
12. http://www.nxp.com/products/identification-and-security/nfc-and-reader-ics/nfc-everywhere/iso-iec-14443a-licensing-information:ISO-IEC-14443A-LICENSING-INFO
13. http://gnuradio.org/redmine/projects/gnuradio/wiki
14. https://sourceforge.net/p/openlte/wiki/Home/
15. Humphreys, T.E., Ledvina, B., Psiaki, M., OHanlon, B., Kintner J. Paul M.: Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In: 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008), pp 2314-2325, Savannah (2008)
16. Huang L., Yang Q.: GPS SPOOFING Low-cost GPS simulator. In: 23th DEFCON https://www.defcon.org/html/links/dc-archives/dc-23-archive.html, Las Vegas (2015)
17. http://www.rtl-sdr.com/adsb-aircraft-radar-with-rtl-sdr/
18. Balduzzi, M.: AIS exposed understanding vulnerabilities & attacks 2.0. In: blackhat asia, https://www.blackhat.com/asia-14/archives.html, Singapore , 2014.E.
19. http://fr.mathworks.com/products/matlab/
20. Feigin, J. : FEATURES-Featured Technologies:-Signal Processing-Practical Costas loop design-Designing a simple and inexpensive BPSK Costas loop carrier recovery circuit. In: RF design, 25(1), (2002)