Comparative Analysis of RFID and NFC Devices

Albert Babichenko
University of Hawai'i - West Oahu

Abstract

Radio Frequency Identification (RFID) and Near-Field Communication (NFC) are examples of secure wireless technologies. An NFC device is a subset of RFID technology that functions similarly but can also act as a reader. This enables two-way communication between two NFC devices. These wireless devices are inexpensive to manufacture, and their ease of use allows them to be utilized for many situations. The distinguishing factor between these devices is the security, compatibility, and the range at which they communicate. It is well known that the security elements in most RFID cards utilize AES, DES, and proprietary Crypto-1 encryption. This encryption is the primary factor against attacks. However, older forum types are well known to be easily defeated. One method in which we can test this is by attacking the older NFC equipped cards and comparing their security against more recent forum types. This will be a test for real world scenarios as attackers can utilize wireless transmissions and potentially steal data without being detected. With the growing number of RFID objects and the abundance of smart devices, the security of these technologies may be at risk. The purpose of this paper is to explore the security of RFID and its standards as well as assess the different architecture and communication protocols of those devices. Recommendations for different tags will be proposed based on their ideal use-case, the standard of communication, and the encryption it uses.

Introduction & Research Question

There are two common types of RFID, active and passive (Want, 2006). Active tags use a direct power source such as a battery. Passive tags, which are the focus of this paper, have no power source but instead rely on the reader to provide the necessary power to emit a signal. There are also two different types of RFID being near-field RFID and far-field RFID. This paper will focus on near-field RFID devices. Near-filed RFID is based on Faraday's principle of magnetic induction (Want, 2006). The reader works by emitting an electromagnetic field that interacts with the passive tag's coil and provides it necessary power to temporarily emit its own signal back. The type of signal depends on the frequency the device operates while the security of the device depends on the standard it uses.

Many businesses and consumers will buy RFID tags without researching the standards or frequencies they use. This can be problematic as old standards use outdated security that leaves them vulnerable to breach. This poses a question of which standard is best to use and what each form type can provide over the other.

This research on RFID and NFC devices determined that most new tags use secure cryptographic ciphers. However, because most manufacturing techniques are kept secret, it's difficult to know exactly how the security in these devices is implemented.

Research Design & Data Collection

The primary objective of this research will be to identify differences between HF and LF tags, the differences in standards, their security vulnerabilities, and their use case. The secondary objective will be to test the security of RFID and NFC tags as well as the relative difficulty of stealing information and duplicating the results to a new tag. For testing, the primarily focus on the HF NXP Mifare Classic 1K, the HF Mifare DESFire EV1 4K, and the LF 125 kHz RFID tag. All the tags and cards used in the experiment are owned by the researcher. I will include hypothetical scenarios in which these tags could be used. The tests will consist of two different RFID readers and writers. This will ensure the ability to test multiple types of RFID tags as well as verify the results between each device. Additionally, the researcher will use three types of RFID and NFC tags. The HF NXP Mifare Classic 1K, the HF Mifare DESFire EV1 4K, and the LF 125 kHz RFID tag. A comparison of the technology that each tag uses, as well as its security standards, and use case with the objective to provide recommendations for RFID and NFC frequencies and standards as well as provide additional information to make informed decisions.

Results

According to my sample list, only the Mifare DESFire EV1 uses secure AES 128 encryption. This read-only card has data in other blocks that cannot be read without the proper key. The key for this card is unknown for this experiment as it would be in real-world scenarios. Without the key, not much can be determined about the card. This tag utilizes the HF 13.56 MHz range using ISO/IEC 14443-4 standard.

The Mifare Classic uses Crypto-1 encryption which is vulnerable to attack. The tag utilizes the HF 13.56 MHz range using ISO/IEC 14443A/B standard. These cards are often found in legacy systems that have yet to be updated. When reading the tag, the UID of the tag in the first block of the data and a decoding operation can be used to find the hex values in the empty sectors.

The RFID T5577 card does not use encryption. This tag is primarily used for inventory control or animals to identify owners or other important information. The tag utilizes the LF 125 kHz range using ISO/IEC 11784 standard.

Card/Tag	Frequency	Encryption	Type	ISO/IEC	SAK	Use Case	UID
Mifare Classic	13.56 MHz (HF)	Crypto-1	NFC	14443A/B	08	Gated Entry	1007265621
Mifare DESFire EV1	13.56 MHz (HF)	AES 128	NFC	14443-4	20	Access Control	4064043770
T5577	125 KHz (LF)	N/A	RFID	11784	N/A	Animal Tag	1165366000
Mifare Classic	13.56 MHz (HF)	Crypto-1	NFC	14443A/B	08	Payment Method	2118376732
T5577	125 KHz (LF)	N/A	RFID	11784	N/A	Inventory Control	1229657982

Data

Block	Data [1]
0	04 63 3C F2 A9 20 44 03 00 08 61 33 16 42 28 80
1	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Block	Data [2]
0	55 A7 09 3C C7 08 04 00 00 08 61 33 16 42 28 80
1	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
2	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Block	Data [3]
0	55 A7 09 3C C7 08 04 00 62 63 64 65 66 67 68 69
1	68 65 6C 6F 20 77 6F 72 6C 64 00 00 00 00 00 00
2	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Discussion

In theory, there are advanced methods that could attempt to exploit possible vulnerabilities in the tags design using what's called a side-channel attack. A side-channel attack exploits the implementation of the device. In this case, the power leakage from the tag can be recorded and calculated to decrease the encryption complexity (Xu et al., 2018). This process requires specialized tools, equipment, and software to perform analysis. Manufacturers are aware of these types of attacks and aim to mask power leakage during critical stages where data can be collected. This research project did not test any of the tags to determine vulnerability to a side-channel attack.

Recommendation

Overall, the research determined the most secure tag to be the Mifare DESFire EV1. This tag is ideal for access control in places like the gym. It provides good encryption while using current standards. Although we can determine the UID of this card, we cannot copy the data it holds. Without the data, copying only the UID will result in errors when attempting to authenticate.

The Mifare Classic was susceptible to attack. The researcher was able to decode the tag to find the hex values in the data sectors. This process takes less than a few seconds as the software determines the secret key used in its encryption. This card should not be used for storing sensitive data, but instead be upgraded to use the newer AES encryption.

The RFID T5577 card is a simple RFID tag. Its primary purpose is for inventory control in places like the hospital or in animals to identify owners or other important information. The tag does not have encryption since the UID does not contain sensitive data.

Contact

Albert Babichenko
University of Hawai'i at West Oahu
Email: albertab@hawaii.edu

References

1. Ahuja, S., & Potti, P. (2010). An introduction to RFID technology. Commun. Netw., 2(3), 183-186.
2. Fennani, B., Hamam, H., & Dahmane, A. O. (2011, December). RFID overview. In ICM 2011 Proceeding (pp. 1-5). IEEE.
3. Masyuk, M. A. (2019, December). Information security of RFID and NFC technologies. In Journal of Physics: Conference Series (Vol. 1399, No. 3, p. 033093). IOP Publishing.
4. Nath, B., Reynolds, F., & Want, R. (2006). RFID technology and applications. IEEE Pervasive computing, 5(1), 22-24.
5. Phillips, T., Karygiannis, T., & Kuhn, R. (2005). Security standards for the RFID market. IEEE Security & Privacy, 3(6), 85-89.
6. Proehl, G., & Transceivers, S. (2013). An Introduction to Near Field Communications. ST-Microelectronics [Online, retrieved: 15th July 2016]. Available from: http://www. st. com/content/st_com/en/applications/connectivit y/near-field-communication-nfc. html.
7. Rieback, M. R., Crispo, B., & Tanenbaum, A. S. (2006). The evolution of RFID security. IEEE Pervasive Computing, 5(01), 62-69.
8. Singh, M. M., Adzman, K. A. A. K., & Hassan, R. (2018). Near Field Communication (NFC) technology security vulnerabilities and countermeasures. International Journal of Engineering & Technology, 7(4.31), 298-305.
9. Want, R. (2006). An introduction to RFID technology. IEEE pervasive computing, 5(1), 25-33.
10. Xu, R., Zhu, L., Wang, A., Du, X., Choo, K. K. R., Zhang, G., & Gai, K. (2018). Side-channel attack on a protected rfid card. IEEE Access, 6, 58395-58404.