Privacy Concerns Surrounding NFC Transactions

Anthony Caligure

Binghamton University

Abstract

Near Field Communication has become a prominent technology in the world of mobile payments. NFC-enabled payment terminals have been introduced in millions of physical business locations in recent years. The ability to store and process credit cards through NFC applications has been a major factor to the popularity of NFC. Many security measures have been implemented to ensure that sensitive information is protected when transferred over NFC. Despite this, many exploits have been developed and proven successful at intercepting transmissions. These exploits pose huge ethical dilemmas. This paper will explore the technical components of these exploits, as well as the ethical implications. The risks of identity fraud and physical harm are consequences that all users of NFC technology must understand before partaking in transactions. When considering the future use of NFC, human implants may be commonplace. When developing and using these implants, it will be imperative for computer professionals to understand the risk of exploits. Severe harm or death can result from irresponsible or faulty software.

Privacy Concerns Surrounding NFC Transactions

**Introduction**

Efficiency and convenience have been the driving factors behind many of the technological advances used daily. Users desire quick and simple ways of checking on friends, money, and services. The widespread adoption of smartphones has enabled users to manage nearly every part of their lives. One such example is the use of mobile payments. Programs including Apple Pay, Samsung Pay, and Google Wallet allow users to store credit card information directly to their smartphones. These applications interact with payment readers at physical business locations, allowing for fast and easy transfer of money. These transactions are performed using Near Field Communication technology. Despite its ease of use, the transmission of personal data over Near Field Communication can have serious consequences. As Near Field Communication technology, NFC for short, expands the global reach of the Internet of Things, the privacy risks associated with eavesdropping on NFC transactions outweigh the convenience of mobile payments and data transfer. The adaptation of earlier Radio Frequency Identification, RFID, technology into NFC leaves private information at risk of being stolen. The assumptions of trust when using NFC technology leaves users vulnerable to Relay, Pre-Play and Eavesdropping attacks, among many others. The ability for a back-end system to unknowingly store transferred information also poses security risks for users. The mechanics of NFC transactions must be understood to analyze the methods of exploiting transferred data.

**Background**

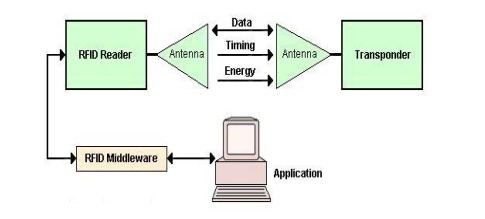
NFC technology allows for two devices to connect wirelessly within a short-range. According to research on security and privacy implications of NFC payments by Nicholas Akinyokun and Vanessa Teague (2017) from the University of Melbourne School of Computing and Information Systems, the two devices must be within ten centimeters of one another for the transaction to successfully occur (1: para. 1). People have given NFC the description of a tap-and-go technology based on the proximity. Supported transfer rates range from 106 to 424 kilobits per second. The quick transfer speeds make NFC technology a perfect fit for transferring small amounts data like a credit card transaction. Devices are determined to be in-range by use of magnetic induction. Transactions are grouped into two categories, open and secure applications. Open applications do not contain security measures to preserve data. A person to person connection is one such example. Secure applications provide security measures to ensure secure transfer of payments and other private information. As one security measure, data is transferred in a binary format called NFC Data Exchange Format. In recent years, the number of NFC readers in physical business locations have increased rapidly. As of December 2016, over 16 million NFC POS, point of sale, terminals are being utilized worldwide. The number of users has nearly tripled from 44.5 million in 2014 to 181.98 million in 2017 (Statista, 2017).

Technology is a tool to improve efficiency. Paying for necessities with NFC is a convenient way to go about a daily routine. However, with the mass adoption of NFC POS terminals, the threat of hacks and security breaches has increased exponentially. Privacy risks associated with technology fall into three categories: data loss, data exploit, and governmental overreach. Data loss can result from bugs, theft or user error. Data exploit occurs when an entity utilizes data for third-party uses without consent. Governmental overreach can occur when a government reveals personal data of citizens to preserve safety and security of the nation. (Aditya, Bhattacharjee, Druschel, Erdélyi & Lentz, 2014, 2: para. 2, 3, 4). NFC transactions can be intercepted by nearby transceivers, routing sensitive information including social security numbers, bank accounts and personal information to an unknown source. If payment data is compromised, there can be serious financial consequences.Hackers can steal identities and ruin credit by abusing the data. Despite the recent advancement of NFC technology, security flaws stemming from earlier RFID technology still exist. Alternatives to NFC including QR Codes and Accelerometer technology contain similar security and technical limitations.

**Precedents & Related Works**

Most smartphones today contain accelerometers, a component used to measure the motion of the device based on its acceleration. The accelerometer has been utilized to create a peer-to-peer data sharing application called Bump. The app allows two users to “bump” their phones together to transfer money, photos, or other files. Although convenient for the user, the time and energy needed to compute the location of the two devices is extensive. Payment info is retrieved from PayPal, rather than being stored directly on the phone. Therefore, an internet connection is required to use Bump (Romero, 2012, p. 64). Quick Response, QR, codes allow for quick interpretation of a matrix barcode, containing a link to websites, applications, or advertisements. Any smartphone camera can take a photo of the code, and redirect the user to the proper website or file. QR codes are also used as a form of mobile payment. Buyers and sellers have unique codes that, when scanned, allow for a successful transaction (Romero, 2012, p. 64). However, information is often not stored on the device. Redirecting the user to PayPal or other online payment sites can impede the effectiveness of transactions. During busy shopping times, servers may become overwhelmed and crash, leaving millions of users without their payment information. In comparison, NFC is a more reliable option when it comes to data transfer and retrieval. However, the technology taken from earlier radio frequency identification puts private information at risk of theft while being transferred.

NFC is derived from radio frequency identification technology, RFID for short. According to research on RFID security by Rand Mahmood and Wasim Al-Hamdani (2011), from the New York Institute of Technology and Kentucky State University respectively,



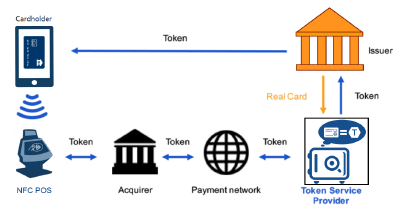
*Figure 1.* Flow chart of a RFID system

an electromagnetic field is used to identify bits of information broadcasted from the small RFID chips, as seen in Figure 1 (p. 43). The chips can be implemented into ID cards, toll booths, and car keys. RFID transactions can be completed from a distance greater than ten centimeters. Due to the long transmission range, interceptions by a third-party entity are frequent. RFID systems can be disrupted “by employing energy at the right frequency” (Mahmood & Al-Hamdani, 2011, p. 43). These disruptions have serious implications in medical facilities, where the chips are used to track and monitor patients. Another serious privacy implication is the ability for chips to be read without one’s knowledge. According to Mahmood and Al-Hamdani (2011, p. 45), RFID chips can be read without physical contact. High-Gain Antennas can increase the distance at which chips are read. With this technology, a user can retrieve a credit card number from a pedestrian’s wallet by walking in close proximity with an active antenna, leaving millions of people vulnerable to identity theft. Successful work-around have been developed to intercept NFC transactions and steal the private information being transferred. Despite the popularity of NFC over alternatives including QR Codes and Bump, the security flaws stemming from earlier RFID technology leave users at risk of data loss. Before analyzing how these security flaws occur, it is important to understand what techniques NFC utilizes to keep information secure.

**Support**

**Security Measures**

The security measures implemented by NFC transactions must be fully understood before analyzing the methods used to steal private information. NFC works on the ISO/IEC 14443 standard, creating a uniform guideline for security measures (Akinyokun & Teague, 2017, 1: para. 2). As a method to prevent unwanted storage of data, NFC works on a half-duplex communication, allowing only the POS terminal or tag to transfer data at a given time. All credit card information is stored in a hardware component called “the secure element” (Akinyokun & Teague, 2017, 3.3: para. 2). This element is separate from all other components of the device. Only developer-enabled applications, including NFC-supported payment applications, have access to the data in the element. As an added level of security, tokenization is utilized to replace credit card numbers with a random sequence of numbers.



*Figure 2.* Flow chart of tokenization in a NFC Transaction

Figure 2 illustrates the creation and transfer of a unique token during an NFC transaction. Only the issuer and the Token Service Provider are given access to the actual card number. All other entities in the transaction utilize the unique token (Akinyokun & Teague, 2017, 3.2: para. 4). The use of a random number sequence protects the user’s actual card number from a potential hack. The bank and credit company verify the unique keys and tokens assigned to each NFC tag.

For a payment to be processed, the Trusted Service Manager, TSM, must authenticate the payment information of the user’s device and the POS terminal. According to research on the security of NFC payments by Nour Tabet and Media Ayu (2016) of Hamad Bin Khalida University, utilizing a third-party entity allows “for building the trust relationship between users to bypass the confirmation and allow the exchange of information” (p. 170). Users can exchange data and payments freely with other NFC devices authenticated by the designated TSM. According to Tabet and Ayu, (2017, p. 172) TSMs utilize secure socket layers, SSLs, or virtual private networks, VPNs, to create a secure connection between the device and the TSM servers. With a secure connection, the TSM can access data from the secure-element and authenticate the credit info. One popular peer-to-peer, P2P, example is Venmo. Credit card companies can approve transactions through Venmo’s application programming interface, API. Although Venmo does not utilize NFC, the concepts of TSM verification can be applied to contactless payment transactions. Further encryption is employed by the wireless service provider to prevent sniffing, a technique used to capture data while being transmitted through a wireless network. There are a multitude of trust assumptions that must be understood when a user transmits data with NFC technology.

**Assumptions of Trust**

NFC users, developers, and POS terminals all engage in a high level of trust when transferring payments. According to Akinyokun and Teague (2017, 4: para. 1), all entities in a NFC transaction are responsible for preserving security and privacy. Liability for compromised transactions must be understood by all entities. All NFC POS terminals are required to operate on one transaction at a time, preventing transfer of data between an incorrect device-terminal pair. All NFC transactions are required to be monitored in real-time by the specified bank or credit company. Quick detection of unauthorized transactions is critical to prevent theft. When a transaction is being processed for an amount larger than the credit card’s limit, the PIN is requested, ensuring the owner of the card is making the purchase. Though these trust assumptions appear to fully protect users from data exploitation, the structure of NFC transactions is still vulnerable to interceptions. With the increasing popularity of NFC technology, the development of hacks and exploits have skyrocketed. These exploits pose significant threats to the safety and privacy of data being transferred.

**Methods of Attack**

The most frequent and well-known NFC exploit is a Relay attack. A Relay attack works by establishing a middle-man that captures the data before forwarding it to the receiver.



*Figure 3.* A relay attack setup for a NFC transaction

According to research on a practical relay attack for NFC transactions by Cavdar and Tomur (2015) of the Middle East Technical University, The attacker, using a cell phone or other WIFI-enabled device, picks up the data and stores it. The attacker creates a proxy, from which the payment information is sent to the POS terminal while assuming the identity of the original user, as seen in Figure 3. This technique is often referred to as card emulation (p. 1310). There is no manipulation of the transferred data, so both the device and POS terminal consider the transaction to be safe and successful. The ISO/IEC 14443 security standard has been determined to be insufficient to prevent relay attacks. The ISO/IEC standard dictates a maximum transmission range of 10 centimeters, enough for an attacker to obtain transmitted data in crowded environments such as train stations and airports. Despite the supposed maximum range, some attack methods have successfully voided the ISO/IEC 14443 standard transmission range, creating a more widespread threat of stolen data.

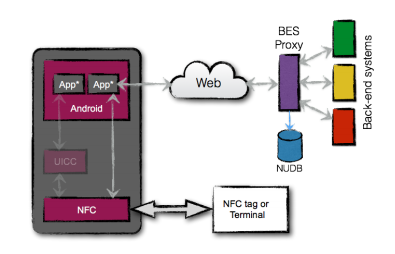
Eavesdropping attacks are another significant threat to secure data. An attacker at a separate location can intercept the frequency signals between a device and POS terminal. According to Akinyokun and Teague (2017, 5.4: para. 1), Eavesdropping attacks can be conducted from a distance up to sixty centimeters with no chance of failure. To intercept the signals, a small “loop antenna” must be affixed to the POS terminal, similar to ATM skimmers. The antenna is nearly invisible to an unsuspecting user. Due to this research, it is apparent that the ISO/IEC 14443 standard operating range of 10cm is insufficient.

Skimming attacks are similar to Eavesdropping attacks, in that the information being stolen comes directly from the POS terminal or device. There is active communication between the attack and the transmission. It is possible for an attacker to carry out a successful Skimming attack because “there is no security mechanism in contactless payment cards to help them distinguish between an authorized or unauthorized NFC-enabled POS terminal” (Akinyokun & Teague, 2017, 5.5: para. 2). The simplicity of these attacks brings about serious privacy concerns. Despite the convenience, there are many possible risks when processing payment transactions. These risks can have serious ethical and privacy implications.

**Implications**

As previously stated, the ISO/IEC 14443 standard fails to properly protect data during NFC transactions. The NFC-supported payment applications must be equipped with proper security measures. However, it is often unknown what measures third-party applications take to ensure user privacy. Terms of agreements are often ignored by users, putting them in a risky position of exposing their information. With the sheer volume of payment applications available, it can be difficult for a user to determine which are safe to trust. According to Akinyokun and Teague (2017, 5.5: para. 3), attackers can create “clones” of contactless payment cards with data retrieved from skimming attacks. Any encryption or transaction information can be routed from the original card to the clone, giving attackers full use of the victim’s credit card. Illegitimate purchases, loss of credit, and denial of loans are all possible outcomes of identity fraud. However, monetary loss is only a fraction of the potential harm that attacks on NFC transactions can cause.

Data mining is utilized by companies to tailor searches for users. Companies have implemented numerous methods to collect mass amounts of data. The end goal is to create a more personalized online experience for the user. According to John Stuart Mill, the act utilitarianism principle justifies the collection of data. The net impact, as determined by the companies, increases utility. Tailoring searches for users can help them find related items quicker. However, the collection of data is often not detailed to the user. NFC technology is one such method companies can use to collect information about users. According to research on mining NFC-based user information by Andersen and Karlsen (2016) of the Arctic University of Norway, a proxy can be utilized to access the application processing the NFC transaction.



*Figure 4.* Collecting NFC data for a back-end system through a NUDB

These proxies have the capability to forward some or all data to a NFC Usage Database, NUDB. Figure 4 illustrates the flow of data from the NFC component to a back-end system (p. 175). The information gathered can give companies insight on what products users are buying or where they are shopping. The extent of the data being stored is often unknown to the user. Any amount of information may be stored in the NUDB, ranging from the store where the purchase occurred to the full credit card number. The database where this information is stored must have its own host of security measures to prevent a data leak. The intentions of the company observing data trends are often unknown. Malicious entities may gain access to secure information. Although human NFC-implants are still in their infancy, the trend of RFID implants has been steadily gaining traction for the last few years. Amal Graafstra, a pioneer of the subject, has brought about many social and ethical debates on the use of technology in the human body. In his TED Talk, Graafstra promotes the benefits of RFID implants by unlocking a “smart lock” by bringing his hand against the lock (Graafstra, 2013, 6:05). Graafstra (2013, 2:22) explains that his implant came from a desire to reduce the number of keys he had to carry. Though the convenience is clear, there are serious privacy and health risks associated with implanting RFID or NFC technology into one's body. Just as Skimming and Eavesdropping attacks can compromise payment data, similar systems could be used to spy on or injure users. The principles of negative rights are important to mention. These include the “right to life, the right to be free from assault, the right to use your property” (Baase, 2012, p. 31). These principles protect users from malicious intent. Though unavoidable, the manipulation of NFC or RFID implants to harm users is morally wrong. With the sheer number of threats to safety and privacy when using NFC technology, the convenience cannot be held as the sole justification for utilizing the technology. Proper caution must be taken to ensure private information is kept secure.

**Conclusion**

With the increasing popularity of mobile payments, NFC technology has filled a niche for fast and easy payments. The amenity of having credit cards stored on a smartphone is one appeal of the technology. NFC technology employs many security systems to keep payment information safe. Multiple levels of authorization are utilized to ensure that the credit card company, bank, and NFC application recognize a proper transaction. Half-duplex transmissions ensure that a device or POS terminal will not receive outside transmissions during a transactions. Although these security measures appear to cover all possible threats, developers have managed to create exploits. Relay, Eavesdropping and Skimming attacks have successfully stolen data from NFC transactions. Attackers can effortlessly redirect payment information to another device. From there, the fate of credit card, social security, or bank account numbers are in the hands of the attacker. These security threats pose real ethical implications pertaining to user privacy when using the Internet. Aside from potentially stolen data, mining NFC transaction-information is a direct violation of user’s privacy when online. Considering all possible risks, and the growing popularity of NFC systems, the privacy risks associated with eavesdropping on NFC transactions leave users, and their personal data, vulnerable to attack. The future of NFC technology is still mostly unclear. Despite this, the introduction of human-implants is gaining traction, and could soon become a widespread practice. When combining technology with the human body, developers must be aware of how faulty software can affect the human body. As the adoption of NFC technology continues to grow, users must exercise caution when using mobile payments. The privacy implications of NFC go far deeper than the convenience. NFC chips can be implanted to supplement a physical credit card, or provide doctors with quick diagnostic information about the user’s health. Hackers may soon develop methods to control vital body-functions or disable implants that serve a similar purpose to pacemakers. Extra care must be taken to preserve security of human-implants, as it becomes a matter of life and death rather than loss of data when hackers gain control.

References

Aditya, P., Bhattacharjee, B., Druschel, P., Erdélyi, V., & Lentz, M. (2015). Brave new world: Privacy risks for mobile users.*ACM* *SIGMOBILE Mobile Computing and Communications Review* *18*(3), 49-54. DOI: http://dx.doi.org/10.1145/2721896.2721907

Akinyokun, N., & Teague, V. (2017). *Security and privacy implications of NFC-enabled contactless payment systems*. In Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES ’17). New York, NY, USA: ACM DOI: https://doi.org/10.1145/3098954.3103161

Andersen, A., & Karlsen, R. (2016). *User profiling through NFC interactions: mining NFC-based user information from mobile devices and back-end systems.* InProceedings of the 14th ACM International Symposium on Mobility Management and Wireless Access (173-176). New York, NY, USA: ACM. DOI: https://doi.org/10.1145/2989250.2989274

Baase, S. (2013). *Gift of fire*. 4th Ed. Boston: Pearson.

Cavdar, D. & Tomur, E. (2015). *A practical NFC relay attack on mobile devices using card emulation mode.* In Proceedings of the 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (1308 - 1312). Opatija, Turkey. DOI: https://doi.org/10.1109/MIPRO.2015.7160477

Graafstra, A. (2013, October 17). *Amal Graafstra: biohacking – the forefront of a new kind of human evolution* [Video file].  TED. Retrieved from https://www.youtube.com/watch?v=7DxVWhFLI6E

Mahmood, R. A. & Al-Hamdani, W. A. (2011). *Is RFID technology secure and* private?. In Proceedings of the 2011 Information Security Curriculum Development Conference (42-49). New York, NY, USA: ACM. DOI: http://dx.doi.org/10.1145/2047456.2047462

Romero, J. (2012, May 24). No more waiting on near field communication. *IEEE Spectrum* *49*(6), 64. DOI: https://doi.org/10.1109/MSPEC.2012.6204183

Statista (2017). *Global number of NFC-ready POS and m-POS terminals shipped in 2016 (in millions).* Statistic. Retrieved from https://www.statista.com/statistics/669207/nfc-ready-pos-and-m-pos-terminals-worldwide/

Tabet, N. E., & Ayu, M. A. (2016). *Analysing the security of NFC based payment systems*. In Proceedings of the International Conference on Informatics and Computing (169-174). Mataram, Indonesia. DOI: http://dx.doi.org/10.1109/IAC.2016.7905710