nShield: A Noninvasive NFC Security System for Mobile Devices

Ruogu Zhou
Michigan State University
3115 Engineering Bld.
East Lansing, MI 48824
zhouruog@msu.edu

Guoliang Xing
Michigan State University
3115 Engineering Bld.
East Lansing, MI 48824
glxing@msu.edu

ABSTRACT

The Near Field Communication (NFC) technology is gaining increasing popularity among mobile users. However, as a relatively new and developing technology, NFC may also introduce security threats that make mobile devices vulnerable to various malicious attacks. This work presents the first system study on the feasibility of and defense again passive NFC eavesdropping. Our experiments show that commodity NFC-enabled mobile devices can be eavesdropped from up to 240 cm away, which is at least an order of magnitude of the intended NFC communication distance. This finding challenges the general perception that NFC is largely immune to eavesdropping because of its short working range. We then present the design of a hardware security system called *nShield*. With a small form factor, nShield can be attached to the back of mobile devices to attenuate the signal strength against passive eavesdropping. At the same time, the absorbed RF energy is scavenged by nShield for its perpetual operation. nShield intelligently determines the right attenuation level that is just enough to sustain reliable data communication. We implement a prototype of nShield, and evaluate its performance via extensive experiments. Our results show that nShield has low power consumption (23 uW), can harvest significant amount of power (55 mW), and adaptively attenuates the signal strength of NFC in a variety of realistic settings, while only introducing insignificant delay (up to 2.2 s).

Categories and Subject Descriptors

C.2.0 [**Computer-communication Networks**]: General—*Security and protection*; B.0 [**Hardware**]: General

Keywords

NFC; Eavesdropping; Smartphone; Energy Harvesting

MobiSys'14, June 16–19, 2014, Bretton Woods, New Hampshire, USA.

http://dx.doi.org/10.1145/2594368.2594376 .

1. INTRODUCTION

In recent years, the Near Field Communication (NFC) technology is increasingly available on the new generation of smartphones, tablets, and smart accessories. It is estimated that more than 200 million NFC-enabled smartphones will be shipped in 2013 [7]. And over 50% of the smart devices to be shipped in 2015 will have NFC support [4]. The growing popularity of NFC has enabled a range of applications, from contactless payment [6] and ticketing [16] to device pairing [15] for ad hoc data exchange.

A major trait of NFC is its short communication range (usually within 10 cm), which is the result of the fast decaying magnetic induction between the antennas of NFC transmitter and receiver. The short communication range is favored by many security-sensitive applications, such as contactless payment, since it provides a natural, physical protection against various attacks, particularly malicious eavesdropping. Unfortunately, as NFC is still a relatively new and developing technology, its implementation on mobile devices often have design flaws, which may be exploited to compromise application security [29]. In particular, our experimental study described in this work shows that, current NFC radios emit significantly more RF energy than intended. With a specially designed portable NFC sniffer, we are able to eavesdrop NFC transmissions from up to 240 cm away, which is at least an order of magnitude further than the intended NFC communication distance. These findings raise major concerns on the physical security of NFC. Moreover, this issue is aggravated by the fact that current NFC chipsets adopt fixed transmission power, which cannot be adjusted to mitigate the potential risks of eavesdropping.

Existing efforts on NFC security can be classified into two basic categories. Several solutions improve the security of NFC by adding more security elements, such as additional secret keys, to the native OS of mobile devices [23]. However, the mobile device would become vulnerable if the integrity of the OS is compromised (e.g., after being rooted). The second category employs additional hardware devices to secure NFC [30][12]. However, these hardware systems are bulky and power-hungry, which are ill-suited for mobile devices. In a recent work [21], a hardware security device is developed to harvest energy from NFC transmissions and jam malicious interactions. However, due to the low energy harvesting efficiency, the system may not provide uninterrupted protection. The above approaches are designed to prevent content-based malicious attacks, and none of them can protect NFC from eavesdropping attacks.

In this paper, we propose a novel, noninvasive NFC security system called *nShield* to protect NFC against passive eavesdropping. nShield is a credit card-sized thin pad that can be easily stuck on the back of mobile devices (see Fig. 6). nShield implements a novel adaptive RF attenuation scheme, in which the extra RF energy of NFC transmissions is determined and absorbed by nShield. At the same time, nShield scavenges the extra RF energy to sustain the perpetual operation. A key contribution of this work is the analysis of the factors affecting the energy harvesting efficiency, and the design of a highly effective energy harvesting system. nSheild is capable of harvesting significant amount of power (55 mW) from commodity mobile devices, which is at least a 1.8X improvement over the state-of-the-art NFC-based energy harvesting systems. Together with the extremely lo-power design, it enables nShield to provide the host uninterrupted protection against malicious eavesdropping. Lastly, the small form factor, self-sustainability, and transparency to OS, makes nShield an attractive solution to retrofit existing mobile devices with protection against passive eavesdropping.

In summary, we make the following key contributions in this paper.

1. We conduct an experimental study on the feasibility of passive NFC eavesdropping, with a specially designed inexpensive NFC sniffer. We show that commodity NFC-enabled devices can be eavesdropped from up to 240 cm away, which is at least an order of magnitude further than the intended NFC communication distance. Moreover, although external signal attenuation is effective in reducing NFC transmission power, the desired attenuation level that can still sustain data communication is highly dependent on the NFC hardware, tags sensitivity, and the physical distance. To our best knowledge, this is the first empirical study on passive NFC eavesdropping in practical settings.

2. We design an NFC security system called nShield to protect NFC from passive eavesdropping attacks. As a key novelty, nShield absorbs the excessive RF energy of NFC to attenuate the signal strength against passive eavesdropping, while the absorbed RF energy is scavenged for its perpetual operation. By exploiting the NFC target discovery process, nShield intelligently determines the right attenuation level that is just enough to sustain reliable data communication. As a result, it can promptly and precisely control the signal strength of NFC transmissions, mitigating the risk of passive eavesdropping.

3. We carefully analyze the factors that affect the NFC energy harvesting efficiency, and apply several design techniques to the antenna and hardware of nShield to maximize the amount of harvested energy, which include quality factor optimization, voltage matching, and tag emulation. As a result, nShield can harvest significantly more power (1.8X and 3.1X) than the two state-of-the-art NFC energy harvesting systems. This capability enables nShield to provide the host uninterrupted protections against passive eavesdropping attacks.

4. We implement a prototype of nShield, and evaluate its performance via extensive experiments. Our results show that nShield has extremely low power consumption, high energy harvesting efficiency, and can adaptively attenuate the signal strength of NFC transmissions in a variety of realistic settings, while only introducing insignificant delay.

2. BACKGROUND

NFC employs the fast decaying magnetic induction between the antennas of transmitter and receiver for communication in close distance. The typical working distance of NFC using compact antenna coils (with the size of a credit card) is a few centimeters. An NFC communication process involves an initiator and a target. Initiator devices are usually smartphones, tablets, and POS terminals, which initiate the NFC communication with the target. The target devices can either be those devices or proximity cards. NFC has two working modes, i.e., passive mode and active mode. The passive mode employs the same communication techniques as those used by the proximity card, in which the target device is powered by the RF field emitted by the initiator, and transmits by modulating the RF field. In the active mode, both initiator and target are powered by their own energy sources. The ASK and PSK modulation schemes are employed by NFC to support a number of data rates (106 kpbs, 212 kbps and 424 kbps).

An NFC communication process always begins with *target discovery*, in which the NFC initiator discovers the nearby NFC targets and learns the capability of the discovered targets. The initial phase of discovery process is probing, in which the initiator broadcasts discovery messages periodically to find nearby target devices. An NFC target device responds after it hears the probe. The initiator and the target then exchange a few parameters back and forth to learn the capabilities of each other before the start of the real data communication. On an NFC-enabled Android phone, when the screen of the phone is unlocked, the NFC radio is activated and the discovery process starts automatically and continues until a target device is discovered. During this process, the discovery probes are broadcast at a frequency of about 1.4 Hz. Using NFC antennas, a device can harvest energy from the RF field generated by NFC initiators within close proximity (a few centimeters). However, the amount of energy that can be harvested during the probing is usually very limited, as NFC radios have a low duty-cycle (10%) during the probing phase.

Passive eavesdropping attacks are harmful to wireless communications in several ways. They could not only compromise the privacy/security of the system, but also serve as the early steps of other more damaging attacks [31], e.g., the man-in-the-middle attacks [31]. Another reason that makes passive eavesdropping attacks especially harmful is that they are hard to detect, as they do not actively transmit any signal and are usually launched from distance. NFC is generally considered to be a secure wireless technology against eavesdropping, due to its short communication range. However, current NFC implementations often emit significantly more RF power than intended. Our study shows that, with specially designed NFC sniffers, NFC signals can be eavesdropped from as far as 2.4 m away, which is much further than the intended NFC working distance. This poses a serious concern for security/privacy-sensitive NFC applications such as contactless payment.

3. A MEASUREMENT STUDY

In this section we experimentally study the passive eavesdropping distance of NFC transmissions. Specifically, we measure the physical distance at which the signals from initiators and targets can be successfully decoded, i.e., eavesdropped. Moreover, we study the impact of transmission power attenuation on the passive eavesdropping distance of different NFC devices. The results provide important motivation for the design of nShield.

We note that the actual eavesdropping distance depends on many factors, such as initiator implementation, initiator position, NFC working mode (active or passive), and environmental factors (e.g., background noise). Our measurements are conducted in typical settings, and an exhaustive evaluation of all these factors is beyond the scope of this paper. Nevertheless, our results raise serious concerns about the physical security of NFC due to the significant discrepancies between the actual and intended working distances, and shed lights on possible defense mechanisms.

3.1 Experimental Setup

Our experiment is conducted using NFC initiators, tags, and a sniffer. Commercial off-the-shelf NFC transceivers do not make good sniffers for two reasons. First, they typically have a small antenna size due to the form factor constraints of mobile devices, which greatly limits the receiving sensitivity. Second, the commercial NFC transceivers are specially optimized for working in close distance with the target. We have designed an NFC sniffer for our experiments. Fig. 4 shows the block diagram of the sniffer, which consists of a 30 cm by 23 cm antenna, a pre-amplifier, and an ADC that is connected to a PC via USB to upload the collected samples. The NFC signal overheard by the antenna is amplified and demodulated by the pre-amplifier and the AM demodulator, respectively. The signal is then digitalized by ADC and transmitted to PC for decoding. Our sniffer has a size of a tablet and average power consumption of 120 mW. Therefore, it can be easily connected to a mobile device via the micro USB interface to form a mobile sniffer. The NFC initiator devices used in this study include a Google Nexus 7 tablet, two smartphones (Google Galaxy Nexus and Samsung Galaxy Note 2), and an Adafruit PN532 NFC breakboard [1]. The NXP PN532 NFC chipset is adopted by the NFC breakboard, while all the other devices employ the NXP PN544 NFC chipset. These two chipsets are currently the most popular NFC chipsets used on commercial off-the-shelf mobile devices. Both chipsets use fixed transmission power which cannot be configured by software [11]. We use an NXP Mifare Classic tag as target.

3.2 Results

In the first experiment, we measure the passive eavesdropping distances of both initiator and tag, without attenuating the RF field radiated by the initiator. We place the initiators on a desk, with the antennas of the devices facing forward. We activate one initiator at a time. The Mifare tag is placed in parallel and 1 cm from the antenna of the activated initiator. We place the sniffer near the initiator, and gradually move it away from the initiator.

Fig. 1 shows the signal strength of the initiators that is measured by the sniffer at different distances. As expected, the received signal strength decreases over distance. We can see that the signal is capped when the initiator-sniffer distance is short, as the output voltage of the sniffer cannot exceed the voltage of its battery. We implemented a Miller decoder in Matlab to decode these samples. We find that the signal can be decoded if its strength is above 100 mV. When the strength is lower, the signal to noise ratio (SNR) is too low for successful decoding. As shown in Fig. 1, the 100 mV signal strength corresponds to physical distances of 152 cm, 131 cm, 116 cm, and 244 cm, respectively, when Nexus 7, Note 2, Galaxy Nexus, and Adafruit NFC breakboard are used as initiators. We are also able to decode the signal transmitted by the tag at maximum distances of 91 cm with Nexus 7, 85 cm with Note 2, 67 cm with Galaxy Nexus, and 121 cm with Adafruit NFC breakboard. Compared to the initiator transmissions, the eavesdropping distance of tag transmissions is significantly shorter, due to the much weaker signal strength of the tag response. We acknowledge that better hardware design and more advanced signal processing techniques could achieve even longer eavesdropping distances. Nevertheless, our results are already sufficient to demonstrate that the current NFC implementations on smartphone and tablet platforms are subject to passive eavesdropping from a distance at least an order of magnitude longer than the intended NFC communication range.

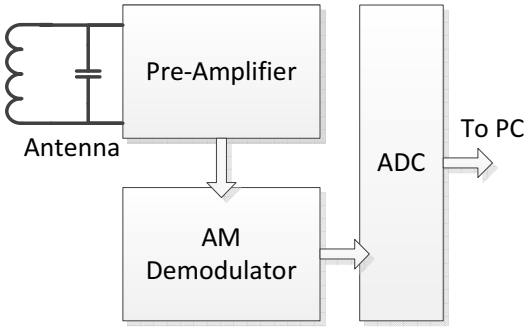

Figure 4: Block diagram of the NFC sniffer used in the measurement study.

A promising approach to defending against passive eavesdropping is to reduce the transmission power of the initiator. However, the current NFC chipsets adopt fixed transmission power, which leaves attenuating the signal externally the only choice. We need to answer the following two questions in order to design an external signal attenuator: 1) what is the maximum attenuation level that could be applied without sacrificing the reliability of data communication, and 2) what is the resulted passive eavesdropping distance. We investigate these questions in the second experiment. We adopt the same experimental setting as in the first experiment, except that we cover the initiators with thin aluminum foils to attenuate the emitted RF field. The thickness and the area of the aluminum foil are adjusted to create different RF field strength, while the maximum passive eavesdropping distances are measured with our sniffer. We use a loop antenna connecting with an Agilent oscilloscope to measure the RF field strength after attenuation.

Fig. 2 shows that, as expected, for all the 4 tested initiators, the passive eavesdropping distances decrease when the attenuation level increases. When the strength of the NFC RF field is just enough to support reliable communication, our sniffer can achieve a maximum passive eavesdropping distance of around 80 cm, which is 67% (NFC Breakboard), 48% (Neuxs 7), 39% (Note 2), and 31% (Galaxy Nexus) shorter than those without attenuation. With such a short

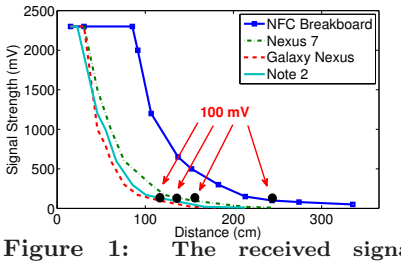

Figure 1: The received signal strength of the unattenuated signal over distance.

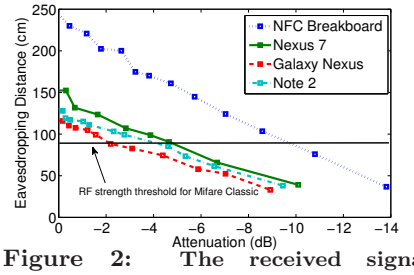

Figure 2: The received signal strength of the attenuated signal over distance.

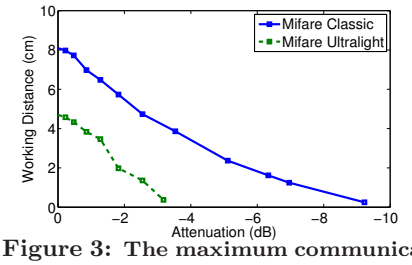

Figure 3: The maximum communication distances of two tags with different attenuation levels.

sniffing distance, the eavesdropping attack becomes significantly more difficult. However, the optimal attenuation level varies significantly for different initiators. Specifically, Fig. 2 shows that, to reduce the signal power to an undecodable level for sniffers, the NFC signal needs to be attenuated by 9.8 dB (NFC Breakboard), 5.9 dB (Neuxs 7), 4.2 dB (Note 2), and 2.2 dB (Galaxy Nexus), respectively. Such significant diversity is caused by the differences in initiator implementations, such as the size of antenna.

We now show that, for a given initiator, the maximum allowed attenuation level also varies significantly across targets. We measure the maximum communication distances between the NFC breakboard and two passive tags, Mifare Classic and Mifare Ultralight, with different attenuation levels applied to the RF field. Fig. 3 shows that the communication distances decrease when the attenuation level increases. However, the Mifare Classic can tolerate a maximum attenuation level of about 9 dB, while Mifare Ultralight can only tolerate about 3 dB. This huge difference is the result of the diverse receiving sensitivities of tags.

3.3 Discussion

We now summarize the results of our experimental study. First, current NFC implementations emit significantly more RF power than intended. As a result, the passive eavesdropping distance is at least an order of magnitude of the intended NFC communication range. This issue greatly increases NFC users' risk of being eavesdropped. Second, the NFC RF field strength can be effectively attenuated externally to enhance the security of NFC without sacrificing the communication reliability. However, the desired attenuation level varies significantly with the specific working conditions, including initiator transmission power, target reception sensitivity, initiator-target distance, and etc. Therefore, simple solutions such as an external signal attenuator with fixed amount of power reduction would not work for all scenarios.

These results have several important implications for the security of NFC systems. Properly implemented cryptosystems can offer strong security assurance even when the communication could be eavesdropped. However, as NFC is usually considered "physically secure", many upper-layer protocols of NFC applications do not implement encryption or only adopt short keys in encryption algorithms (such as DES [3]). With an passive eavesdropping distance up to 244 cm as shown in our study, these systems hence are exposed to malicious attacks. For instance, the leakage of pairing code during NFC-based Bluetooth paring could lead to possible passive eavesdropping or even man-in-the-middle attack on the following data communications. This issue is aggravated in active NFC communication scenarios, where both NFC devices actively transmits using high transmission power, and eavesdropping attacks on both of the devices could be launched over distance. Moreover, the feasibility of NFC eavesdropping attack renders encryption the last line of defense against attacks. Unfortunately, with the rapid advance of decryption techniques, many once considered "safe" encryption protocols, including WEP [18], DES [3], and RSA [13], have been demonstrated vulnerable when sufficient encrypted data is observed through eavesdropping.

4. OVERVIEW OF nShield

4.1 Design Objectives and Challenges

It is shown in Section 3 that current NFC initiator implementations emit significantly more RF power than intended, which greatly increases the user's risk of being eavesdropped. This result motivates us to develop an NFC security protection device called nShield that dynamically regulates the strength of the RF field radiated by NFC initiators. nShield regulates the RF strength by absorbing the excessive RF power with its own antenna. nShield can be easily stuck on the back of mobile devices, and is solely powered by the absorbed RF energy, thus eliminating offline charging. Specifically, we have the following design objectives.

Adaptive RF field strength regulation. Today's NFC devices exhibit significant diversity in terms of initiator transmission power and the receiver sensitivity. nShield must be able to dynamically adjust the amount of absorbed power to ensure that the remaining RF power is just enough to sustain successful NFC communications. As nShield has no prior knowledge about the receiving sensitivity of the target, a "trial and error" approach is needed to determine whether NFC communications can be sustained at a particular power level. However, trying all possible attenuation levels incurs high delay due to the wide attenuation range and the low frequency of NFC transmissions.

Noninvasive operation. The operation of nShield should not rely on either initiator nor target. In other words, it should work in a standalone manner with no physical connections to neither initiator nor target. This requires nShield to be a self-sustained, self-powered device which has its own CPU and power source. Moreover, it should be transparent to the host, without the need to communicate with the host or modify the NFC protocols. The noninvasive and transparent nature of nShield enables it to easily retrofit the existing NFC devices with security protection. However, a key challenge presented by this design is that, as nShield cannot interact with either initiator or target, it has to determine the right transmission power solely based on the overheard transmissions.

Unintermittent protection. nShield should provide the host devices unintermittent protection against passive eavesdropping. In particular, the down time of protection caused by battery depletion should be minimized. As discussed in Section 2, nShield scavenges energy from the NFC RF field, which is available only when the host device is active (e.g., when the screen of a smartphone is unlocked). When energy harvesting is not possible, nShield has to survive using the energy scavenged previously. Moreover, to keep the small form factor, nShield cannot adopt bulky high capacity batteries. Due to these challenges, nShield must minimize its power consumption as well as maximize the amount of power harvested from the host device. However, wireless charging is inherently inefficient [27], especially for peripherals like nShield that has tight cost budget and form factor constraints.

4.2 System Overview

nShield is composed of two major components, a software-defined passive NFC radio platform and an adaptive RF field attenuation algorithm. The software-defined platform is capable of receiving data from and transmitting data to NFC initiators, attenuating the NFC RF field using its antenna, and harvesting energy from the RF field. The adaptive attenuation algorithm dynamically determines the highest attenuation level that can still ensure communication reliability, according to the overheard NFC traffic. Fig. 5 shows the system architecture of nShield. An on-board MCU runs signal processing tasks such as encoding/decoding. nShield has two tuned loop antennas. The larger antenna is used for harvesting energy from the NFC initiator, as well as transmitting data to the initiator. The smaller antenna is responsible for overhearing data from the initiator. We show in Section 5 that, this dual antenna configuration is essential for maximizing the energy harvesting efficiency without sacrificing the receiving performance, as the receiving antenna and the harvesting antenna require fundamentally different design methods.

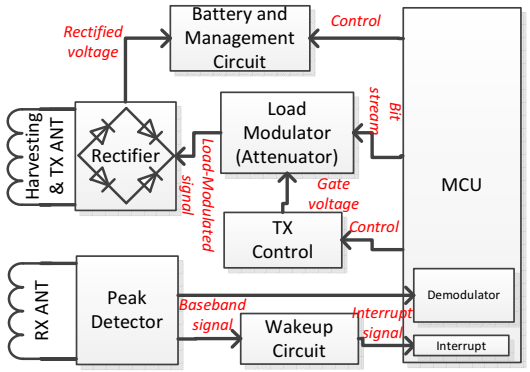

Figure 5: Block Diagram of nShield.

The harvesting antenna is connected with an RF bridge rectifier, which rectifies the RF signal to a DC voltage. The DC voltage is then regulated to provide power to the system and charge a 20 mAh on-board battery. In Section 5 we show that the voltage matching between the harvesting antenna and the battery plays a critical role in maximizing the amount of power harvested by the system. The load modulator is connected with the rectifier, which alters the load of the harvesting antenna to transmit data to the NFC initiator. Since the load modulation-based communication scheme adopted by NFC standard requires strict timing, nShield employs a hardware TX control circuit to accurately generate the clock used by the load modulation and precisely synchronize the data to be transmitted. The TX control circuit can generate different clock frequencies according to the data rates of the modulation schemes. nShield reduces the risk of eavesdropping by absorbing the excessive RF power radiated by the initiator with an adjustable attenuator, which is multiplexed with the load modulator.

The receiving antenna is connected to a peak detector, which removes the AM carrier from the RF signal. The hardware-based demodulator on the MCU demodulates the baseband signal, from which the raw data is retrieved. A key novelty in the design of nShield is to exploit the hand-shake mechanism in the target discovery process to determine the optimal transmission power of the initiator. Specifically, nShield infers whether the previous messages are successfully received by examining the logical relationship between consecutive initiator messages. To reduce the delay of determining the optimal attenuation level, nShield adopts a binary search algorithm to accelerate the search. nShield falls asleep to conserve energy when no NFC signal is present. A low-power wakeup circuit connected with the peak detector generates an interrupt signal to wake up the system once NFC RF field is present.

Fig. 6 shows a prototype system of nShield. The size of the circuit board and the antenna is 5.5 cm by 5.3 cm and 9.6 cm by 9.6 cm, respectively. We note that this antenna is specially designed for Nexus 7 tablet. The size of antenna can be reduced for smartphones, without sacrificing the energy harvesting efficiency and attenuation performance. The size of the prototype circuit board can be shrunk significantly by removing unnecessary components like debug port, buttons and LEDs. As a result, nShield can be easily fit on diminutive thin-film circuit boards, which could be stuck to the back of small-size mobile devices. The total component cost of our prototype implementation is under $20, and could be further reduced when nShield is mass-manufactured.

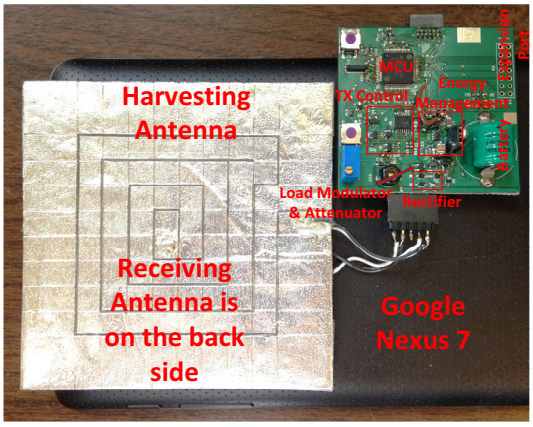

Figure 6: Antenna and circuit of nShield mounted on the back of a Google Nexus 7 tablet.

5. MAXIMIZING HARVESTED ENERGY

nShield is powered solely by the energy harvested from NFC transmissions. The capability of harvesting a large amount of power not only enables the uninterrupted protection of nShield, but also helps increase the attenuation range of the host's NFC transmission power. Fig. 7 shows the block diagram of the energy harvesting subsystem of

nShield, which comprises a harvesting antenna and an energy management circuit. These two components work together to determine the amount of power that could be harvested. We show that they must be carefully designed to maximize the harvested power. We define the following two terms to characterize the performance of energy harvesting. *Energy (power) transfer efficiency* is defined as the ratio of the amount of energy (power) transferred to the harvesting antenna, to the amount of energy (power) transmitted by the NFC initiator. *Energy (power) harvesting efficiency* is defined as the ratio of the amount of energy (power) transferred to the receiving system after rectifying and regulation, to the amount of energy (power) transmitted by the NFC initiator. Obviously, for any wireless power transfer system, energy (power) harvesting efficiency is always lower than energy (power) transfer efficiency.

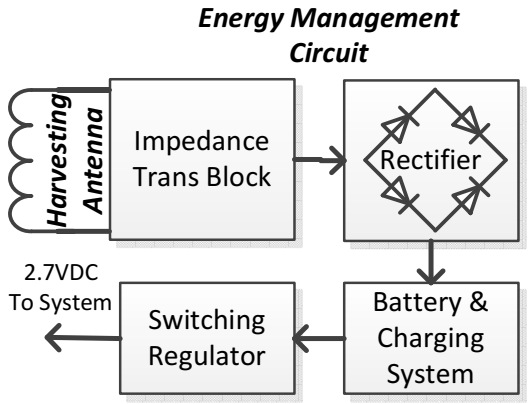

Figure 7: Block Diagram of energy management circuit on nShield.

5.1 Harvesting Antenna

When the communication between an NFC initiator and a target device commences, energy transfers from the transmitting antenna to the harvesting antenna via resonant inductive coupling [25] through air. The NFC antennas are essentially inductors, which have inductance as well as series resistance. The radiation efficiency of NFC antennas can be quantified using *quality factor* (or Q-factor), which is the ratio of the inductive reactance to the series resistance of the antenna at 13.56 MHz:

$$Q = \frac{\omega L}{R} = \frac{27.12\pi L}{R} 10^6 \quad (1)$$

where ω is the working frequency of the antenna, and L and R are the inductance and the series resistance of the antenna, respectively. The Q-factors of the transmitter antenna and the harvesting antenna largely determine the power harvesting efficiency between antennas. Given the Q-factors of transmitter antenna, Q_t, and the harvesting antenna, Q_h, the maximum power transfer efficiency of the NFC antenna pairs can be expressed as [25]:

$$\Pi_{max} = \frac{U^2}{(1+\sqrt{1+U^2})^2} \quad (2)$$

$$U = k\sqrt{Q_t Q_h} \quad (3)$$

where k is the coupling coefficient, with 0 being completely uncoupled and 1 being perfectly coupled. k depends on many factors such as the distance between the two antennas, antenna alignment, and etc. For NFC, since the communication pairs are always placed in proximity, k is usually above 0.1 [8]. For each nShield installation, k is largely a constant value, as nShield is fixed on the back of the mobile device. Due to the NFC communication bandwidth requirement (about 1.8 MHz [8]), the Q-factor of the transmitting antennas, Q_t, is about 15 for most NFC devices [17]. As a result, the maximum power transfer efficiency of nShield is largely determined by the Q-factor of the harvesting antenna, Q_h. A high power transfer efficiency can thus be achieved by using harvesting antennas with high Q-factors (above 50). For example, if k, Q_t, and Q_h of an NFC energy harvesting system are 0.2, 15, and 100 respectively, a maximum power transfer efficiency of 77% could be achieved. A key insight of this analysis is that, the harvesting antenna cannot be reused by the NFC transceiver, due to the conflicting requirements of the Q-factors. Therefore, to support efficient energy harvesting and reliable NFC communication at the same time, a dual antenna configuration (one high Q-factor antenna and one low Q-factor antenna) must be adopted.

According to (1), to improve Q-factor of an NFC antenna, we can either increase its inductance or decrease its series resistance. In our harvesting antenna design shown in Fig. 6, we use wide antenna tracks to decrease the series resistance, and closely couple the antenna tracks to increase the inductance. The parasitic capacitance also contributes to the series resistance of the antenna. We adopt a single layer antenna to decease the parasitic capacitance. The resulted high Q-factor ensures that, when the transmitter antenna and the harvesting antenna are closely coupled, the harvesting antenna can receive most of the radiated energy. The implementation details of the harvesting antenna are given in Section 7.

5.2 Energy Management Circuit

Another major factor that affects the amount of power harvested to the system is the design of the energy management circuit. The energy received by the harvesting antenna has to be transferred to the energy storage components in the system, e.g., batteries or super capacitors. A common practice for maximizing power transfer is to match the output impedance of the antenna with the input impedance of the load [24]. The maximum power that can be transferred, P_{load}, can be expressed as:

$$P_{load} = \left(\frac{U_{ant-open}}{R_{ant}+R_{load}}\right)^2 R_{load} = \frac{U_{ant}^2}{4R_{ant}} = 0.25P_{max} \quad (4)$$

where $U_{ant-open}$ is the open-circuit root-mean-square voltage inducted on the harvesting antenna, R_{ant} and R_{load} are the impedances of the antenna and the load, respectively, and P_{max} is the maximum power that the harvesting antenna can receive. We can see that P_{load} equals a quarter of P_{max}, when and only when $R_{load} = R_{ant}$.

However, the perfect impedance matching is impossible for energy harvesting systems, since the input impedance of the energy management circuit, R_{load}, varies significantly with the system load. To solve this problem, instead of matching impedance, nShield employs *voltage matching*. Since R_{ant} and R_{load} are in series, when $R_{ant} = R_{load}$, the voltage across R_{ant} and R_{load}, denoted as U_{ant} and U_{load}, respectively, are also identical, i.e., $U_{ant} = U_{load} = 0.5U_{ant-open}$. Therefore, an alternative way to achieve the maximum power transfer is to match U_{load} to $0.5U_{ant-open}$. Since $U_{ant-open}$ is a constant value when the harvesting antenna is attached to the initiator, the maximum power trans-

fer can be achieved by letting $U_{load} = 0.5U_{ant-open}$. A key question is how to stabilize U_{load} when system load varies. nShield connects the battery directly to the output of the rectifier, which makes U_{load} stay equal to the voltage of the battery, U_{bat}. Since most batteries have stable output voltage regardless the discharging level and the output current (system load), the optimal energy transfer rate can be always maintained.

However, $0.5U_{ant-open}$ could be difficult to match with U_{bat} in practice, as the harvesting antenna and the energy management circuit are usually separately designed to meet different requirements (e.g., Q-factor, system power consumption, system voltage, etc.). An impedance transformation block, such as L-section circuit or RF transformer [5], can be employed to shift $U_{ant-open}$ to a given voltage. Although an impedance transformation block is not required by our current implementation of nShield, it would be required if nShield employs a Lithium battery (3.6 V). It is also worth noting that, super capacitors are ill-suited for nShield, as their output voltages vary significantly with the discharging levels. To protect the batteries, we use a linear regulator and MOSFET switches to manage the charging. We do not use a switching regulator since it tends to alter the voltage matching point thus reduces the energy harvesting efficiency. Fig. 7 shows the design of energy management circuit of nShield. Our experiment in Section 8.1 shows that nShield can harvest 55 mW power constantly from the NFC initiators on typical smartphones.

5.3 Tag Emulation

As discussed in Section 2, the initiator adopts a low probing rate [21] when no target device is nearby, which only allows limited amount of energy to be harvested. Nevertheless, we show in Section 8.2 that, as long as the host device is active for more than 429 seconds/day, the energy harvested during the probing phase is sufficient for keeping the battery charged. In the rare case when the mobile device is only infrequently unlocked for a long period, nShield may deplete its battery. To address this issue, we adopt a technique called tag emulation to have the initiator significantly increase its duty-cycle. Specifically, nShield emulates itself as a passive ISO14443A tag and responds to the probing messages sent by the initiator. As a result, it triggers the initiator to stay active. This leads to a 10X increase of the initiator output energy, allowing nShield to be rapidly charged. However, this process may interfere with NFC transactions, as the initiator cannot communicate with other target devices when the tag emulation is active. We adopt the following adaptive mechanism to address this issue. First, nShield pauses the tag emulation for 1 second every 2 seconds, allowing the initiator to discover other target devices during the pause. Second, nShield only activates tag emulation when the discharging level of the onboard battery is lower than 30%.

6. ADAPTIVE RF FIELD ATTENUATION

6.1 Attenuator

nShield reduces the risk of being eavesdropped by attenuating the NFC RF field strength using the harvesting antenna. The level of attenuation to the RF field is adjusted by the load of the harvesting antenna. nShield adopts a MOSFET as the variable load, i.e., attenuator to the antenna. The resistance of the MOSFET is controlled by its gate terminal voltage, which is dynamically set by the adaptive RF field attenuation algorithm described in Section 6.2, using an onboard DAC. A novel design of nShield is that the attenuator is multiplexed with the load modulator of the NFC transmitter. This design reduces the cost and size of nShield. Our experiment in Section 8.4 shows that nShield can achieve an attenuation range of 10.86 dB, which is sufficient for the purpose of regulating NFC RF field strength.

6.2 Adaptive RF Field Attenuation Algorithm

nShield adapts the signal attenuation level dynamically to ensure reliable communication between the initiator and the target device. nShield equally divides the whole attenuation range into N discrete levels. The goal of adaptive RF field attenuation is to find the optimal attenuation level in the N levels, with which the attenuated field strength is just enough to support reliable bi-directional communications between the initiator and the target. Fig. 8 illustrates the relationship between Packet Reception Ratio (PRR) and the attenuation levels (AL). nShield tries to use an attenuation level as high as possible, while ensuring the resulted PRR to be close to 1, i.e., high communication reliability. A_{opt} shown on Fig. 8 is the optimal attenuation level.

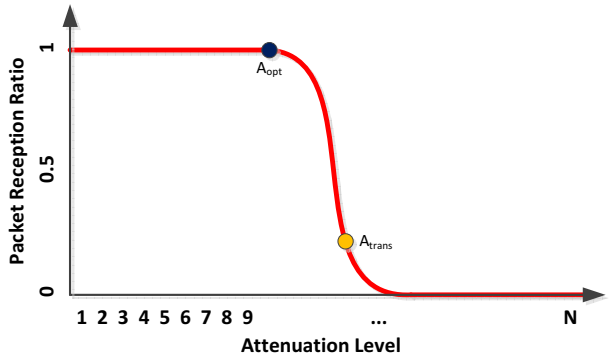

Figure 8: An illustration of the attenuation level vs Packet Reception Ratio relationship.

However, a key challenge in the design of nShield is that, without prior knowledge about the target device, such as reception sensitivity and initiator-target distance, nShield cannot know what RF field strength would support reliable communications. NFC work in a poll-response fashion, in which the target only transmits after it was polled by a message from initiator. We refer to the process of a polling and its subsequent response as a *polling round*. To find out wether an attenuated field strength can support bi-directional communication, the initiator has to attempt a polling round with the attenuation level in question. nShield learns if a polling round is successfully complete, by examining the logic of the polling messages of consecutive polling rounds. In particular, some polling messages, such as the Single Device Detection Request and the Select Request defined in the NFC-A standard, can only be transmitted if the previous polling round succeeds. When overhearing such polling messages, nShield infers that the previous polling round ends successfully.

As shown in Section 8.3, for the passive communication mode, the field strength required for completing the first polling round is lower than that for completing later polling rounds. This phenomenon is caused by insufficient energy left on the tag after the first polling round. Passive tags

rely on the energy from the NFC RF field to operate. After activating the RF field, the initiator pauses for certain time to charge the tag before starting the first polling round. The length of this charging period is usually much longer than the interval between consecutive polling rounds. Even if the RF field strength was not sufficient to sustain the successive polling, the first polling round may still succeed due to the energy harvested from the initial charging period. As a result, for passive communication mode, the success of the first polling round after the activation of the RF field is not a good indicator if the field strength is strong enough for sustaining bi-directional communication. In our design, we deem a field strength sufficient only if it can support the first three consecutive polling rounds.

Algorithm 6.1 *Adaptive RF Field Attenuation*

Input: N: number of attenuation levels.
Output: n_{opt}: optimal attenuation level.
Used sub-function: $Comm(n_i)$: attempt communication with attenuation level n_i. This sub-function returns "success" only if the first three polling rounds are completed successfully with the attenuation level n_i

```
1: N_upper = N
2: N_lower = 1
3: n_opt = N/2
4: while N_upper − N_lower > 2 do
5:    if Comm(n_opt) = success then
6:       N_upper = round((N_upper + n_opt)/2)
7:    else
8:       N_lower = n_opt
9:    end if
10:   n_opt = round((N_upper + N_lower)/2)
11: end while
12: return n_opt
```

An interesting question is that, with N different attenuation levels, in what order should nShield attempt communications. A naive solution is to attempt with all N levels from a high-to-low or low-to-high order, until an attenuation level for supporting reliable bidirectional communication is found. However, this approach incurs high delay (at least several seconds). We adopt the Binary Search Algorithm (BSA) to accelerate the search process. With BSA, the search starts from the middle of all attenuation levels. Depending on whether the following polling rounds are successful or not, BSA discards the lower or higher half of the levels that unlikely contain the optimal level. For example, if any of the three following polling round fails, BSA discards all the levels that are higher than the currently attempted level. BSA repeats this process with the remaining levels until there is only one level left. However, due to the transition region on the PRR-AL curves (see Section 8.3), BSA may fail to locate the optimal attenuation level. This is because whether an attenuation level in the transition region, such as A_{trans} on Fig. 8, can support a successful polling round is probabilistic. When the polling rounds attempted with A_{trans} succeed, all the attenuation levels higher than A_{trans}, including the optimal level A_{opt}, would be discarded. To address this issue, we adopt a modified BSA in nShield. It works in the same way as the original BSA, except that it only discards half of the higher levels after three successful polling rounds. As the transition region of the PRR-AL curve is very narrow (see Section 8.3), this ensures that the optimal level would not be accidentally discarded. Algorithm. 6.1 shows the pseudo-code of the adaptive RF field attenuation algorithm.

nShield exploits the target discovery process, which is always performed by the initiator in the initial phase of the communication, to perform adaptive RF field attenuation. The NFC initiator periodically performs this process by broadcasting NFC discovering probes (at a rate about 3Hz on Android smartphones). If a target NFC device (which can be a tag or another NFC initiator working in active mode) hears this probe, it will send an acknowledgement message back to the initiator. The initiator will then confirm the discovery of the target device by broadcasting a response. The two devices will then exchange a few messages back and forth to learn a few parameters (such as IDs and capabilities). There are several advantages of exploiting this process for adaptive RF field attenuation. First, the NFC target discovery process is mandatory in all NFC communication modes and NFC standards (NFC-A, NFC-B, and NFC-F) [9]. Second, this process does not involve the data payload. The communication conducted during adaptive RF field attenuation might be eavesdropped, due to the possibly high initiator transmission power. However this does not lead to security breach since there is no data payload exchange. Once adaptive RF field attenuation is done, the following data communication is protected from passive eavesdropping. If the adaptive RF field attenuation is not finished yet in the last phase of the target discovery process, nShield will jam the communication to force the initiator to restart the process.

7. IMPLEMENTATION

We implemented a prototype nShield, which is shown in Fig. 6. We use a TI MSP430F2618 as the MCU on nShield. It integrates many low-power components used by nShield, such as comparator, ADC, DAC, and DMA controller. A 4.8 V 20 mAH NiMh battery is adopted to store the harvested energy.

We implement the harvesting antenna using layered tapes and aluminum foil. To maximize the attenuation range, the size of the harvesting antenna should be slightly larger than the antenna on the NFC initiator, so that all magnetic flux generated by the initiator would undergo the attenuation before reaching the target. For example, our prototype antenna attached to Nexus 7 has a dimension of 9.6 cm by 9.6 cm, slightly larger than the NFC antenna in Nexus 7. We build the base of the antenna using 2mm thick layered tapes. We apply the aluminum foil to one side of the base, and cut the foils into 7 mm wide tracks to reduce the series resistance. The tightly coupled tracks increase the inductance of the antenna. The combination of high inductance and low series resistance leads to a high Q-factor (> 100), which is essential for achieving high energy transfer efficiency. The NFC signal reception antenna is prototyped using the same materials and techniques, except that it has much thinner tracks. We use an impedance analyzer to tune the Q-factor of the antenna to the optimal value of 15 [17]. The harvesting and receiving antennas are then glued together. The two prototype antennas can be easily mass-manufactured using flexible thin film circuits.

We implement an NFC transceiver on nShield. The reception path is composed of a peak detector, a comparator, and a software decoder. The RF signal from the antenna is first converted to baseband signal by the peak detector, and

then converted to clean logic levels by the comparator. The decoder is implemented in software on the MCU. To decrease the computational overhead, hardware components on the MCU are adopted to assist the decoding. Specifically, a hardware timer is adopted to timestamp the transitions of the logic levels, and a DMA controller is employed to automatically transfer the timestamps to the RAM. This design automatically collects samples without software intervention, enabling low power asynchronous decoding. The data is then verified using CRC and reported to upper layer protocols. For transmission, nShield adopts the load modulation communication techniques [9], in which the load of the antenna is modulated according to the data to be transmitted. We adopt a high speed MOSFET (Fairchild FDV301N) as the load modulator (multiplexed with attenuator), which can be easily driven by the onboard DAC due to its very low gate driving voltage (less than 1 V). The bridge rectifier is implemented by four NXP PMEG600 low forward drop Schottky diodes to minimize the energy loss on rectifying. To generate accurate baud rates and subcarrier frequencies, a 13.56 MHz crystal oscillator and a hardware clock divider are employed. We implemented the ISO14443A (NFC-A) protocol on nShield, which supports a data rate of 106 kbps. Since the modulation/demodulation tasks are mainly handled by hardware, higher data rates can also be easily supported by nShield. Moreover, since many protocols are implemented in software, nShield can be easily customized to meet the requirements of different applications. As a software-defined radio platform, nShield can also be configured to provide malicious content protection functions [21].

nShield employs several techniques to optimize its power consumption. For example, at runtime, unused components are shut down. The clock rate of the MCU is also dynamically adjusted according to the workload. To further reduce power consumption, nShield enters sleep state when no NFC RF field is detected. During sleep, all onboard components except the low-power time keeping timer are shut down.

8. EXPERIMENTATION

In this section, we study the performance of nShield using a set of experiments. We adopt two initiators (Google Nexus 7 tablet and Adafruit PN532 breakboard) and two tags (Mifare Classic and Mifare Ultralight). We choose these devices not only because they are representative NFC devices on the market, but also due to their diverse characteristics. For example, the Adafruit PN532 breakboard has a large antenna and can transmit a large amount of power (about 450 mW), while Google Nexus 7 has a much smaller antenna and much lower transmission power (about 200 mW). The Mifare Classic tag has an antenna size of a credit card which is very common among passive tags, while Mifare Ultralight only has an antenna size of a coin, which is considered to be a "weak" tag. The testing equipments we use include an Agilent DSOX2024 oscilloscope, an Agilent 34410A benchtop multimeter, an Extech handheld multimeter, and an SDR-Kits VNWA3 Vector Network Analyzer.

8.1 Amount of Harvested Power

We measure the amount of power that can be harvested by nShield, and the power transfer and harvesting efficiency with two experiments in this subsection.

In the first experiment, we employ both of the initiators for testing. The harvesting antenna (shown in Fig. 6) is attached to the back of Google Nexus 7, and to the surface of the PCB antenna on PN532 breakboard. We connect a potentiometer to the antenna as the load. The output voltage and current of the antenna under different loads are measured with an Agilent 34410A benchtop multimeter. A linear regression is applied to the results to compute the internal resistances and the open-circuit output voltages of the harvesting antenna. We then compute the power harvested by the system and the power transferred to harvesting antenna under different loads.

Fig. 9 (a) depicts the harvested power under different antenna output voltages. We can see that the curves are parabolas, with the maximum power of 55 mW at 5 V, and 90 mW at 12 V, respectively, when Google Nexus 7 and PN532 breakboard are used. The amount of power that can be harvested from PN532 breakboard nearly doubles that from Google Nexus 7. This is because PN532 breakboard has a much higher transmission power than Nexus 7, according to our measurement. However, as the antenna is optimized for working with Nexus 7, nShield cannot harvest the maximum amount of power from PN532 breakboard. In particular, the maximum power is harvested at 12 V output and the battery voltage on nShield is only 4.8 V. This voltage mismatch limits the maximum harvested power to be only 57 mW. An impedance matching block is required to shift the open-circuit voltage to around 10 V for PN532 breakboard, as discussed in Section 5.2. On the other hand, nShield can receive the maximum power when working with Nexus 7, due to the tight voltage matching. These results also confirm that a super capacitor is a poor choice for energy storage on nShield, since the voltage of super capacitors varies significantly with its discharging level, resulting a poor voltage matching.

Fig. 9 (b) shows the power transferred to the harvesting antenna at different output voltages. We can see that the transferred power decreases linearly when the output voltage increases. When the output voltage of the harvesting antenna is zero, the antenna receives the maximum power. However, it also delivers virtually no power to the system, resulting in an extremely low power harvesting efficiency, as observed from both Fig. 9 (a) and (b). When the output voltage is about half of the antenna open-circuit voltage, the maximum power is harvested, although the power transferred to the antenna is significantly lower. These results show that, in order to deliver the maximum power to the system, the battery and the harvesting antenna must achieve a voltage matching.

We next evaluate the power harvesting and transfer efficiencies of nShield. We only use Adafruit PN532 breakboard as initiator in this experiment because the transmission power of Nexus 7 cannot be accurately measured due to its packaging. The transmission power of the PN532 board can be obtained by measuring the current draw on the TVDD pin of PN532 chip, which supplies power to its internal coil exciting circuits. The harvesting antenna is connected with a potentiometer which serves as a variable load.

Fig. 10 (a) shows the amount of power transmitted, transferred, and harvested, under different loads to the harvesting antenna. We can see that the transmission power increases when the load becomes lighter. The change of the transmission power is due to the detuning effect, in which the tuning of the initiator's antenna is varied by the mutual coupling between the harvesting antenna and the initiator antenna.

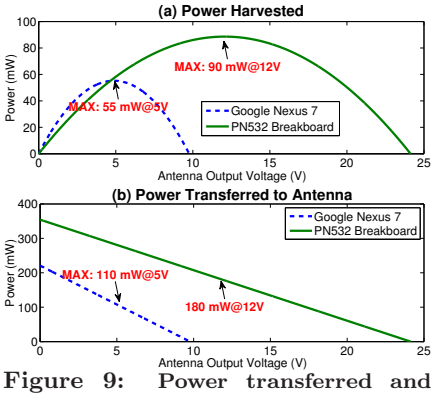

Figure 9: Power transferred and harvested from Nexus 7 and PN532 breakboard.

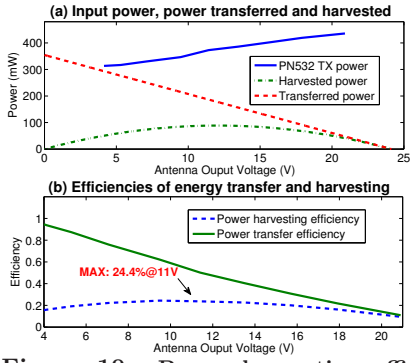

Figure 10: Power harvesting efficiency and power transfer efficiency.

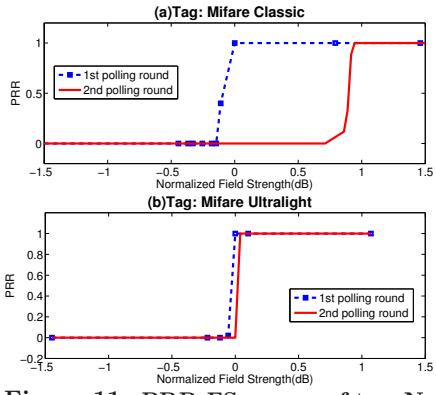

Figure 11: PRR-FS curves of two NFC tags

A heavier (lighter) load to the harvesting antenna creates a slightly stronger (weaker) mutual coupling, which in turn leads to a stronger (weaker) detuning effect. The detuning effect changes the impedance of the antenna, resulting in less power transferred. The highest transmission power is about 440 mW.

Fig. 10 (b) shows the computed energy transfer and harvesting efficiencies. We can observe that the energy transfer efficiency increases linearly with the load to the harvesting antenna, while the energy harvesting efficiency is a parabola curve which peaks at the voltage matching point (11 V). When the output voltage of the harvesting antenna is below 4 V, the energy transfer efficiency is close to 1. At this point, most of the transmitted energy is absorbed by the harvesting antenna, and the strength of the RF field created by the initiator is significantly attenuated. The energy harvesting efficiency peaks at 24.4% when the output voltage of the harvesting antenna is 11 V. We discuss the energy harvesting efficiency in Section 10.

8.2 System Power Consumption and Lifetime

We use an Agilent 34410A benchtop multimeter to measure the power consumption of nShield. The results are summarized in Tab. 1. The most power consuming states are data reception and transmission. This is because the MCU has to work at a higher system clock rate to meet the strict timing requirements of the NFC data reception and transmission, and several system components (e.g., TX control circuit) need to be powered on. Although the idle/RX/TX power consumption are high, their impact on system lifetime is actually insignificant, since nShield spends most of the time in the sleep state with a power consumption of only 23 uW. This is due to the fact that, the NFC initiator is usually inactive most of the time (e.g., when the mobile device is locked), during which nShield is asleep.

Thanks to the large amount of power harvested from NFC transmissions and low power design, nShield can sustain its operation solely on the harvested energy. NFC standard requires initiators to insert long guard time between consecutive polling rounds [9]. As a result, NFC initiators are in idle listening most of the time when activated. This causes nShield to be idle during most of its active period, leading to an average active power consumption of 8.7 mW. As nShield can harvest 55 mW power from an active NFC initiator, it maintains a net power gain of 46.3 mW during its active state. For typical Android devices, the integrated NFC initiators are duty-cycled at 10% [21] during probing. With its low sleep power consumption, the battery on nShield can stay fully charged if the mobile device is unlocked for average 429 seconds per day, which can be met by smartphones and tablets in most circumstances [20][2]. When the discharging level of the onboard battery is low, nShield automatically activates tag emulation, which increases the charging rate by 10X to rapidly charge the battery. Moreover, even when energy harvesting is not possible (e.g., NFC is disabled), the lifetime of a fully charged nShield still exceeds one month, thanks to its low sleep power consumption.

Sleep	Idle listening	RX	TX	Attenuation
23 uW	8.7 mW	13.1 mW	18.1 mw	9.8 mW

Table 1: System power consumption under different states.

The above results show that nShield's capability of harvesting high amount of power plays a significant role in achieving the perpetual operation. As nShield can be only charged when the screen of the device is unlocked, the minimum harvested power for sustaining nShield depends on how the users interact with mobile devices. A recent survey [28] shows that on average U.S. users spend 58 minutes on smartphones per day, which is more than enough for nShield to stay fully charged. However, for light smartphone users, the harvesting power should be sufficiently high. Compared to EnGarde whose harvested power is only about 30 mW[1], nShield decreases the minimum active time of the phone by more than 50% (7.15 min vs 15.5 min).

8.3 Receiver Characteristics

In this subsection, we study the receiving characteristics of passive NFC tags, by measuring the PRR-FS (Packet Reception Ratio vs Field Strength) curves. The purpose of this experiment is to show two key observations based on which the adaptive RF field attenuation algorithm is designed: 1), the transition regions on the PRR-FS curves are very narrow, and 2), the field strength required for completing the first polling round is higher than the subsequent rounds.

We attach a thin aluminum antenna to the back of each tag to measure the field strength, using an Agilent DSOX2024A

[1]The exact amount of harvested power is not given in [21]. However, it is expected to be much lower than 30 mW, due to the load-source mismatch and the loss on rectifying and regulating components.

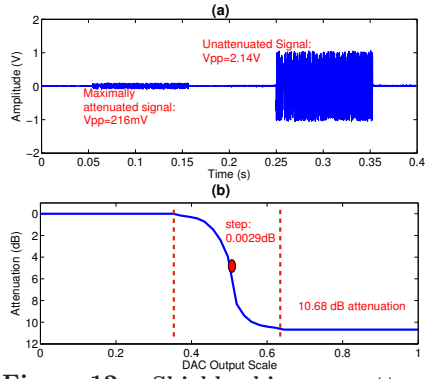

Figure 12: nShield achieves an attenuation range of about 10dB.

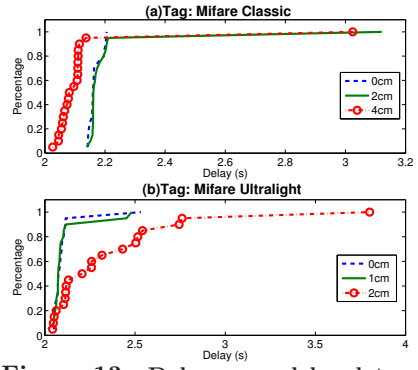

Figure 13: Delay caused by determining attenuation level.

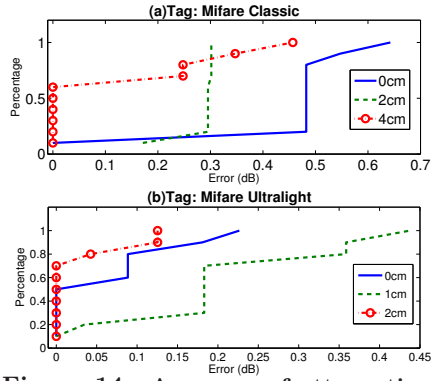

Figure 14: Accuracy of attenuation level determined by nShield.

oscilloscope. A Nexus 7 serves as the NFC initiator in this experiment. We vary the field strength near the tag by changing the distance between the initiator and the tag. The PRR associated with each field strength value is computed from 100 transmissions. The field strength measurements are normalized.

Fig. 11 (a) and (b) show the PRR-FS curves of Mifare Classic tag and Mifare Ultrlight tag, respectively. We can see that, all the curves have narrow transition regions (<0.2 dB) in which the PRR values quickly increase from 0 to 1. We further observe that, Mifare Ultralight tag has a narrower transition region than the Mifare Classic tag (0.05 dB vs 0.2 dB). This is because the Mifare Ultralight tag has a much smaller antenna size, making it more sensitive to the field strength. For each tag, we can see that the field strength required for a successful first polling round is lower than that for the second polling round. As mentioned in Section 6.2, this is due to the fact that the tag has more time to harvest energy before the first round of polling.

8.4 Attenuation Range and Granularity

nShield provides a wide attenuation range and fine attenuation granularity, which allows it to precisely control the strength of the NFC RF field to the optimal level. This subsection evaluates the attenuation range and step that can be achieved by nShield. We manually tune the DAC connected with the attenuator to sweep through its entire voltage output range with a step of 0.05 V. To measure the attenuated signal strength, we use an Agilent probe to form a small loop antenna, and connect the probe to an Agilent DSOX2024A oscilloscope. We record the measured peak-to-peak amplitude (Vpp) of the NFC signal.

Fig. 12 (a) depicts the signals that are maximally attenuated and unattenuated. We can see that nShield can significantly decrease the strength of NFC signals, as the Vpp of the signal decreases from 2.14 V to only 0.216 V after the maximum attenuation level is applied. Fig. 12 (b) shows the computed attenuation levels with different DAC output. We can observe that the effective attenuation region roughly takes about a quarter of the full output scale of the DAC, ranging from 0.8 V to 1.4 V. This is due to the characteristic of the attenuator on nShield, which is a high-speed switching MOSFET. The MOSFET is completely shut down when the gate voltage is below 0.8 V, and is saturated when the gate voltage is above 1.4 V. Therefore, it operates as a variable attenuator only when the gate voltage is between 0.8 V and 1.4 V. The maximum attenuation, 10.86 dB, is achieved when the MOSFET is saturated. We can also observe that the attenuation is nonlinear with the DAC output, resulting in a nonconstant attenuation steps. The maximum step occurs when the MOSFET operates near the middle of the effective attenuation region. For a 16 bit DAC with 2.3 V reference, the maximum step is 0.0029 dB. The wide attenuation range and fine attenuation step allows nShield to precisely attenuate the RF field with wide strength range to the optimal level. This ensures nShield to best protect the security of NFC while maintaining reliable communication.

8.5 Delay of Adaptive Attenuation

The delay caused by the adaptive attenuation algorithm is a critical performance metric for nShield, since a long delay would have significant impact on the user's experience. In this section, we measure the delay introduced by the adaptive attenuation algorithm, using a Mifare Classic tag and a Mifare Ultralight tag. We define the delay as the interval from the time instant when the initiator sends the first probe to the tag to the time instant when the optimal attenuation level is determined. We use the hardware timer on nShield to timestamp these events and measure the delay. For each tag, we measure the delay associated with 3 different optimal attenuation levels, by varying the tag-initiator distances. To illustrate the delay in practical settings, we hold the tags with hands, which introduces small tag-initiator distance variations during communications. We repeat the experiment at each distance for 20 times.

Fig. 13 shows that, most of the delays fall below 2.2 s, while the mean delay is 2.1 s. An interesting phenomenon is that the delay of Mifare Classic incurred at a distance of 4 cm is smaller than those incurred at 2 cm and 0 cm. This is because, the delay is largely proportional to the number of steps that the adaptive attenuation algorithm has to take to find the optimal attenuation level, which varies between 6 and 12 in nShield. Thus a longer communication distance could possibly incur a shorter delay. We also notice that the adaptive attenuation algorithm is resilient to minor tag-initiator distance variation, as nShield can almost always find the optimal attenuation level within 2.2 seconds. We did observe some long delays (3s to 4s), although they are rare (< 5%). Our further investigation indicates that they are caused by occasional initiator halts, in which the initiator pauses its transmission for 1 to 2 seconds, while the RF

field remaining active. Finding the exact reason of this long initiator halt is left for future work.

8.6 Accuracy and Effectiveness of Adaptive Attenuation

We evaluate the accuracy of adaptive attenuation algorithm in estimating the optimal attenuation level in this subsection. The initiator we use in this experiment is the PN532 breakboard. For each tag under test, we evaluate the optimal attenuation level with different tag-initiator distances. We define the optimal attenuation level as the highest attenuation setting that can support successful initiator-tag communications for 10 seconds. We manually determine the ground-truth optimal attenuation level for each tag-initiator distance, by examining all attenuation levels from a high to low order. We use an Agilent probe to form a small loop antenna, and connect the probe to an Agilent DSOX2024A oscilloscope to measure the attenuated RF field strength. We then run the adaptive attenuation algorithm for ten times, and measure the resulted RF field strength of each run.

Fig. 14 shows that, 90% of the estimation errors of the Mifare Classic tag at distances of 0 cm, 2 cm and 4 cm fall below 0.3 dB, 0.34 dB and 0.52 dB, respectively. For the Mifare Ultralight tag at distances of 0 cm, 1 cm and 2 cm, 90% the errors fall below 0.12 dB, 0.16 dB and 0.35 dB, respectively. The mean errors of the two tags are only 0.29 dB and 0.1 dB, respectively. We can observe that Mifare Ultralight tag generally incurs smaller error than Mifare Classic tag. This may be because the Mifare Ultralight tag has a much smaller antenna size, which makes it more sensitive to the field strength. As a result, it has a narrower transition region, which conforms the finding in Section 8.3. This makes Mifare Ultralight tag more responsive to our adaptive attenuation algorithm, resulting in a smaller estimation error.

Next we evaluate the eavesdropping distances achieved with our sniffer at different initiator-tag distances. We record the eavesdropping distances at which the received signal strength of the initiator falls below 100 mV by following the same procedure of the measurement study in Section 3. The results are summarized in Table 2. It can be seen that, for each tag, the eavesdropping distance decreases with the initiator-tag distance. This is because a longer initiator-tag distance requires a stronger signal strength to ensure reliable communication, which increases the eavesdropping distance. We also notice that the Mifare Ultralight tag always incurs longer eavesdropping distances than Mifare Classic tag. This is because the low-sensitivity receiver of the Mifare Ultralight tag requires higher transmission power to maintain reliable communication. The shortest eavesdropping distances for the two tags are 48 cm and 70 cm, respectively. It is worth noting that, even after significant reduction, the resulted eavesdropping distance may still be further than the expected NFC working distance. This is largely due to the fundamental design trade-off of NFC. nShield could apply higher attenuation to decrease the eavesdropping distance to only a few centimeters, but this would significantly reduce the reliability of the NFC communication.

	Initiator-tag Distance			
	0 cm	1 cm	2 cm	4 cm
Classic	48 cm	75 cm	110 cm	140 cm
Ultralight	70 cm	92 cm	122 cm	151 cm

Table 2: Eavesdropping distances after attenuation.

9. RELATED WORK

Near Field Communication (NFC) is a new short-range wireless communication standard evolved from HF RFID technology. Several studies have been conducted on the distance of eavesdropping RFID proximity cards. In [22], the authors measure the passive eavesdropping distance of the communication between a commercial reader and a Philips Mifare card using a wide band sniffer. The results show that the possible eavesdropping distance is more than 4 m [22]. In [23], the authors analyze the security of NFC and estimate the passive eavesdropping distance of NFC to be about 10m. However, this result is not experimentally validated. In [26], the maximum passive eavesdropping distance of NFC is empirically measured to be 30 cm using Mifare tags and an oscilloscope. However, the antennas of Mifare tags used in their experiments are not optimized for eavesdropping. To our best knowledge, our work is the first empirical study on the practical passive NFC eavesdropping distance under realistic experimental settings. We have designed and implemented a prototype NFC sniffer. Its small form factor and high sensitivity demonstrated the feasibility of launching passive eavesdropping attack from distance. In particular, we are able to achieve a 2.4 m eavesdropping distance with our portable NFC sniffer (see Section 3).

Several approaches have been proposed to protect NFC from malicious attacks. A common solution is to modify the OS of mobile devices [23] to enhance the security of NFC. However, the mobile device would become vulnerable if the integrity of the OS is compromised (e.g., by rooting the device)[21]. To address this issue, several systems adopt additional hardware security devices. RFID guardian [30] provides protection by actively jamming suspicious NFC transactions. However, active jamming consumes considerable power and requires bulky hardware (e.g., RF amplifier and large battery), which significantly limits RFID guardian's applications. Proxmark III [12] is a widely used RFID/NFC software defined radio that is capable of detecting an attack, and generating jam signals. However, it must be plugged in as its FPGA-based design consumes significant power (about several hundred milliwatts). Furthermore, none of these approaches can provide anti-eavesdropping protection.

NFC is ideal for energy harvesting, due to the condensed RF field strength generated by its high transmission power and short communication range. Energy harvesting enables a mobile device to replenish its energy in the presence of NFC RF field. The NFC Discover kit [14] from ST include a sensor board can be wirelessly powered by nearby NFC initiators. NFC-WISP [19][10] is a software defined passive tag platform, which is capable of harvesting energy from NFC transmissions and conducting simple sensing and computational tasks. A key difference between the energy harvesting component of nShield and the above two systems is the amount of power harvested. With extensive optimizations to harvesting antenna and energy management circuit, nShield can harvest a power of about 55 mW, compared to mere 10.2 mW and 17.7 mW of NFC Discover kit and NFC-WISP, respectively. The significant improvement

		nShield	EnGarde
NFC radio	Radio type	Software-define radio	Dedicated ASIC NFC radio
	TX capability	Supports NFC-A (implemented), NFC-B, NFC-F HW accelerated SW encoding	Jamming only No TX support
	RX capability	Supports NFC-A (implemented), NFC-B, NFC-F HW accelerated SW decoding	NFC-A, NFC-B, and NFC-F HW decoding
Energy harvesting	Ant. configuration	Dual antenna	Dual antenna
	Optimization	High Q antenna Voltage matching	N/A
	Harvestable power	55 mW constant	maximum 30 mW transferred to antenna
	Max initiator duty-cycle	100% (tag-emulation)	66% (subcarrier)
System pwr consumption	Active	8.7 mW	32.7 mW
	Sleep	23 uW	38.8 uW

Table 3: Comparison of hardware of nShield and EnGarde.

on the energy harvesting efficiency enables nShield to power additional components and perform sophisticated operations to ensure system security.

To date the most relevant work to ours is EnGarde [21]. EnGarde is a hardware NFC security device that jams ongoing malicious NFC transactions. Different from RFID guardian and Proxmark III, EnGarde is optimized for mobile devices and harvests energy from NFC transmissions. However, EnGarde protects NFC by censoring the content of NFC transactions, and hence cannot defend against eavesdropping attacks. We provide a comparison between the hardware of the two systems, which is summarized in Table 3.

nShield is built based on a software-define radio (SDR), which is capable of transmitting to and receiving from NFC initiators. The SDR can be programmed to support standard and custom protocols. However, as SDR relies on software radio stack to decode and encode messages, it tends to incur longer delays. In the case of nShield, hardware components (demodulator, modulator, etc.) are utilized to accelerate the encoding/decoding, which significantly reduces the delay. EnGarde, on the other hand, employs a hardware-based NFC transceiver (TI TRF7970A) that incurs shorter delay than SDR-based transceiver. However, EnGarde only employs the receiving chain of the hardware transceiver, due to its dual antenna configuration. Although EnGarde implements a simple transmitter that can generate jamming signals, it does not support data transmissions. The capability of transmission is critical for tag emulation, which increases the amount of energy harvested from initiator significantly. Another disadvantage of this configuration is the resulted high power consumption, since the hardware transceiver employed by EnGarde is mainly designed for power-hungry NFC initiators. Moreover, the hardware-based transceiver does not support the development of new physical and link-level protocols.

The energy harvesting system of nShield also differs significantly from that of EnGarde. Although a dual antenna configuration is employed by both systems, it is used to meet fundamentally different requirements. Specifically, EnGarde employs the dual antenna configuration for tag proximity detection, while nShield adopts it for improving power harvesting efficiency. The harvesting antenna of nShield is specially designed to achieve high Q-factor. nShield also employs a technique called voltage matching, which carefully matches the output voltage of the antenna to that of the battery to maximize the amount of power harvested. On the another hand, EnGardes does not perform any load-source matching, which significantly limits the power harvesting efficiency. Moreover, EnGarde does not support tag emulation due to the lack of transmission capability, and can only trigger the initiator to raise its duty-cycle to 66% by using jamming. This further lowers the amount of energy harvested. Lastly, the active power consumption of EnGarde is much higher than nShield (32.7 mW vs 8.7 mW), due to the use of hardware-based transceiver.

10. DISCUSSION

Although NFC does not support single-initiator-multiple-target communication, the presence of multiple target devices may lead to collisions in the discovery process. NFC standards require the initiator to resolve collisions observed in discovery process using anti-collision techniques similar to RFID standards, and interact with resolved targets one by one after the discovery process. nShield currently does not consider the multiple tag case. However, nShield can learn if a collision has occurred by overhearing the traffic from the initiator, and act accordingly. However, this extension is left for future work.

nShield significantly improves the amount of harvested energy over existing NFC-based energy harvesting systems [21][14][19][10]. However, compared to specialized wireless power transfer systems [28] that often achieve power harvesting efficiencies of at least 70%, nShield's efficiency is much lower (24.4%). This is mainly because the current NFC initiator is not optimized for high efficiency wireless power transfer. The antenna on NFC transmitter has low Q-factor, which significantly limits the power transfer efficiency. Moreover, achieving high efficiency also requires that the transmitter and receiver must be precisely tuned to the same resonant frequency, which varies with the transmitter-receiver distance. High efficiency inductive power transfer systems adopt several techniques including resonant frequency auto-tuning and antenna impedance auto-tuning to deal with the detuning effects. Unfortunately, these mechanisms are not implemented on NFC initiators.

We acknowledge that a complete redesign of the NFC initiator would be a more effective way to improve physical security. However, such a "clean-slate" approach may prove challenging in practice due to the need of involving many players (from IC to device manufacturers). Moreover, this would leave the legacy devices already shipped exposed to malicious attacks. The next-generation NFC chipsets may

have native transmission control capabilities, which allow mobile devices to configure their NFC transmission power from software. This eliminates the need of accessory security hardware like nShield. In such a case, the adaptive attenuation algorithm of nShield can be integrated by the NFC driver to attenuate the transmission power.

Thanks to the high energy harvesting efficiency, the nShield platform is capable of powering additional hardware components like sensors. Moreover, it can be used as a software-defined radio platform for studying NFC protocols.

11. CONCLUSION

This paper presents a novel, noninvasive security system called nShield to protect NFC against passive eavesdropping. nShield dynamically attenuates the signal strength of NFC transmissions by absorbing the excessive RF energy. nShield intelligently determines the amount of absorbed energy, so that the attenuated signal strength is just enough to sustain successful NFC communications. As a result, in order to launch an attack, the eavesdroppers must be in close proximity of the mobile device, making possible security breach significantly more challenging. We have implemented a prototype of nShield, and evaluated its performance via extensive experiments. We show that nShield can harvest up to 55 mW power, which outperforms two state-of-the-art NFC energy harvesting systems by 1.7X and 3.1X, respectively. Moreover, nShield can accurately attenuate the NFC signal strength in fine granularity, which allows it to provide security protection for a diverse set of NFC platforms. Lastly, nShield only introduces insignificant delay (up to 2.2 s) to NFC data communications.

12. REFERENCES

[1] Adafruit PN532 breakboard. http://www.adafruit.com/products/364.

[2] Americans spend 58 mins a day on smartphones. http://www.experian.com/blogs/marketing-forward/2013/05/28/americans-spend-58-minutes-a-day-on-their-smartphones/.

[3] DES wikipedia site. http://en.wikipedia.org/wiki/Data_Encryption_Standard.

[4] How soon is now: NFC smartphones and physical access control systems. http://blogs.gartner.com/mark-diodati/2011/10/31/how-soon-is-now-nfc-smartphones-and-physical-access-control-systems/.

[5] Impedance matching wikipedia site.

[6] Mobile payments today. http://www.mobilepaymentstoday.com/research/400/Contactless-NFC.

[7] Near field communication (NFC) 2014-2024. http://www.prnewswire.com/news-releases/near-field-communication-nfc-2014-2024-227654461.html.

[8] Near field communication wikipedia. http://en.wikipedia.org/wiki/Near_field_communication.

[9] NFC forum technical specifications. http://www.nfc-forum.org/specs/spec_list/.

[10] NFC-WISP project site. http://www.alansonsample.com/research/NFC-WISP.html.

[11] NXP: PN532 user manual. http://www.nxp.com/documents/user_manual/141520.pdf.

[12] Proxmark 3 project site. http://www.proxmark.org/.

[13] RSA wikipedia site. http://en.wikipedia.org/wiki/RSA_%28cryptosystem%29.

[14] ST discovery kit. http://www.st.com/web/en/catalog/tools/FM116/SC1444/PF253360.

[15] Still not a wallet, NFC has a second life as a safe, simple pairing tool. http://gigaom.com/2013/08/08/still-not-a-wallet-nfc-has-a-second-life-as-a-safe-simple-pairing-tool/.

[16] Strasbourg NFC ticketing moves to commercial launch. http://www.nfcworld.com/2013/07/05/324901/strasbourg-nfc-ticketing-moves-to-commercial-launch/.

[17] Ti:HF antenna design notes. http://www.ti.com/rfid/docs/manuals/appNotes/HFAntennaDesignNotes.pdf.

[18] WEP wikipedia site. http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy.

[19] A. Dementyev, J. Gummeson, D. Thrasher, A. Parks, D. Ganesan, J. R. Smith, and A. P. Sample. Wirelessly powered bistable display tags. In *UbiComp 2013*.

[20] H. Falaki, R. Mahajan, S. Kandula, D. Lymberopoulos, R. Govindan, and D. Estrin. Diversity in smartphone usage. In *Mobisys 2010*.

[21] J. J. Gummeson, B. Priyantha, D. Ganesan, D. Thrasher, and P. Zhang. Engarde: protecting the mobile phone from malicious nfc interactions. In *MobiSys 2013*.

[22] G. Hancke. Practical attacks on proximity identification systems. In *Security and Privacy, 2006 IEEE Symposium on*, pages 6 pp.–333, 2006.

[23] E. Haselsteiner and K. Breitfu? Security in near field communication (nfc). In *Printed handout of Workshop on RFID Security, July 2006*.

[24] J. J. Karakash. *Transmission lines and filter networks*. Macmillan New York, 1950.

[25] M. Kesler. Highly resonant wireless power transfer: Safe, efficient, and over distance. 2013.

[26] H. S. Kortvedt and S. F. Mj?lsnes. Eavesdropping near field communication. In *The Norwegian Information Security Conference (NISK) 2009*.

[27] A. Kurs, A. Karalis, R. Moffatt, J. D. Joannopoulos, P. Fisher, and M. Soljačić. Wireless power transfer via strongly coupled magnetic resonances. *science*, 317(5834):83–86, 2007.

[28] Z. N. Low, R. Chinga, R. Tseng, and J. Lin. Design and test of a high-power high-efficiency loosely coupled planar wireless power transfer system. *Industrial Electronics, IEEE Transactions on*, 56(5):1801–1812, 2009.

[29] C. Miller. Exploring the nfc attack surface. *Proceedings of Blackhat*, 2012.

[30] M. R. Rieback, G. N. Gaydadjiev, B. Crispo, R. F. H. Hofman, and A. S. Tanenbaum. A platform for rfid security and privacy administration. In *LISA 2006*.

[31] D. Welch and S. Lathrop. Wireless security threat taxonomy. In *Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society*, pages 76–83, 2003.