Homeland Security

CYBER-PHYSICAL SECURITY IMPLICATIONS FROM NEAR FIELD COMMUNICATION TECHNOLOGY USE IN ACCESS CONTROL AND MOBILE PAYMENT SYSTEMS

March 10, 2015, 1300 EST

PREPARED BY: OCIA/OPERATIONAL ANALYSIS DIVISION

SCOPE

The Department of Homeland Security's Office of Cyber and Infrastructure Analysis (DHS/OCIA)[1] produces Critical Infrastructure Security and Resilience Notes to address emerging risks to critical infrastructure and provides increased awareness of the threats, vulnerabilities, and consequences of those risks to the Homeland. This product provides situational awareness for Near Field Communication (NFC) developers, users, and critical infrastructure owners and operators that view the integration of NFC technology into secure systems and processes (particularly access control and mobile payment systems) as a viable option for increasing efficiency, effectiveness, and user convenience.

This product has been coordinated with the DHS National Protection and Programs Directorate's (NPPD) Office of Infrastructure Protection's Sector Outreach and Programs Division, NPPD's Office of Cybersecurity and Communications' (CS&C) National Coordinating Center for Communications, NPPD/CS&C's Stakeholder Engagement and Cyber Infrastructure Resilience Division, NPPD's Federal Protective Service, the Department of Treasury, the Commercial Facilities Sector, the Information Technology Information Sharing and Analysis Center, and the Financial Services Information Sharing and Analysis Center.

KEY FINDINGS

- **OCIA assesses that NFC-enabled devices, transactions using this technology, and market revenue derived from these transactions in the United States are expected to grow over the next 3 to 5 years as United States information technology (IT) and telecommunication industries discover new and innovative applications for this technology.**
- **OCIA assesses that the integration of NFC technology into critical systems and functions may provide user flexibility and convenience; however, vulnerabilities associated with data availability, confidentiality, and integrity exist—particularly in some implementation of access control and mobile payment systems.**

[1] In February 2014, the DHS National Protection and Programs Directorate (NPPD) created the Office of Cyber and Infrastructure Analysis by integrating analytic resources from across NPPD, including the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and the National Infrastructure Simulation and Analysis Center (NISAC).

OVERVIEW

NFC, a form of wireless communication between electronic devices like smartphones and tablets, stemmed from advancements in radio-frequency identification (RFID) technology developed in the early 1980s.[2] Based on RFID technology, NFC emerged as an alternative to other wireless technologies for short range data exchange such as Wi-Fi, Bluetooth, and other radio protocols.[3] NFC advertises greater security and connectivity features when compared to other wireless technologies and has emerged as a strong contender as an alternative to the current transaction and payment techniques.[4] NFC uses electromagnetic radio fields to facilitate data exchange between digital devices through magnetic induction, a process whereby an initiating device emits a small electric current which creates a magnetic field that bridges the physical space between devices (see Figure 1).[5]

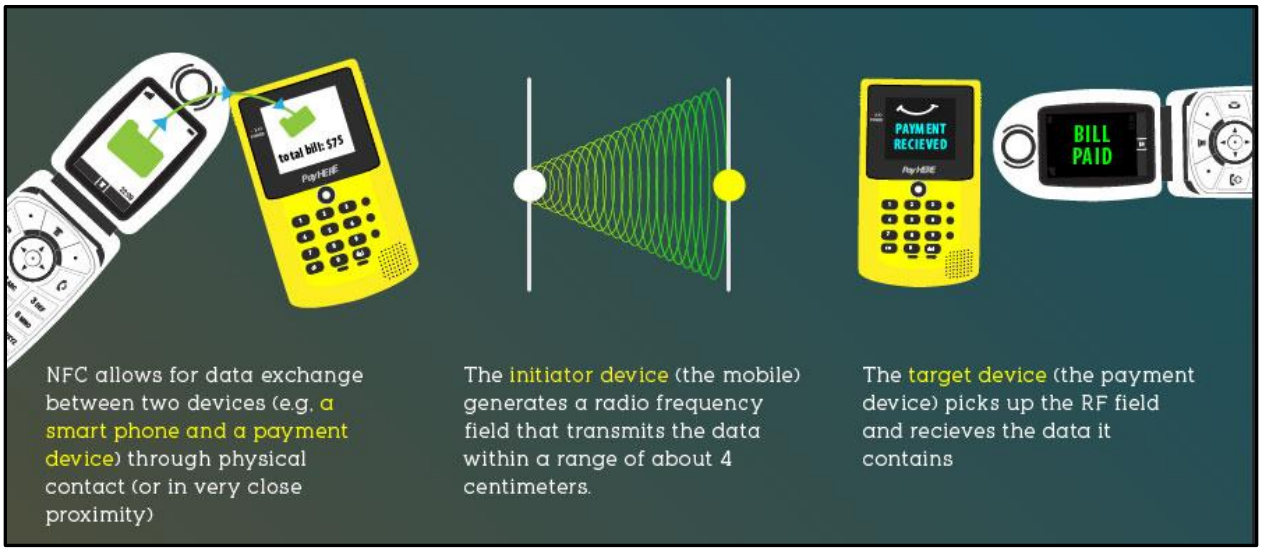

FIGURE 1—HOW NEAR FIELD COMMUNICATION WORKS[6]

NFC-enabled devices contain some or all of the following five elements:

- An NFC protocol stack installed on the device's processor to enable NFC capabilities;
- A mobile wallet that allows users to view NFC related information stored on the device;
- NFC controller chip that manages the flow of information within the device;
- A secure element that acts as a digital vault to store personal and sensitive data; and
- A short-range radio antenna that makes it compatible with contactless cards, terminals, and some RFID tags.[7]

NFC services use a combination of NFC-enabled smartphones, tags, and terminals to provide businesses and consumers with easy, flexible ways to interact with the world around them. NFC tag reading and writing allows users quick and easy access to the web. For example, consumers can touch an NFC-enabled smartphone to NFC tags to access information and download coupons that are affixed to posters, marketing materials, product packaging, signage, and more. NFC also provides peer-to-peer communication allowing people to exchange information instantly, such as business cards and photos. Due to the aforementioned flexibility and uses of NFC technology, utilization of NFC-enabled devices could potentially provide increased functionality to owners and operators in all 16 critical infrastructure sectors.

---

[2] http://www.nearfieldcommunication.org/history-nfc.html, accessed October 8, 2014.
[3] Research and Markets, Near Field Communication (NFC) Market - Global Industry Analysis, Size, Share, Growth, Trends and Forecast, 2013 – 2019, July 2014, http://www.researchandmarkets.com/research/flnvp6/near_field, accessed October 24, 2014.
[4] *Ibid.*
[5] http://apcmag.com/inside-nfc-how-near-field-communication-works.htm, accessed October 8, 2014.
[6] Accountable Worldwide E-Payments, http://www.awepay.com/make-payments-with-near-field-communications-nfc/#, accessed October 9, 2014.
[7] NFC Technologies and Systems by Sarah Clark; http://nfcworld.s3.amazonaws.com/nfc-technologies-and-systems.pdf?AWSAccessKeyId=AKIAJFSN3XR53YRG6YKQ&Expires=141287910&Signature=fEyfGSU4jfL2dQApZMx7i9RqElY%3D, accessed October 9, 2014.

NFC VULNERABILITIES

NFC developers, users, and security professionals should be aware of the vulnerabilities in this technology. Some NFC security risks are:

- Data Corruption and Disruption—Attackers could corrupt or interrupt the data being transmitted in an attempt to block the communication channel.
- Data Manipulation (Man-in-the-Middle)—Perpetrators could attempt to intercept data being transmitted, manipulate it, and send the altered data to the desired destination. It is particularly difficult to achieve this type of attack on an NFC link due to the short distance capability of the communications.
- Eavesdropping—A third party can gain unauthorized access to NFC data being transmitted. Eavesdropping represents the most common vulnerability in NFC.
- Mobile Malware—If malware were implanted on an NFC-enabled device, the malware could identify sensitive information stored on the device and forward this information to the attacker over an NFC channel or the Internet. [8]

SECURITY IMPLICATIONS

NFC GROWTH IN THE UNITED STATES

OCIA assesses that NFC-enabled devices, transactions using this technology and market revenue derived from these transactions in the United States are expected to grow as United States IT and telecommunication industries discover new and innovative applications for this technology.

- NFC technology has been primarily adopted overseas as a fast and convenient short-range wireless communication method which provides users easy and flexible ways to interact. This technology has been quickly spreading throughout the United States. By 2016, some estimates predict that 25 percent of United States consumers will use NFC-enabled devices to pay for goods.[9]
- As depicted in Figure 2, global mobile payment users are expected to grow to 450 million users in 2017 up from 245 million users in 2013 resulting in 54 percent growth. Global mobile transactions are expected to grow to $721B in 2017 up from $235B in 2013, resulting in 67 percent growth. Global NFC transactions are forecasted to grow to $36B in 2017 up from $4.7B in 2013, resulting in 87 percent growth.[10]

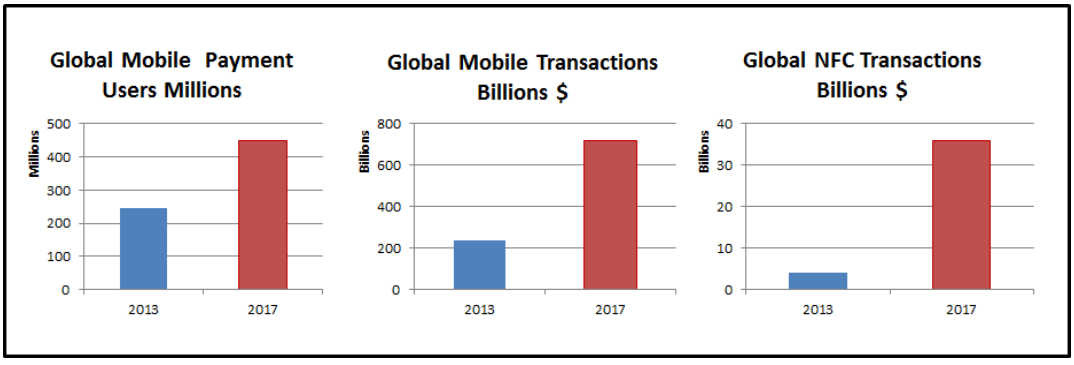

FIGURE 2—FORECAST OF GLOBAL GROWTH IN MOBILE PAYMENT USERS, MOBILE TRANSACTIONS AND NFC TRANSACTIONS

[8] CSO Online, Near Field Communication—The Security Risks, November 1, 2012,
[9] Internet Retailer, North America will be the Top NFC Market in Five Years, April 21, 2011, http://www.internetretailer.com/2011/04/21/north-america-will-be-top-nfc-market-five-years, accessed October 30, 2014.
[10] Global Mobile Payment Industry to Exceed $235 Billion in 2013: Regardless of The Hype, NFC Blighted The Hope; accessed December 17, 2014; http://www.dazeinfo.com/2013/06/21/global-mobile-payment-industry-2013-study/.

NFC APPLICATIONS

OCIA assesses that the integration of NFC technology into critical systems and functions provides user flexibility and convenience; however, vulnerabilities associated with data availability, confidentiality, and integrity exist—particularly in some implementations of access control and mobile payment systems.

ACCESS CONTROL SYSTEMS

The physical security of commercial and government facilities are increasingly dependent on the implementation of cybersecurity procedures and protocols of those facilities. Security companies are piloting programs whereby NFC-enabled mobile devices are used to control physical access to facilities. In 2012, HID Global, a security identity solutions company, successfully piloted a program to integrate mobile technology into Netflix's (provider of on-demand Internet streaming media) and Good Technology's (mobile security company) access control procedures providing employees the ability to open doors within their facilities using NFC-enabled devices.[11] On October 15, 2014, HID Global announced that it successfully completed a second mobile access control pilot with RFI Communications and Security Systems at Netflix, whereby Bluetooth technology (similar to NFC technology, but delivers longer connection ranges) was used to provide greater access control flexibility, allowing employees to open doors and gates while driving or walking near NFC-enabled readers.[12]

Mass transit authorities throughout the United States are now considering integrating NFC technology into fare stations for access control and mobile payments, similar to the mass transit systems in Canada and the Netherlands. These NFC enabled mass transit access control and fare stations would facilitate access control and fare payments through the use of NFC-enabled credit cards, Federal Government identification cards, smartphones, and other devices.[13]

A major concern for facility owners and operators integrating NFC into access control systems is that the cybersecurity postures of facilities are becoming dependent on NFC users' ability to install and properly maintain security software updates. This concern is amplified when considering that many United States businesses are encouraging employees to bring their own devices into the workplace, which can increase the cyber vulnerabilities due to the lack of security software. Smartphones are increasingly vulnerable to cyber attacks, providing cybercriminals with access to personal data and operational control of devices.

- For example, at the 2012 BlackHat Security Conference, a security researcher at Accuvant, an information security company, demonstrated the ability to exploit NFC technology to take control of devices remotely. After successfully hacking three different NFC-enabled smartphones, the individual was able to access photos and text messages, browse the internet, and make unauthorized phone calls without physical contact with the phones or victims.[14]

In 2013, Ponemon Institute conducted a survey of over 4,000 IT and IT security practitioners. In the survey, 74 percent of respondents acknowledged that employee use of mobile devices in the workplace represents a serious risk to their organization and 60 percent revealed that their organization experienced an increase in malware infections as a result of insecure mobile devices in the workplace (see Figure 3).

- Twenty-one percent of respondents were unsure if malware infections increased. Fifty-one percent of respondents stated that their organizations experienced a data breach due to insecure mobile devices while 23 percent of respondents were unsure.

[11] Mobile Access Pilots with Enterprise End Users Completed Successfully, September 26, 2012, http://www.assaabloy.com/en/com/Press-News/News/2012/Mobile-access-pilots-with-enterprise-end-users-completed-successfully/, accessed October 15, 2014.
[12] HID Global and RFI Pilot Use of Smartphones and Gesture Technology for Enterprise Access Control, October 15, 2014, http://www.hidglobal.com/press-releases/hid-global-and-rfi-pilot-use-smartphones-and-gesture-technology-enterprise-access, accessed October 15, 2014.
[13] Washington Metropolitan Area Transit Authority, Pay for Metro with your Smartphone or Watch, September 9, 2014, http://www.wmata.com/about_metro/news/PressReleaseDetail.cfm?ReleaseID=5778, accessed October 30, 2014.
[14] New York Times, From Black Hat: Hackers Demonstrate a Rising Vulnerability of Smartphones, July 26, 2012, http://bits.blogs.nytimes.com/2012/07/26/from-black-hat-hackers-demonstrate-nfc-dangers/?_php=true&_type=blogs&_php=true&_type=blogs&_php=true&_type=blogs&_r=2&, accessed October 21, 2014.

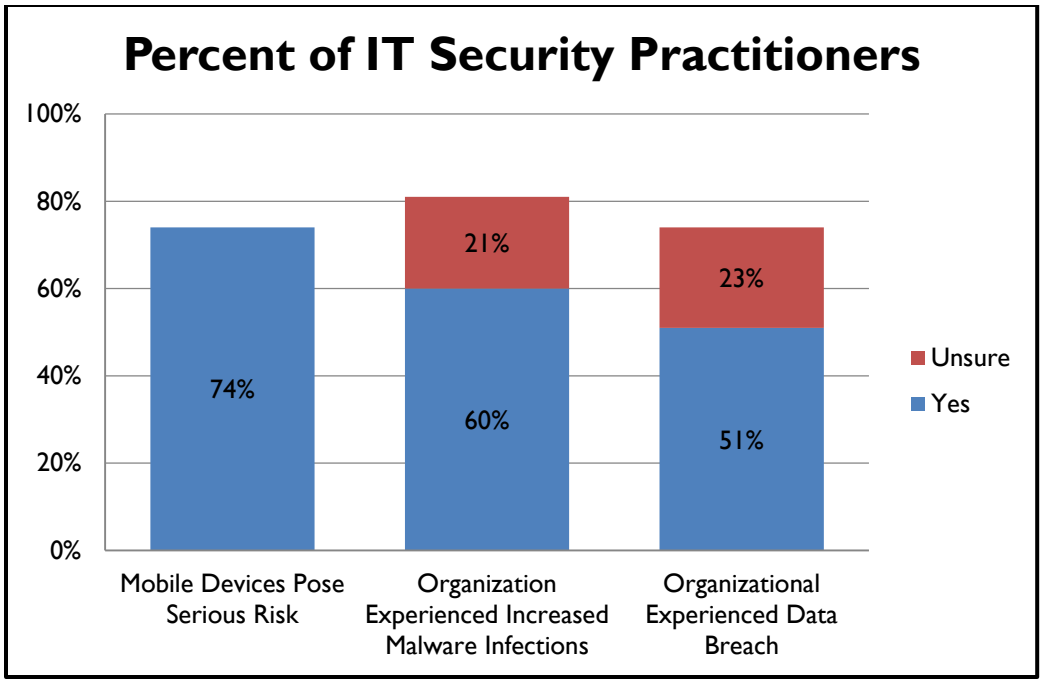

FIGURE 3—2013PONEMON INSTITUTE SURVEY RESULTS

MOBILE PAYMENT SYSTEMS

NFC technology is quickly gaining popularity in the United States with private sector companies integrating this technology into their payment system infrastructure. These mobile payment systems require users to launch mobile payment applications from NFC-enabled smartphones and then wave or touch the device to an NFC-enabled credit card terminal. The user then uses either biometric (finger scan) or passcode authentication to approve the transaction. Subsequently, the transaction is validated by a secure element (relays information to the NFC modem to be processed). The remaining payment processing finalization mirrors the traditional credit card transaction process.[15]

Security is one of the major concerns with NFC payments (see Figure 4). The NFC payment process combines the traditional credit card transaction process with NFC-enabled devices.

[15] CNET, Everything you Need to Know about NFC and Mobile Payments, September 5, 2014, http://www.cnet.com/how-to/how-nfc-works-and-mobile-payments/, accessed October 30, 2014.

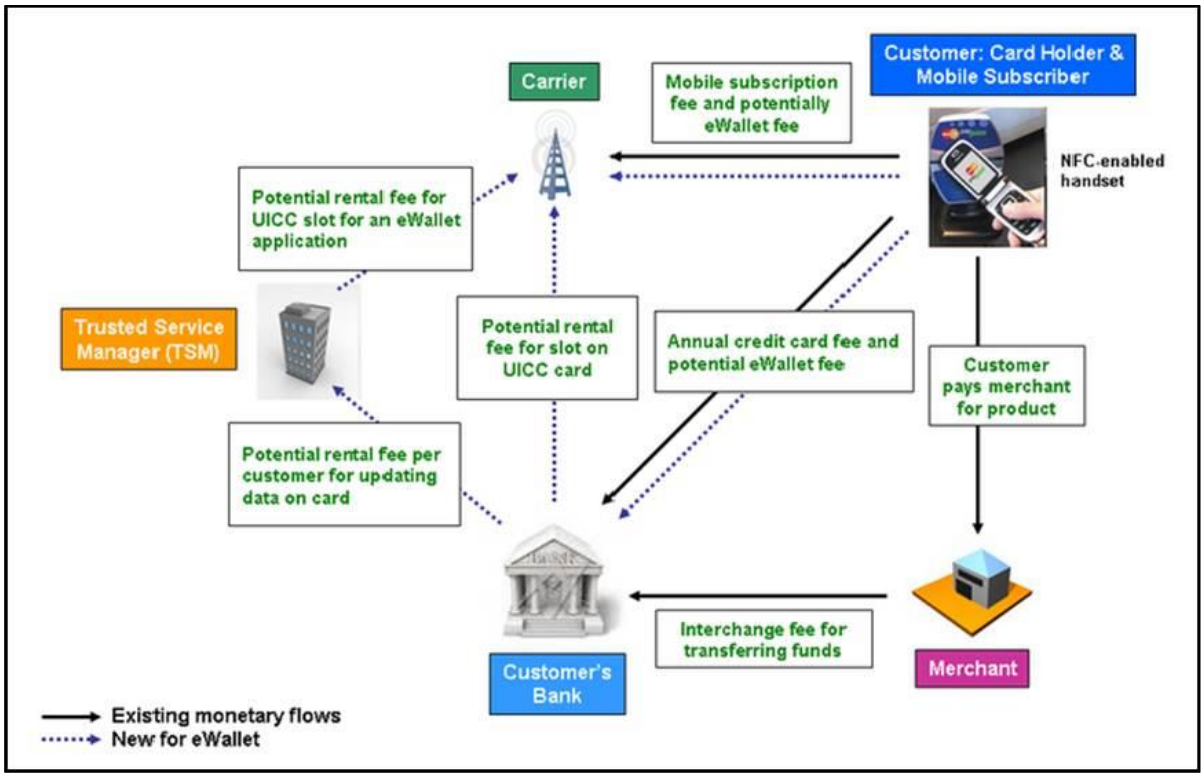

FIGURE 4—DATA AND MONETARY FLOW FOR NFC MOBILE PAYMENT TRANSACTIONS[16]

The increasing availability of NFC-enabled mobile devices and payment systems are key drivers of projected growth in United States markets. NFC-enabled mobile payment applications Google Wallet, Apple Pay, and CurrentC have secure methods for purchasing goods and service. However, security researchers discovered design flaws in the early versions of two of the three common mobile payment applications that could allow cybercriminals to steal personal and financial information through some applications.

- In 2012, a year after the debut of Google Wallet, security researchers hacked a Google Wallet PIN by installing password-cracking software onto a rooted Android smartphone.[17] It is important to note: the study was conducted on the researchers' rooted smartphone, a configuration the majority of consumers do not share.[18]
- At nearly the same time, researchers discovered a simpler way to hack the application by clearing user's Google Wallet application data and using a Google prepaid card tied to the device to gain full access to the owner's funds.[19] While this method required physical access to the device, it did not require root access or any sophisticated hacking skills.
- In October 2014, an NFC digital payment application called CurrentC, developed by a group of retailers (including: Best Buy, CVS, Kmart, Rite-Aid, Target, Walgreens, and Wal-Mart), notified customers that their applications were breached and resulted in thieves obtaining user email addresses.[20]

[16] Craig Conkling Blogspot, NFC and the Mobile Payment Initiative, January 17, 2011, http://craigconkling.blogspot.com/2011/01/nfc-and-mobile-payment-initiative-4.html, accessed October 31, 2014.
[17] Password-Cracking is the process of obtaining privileged control to overcome limitations placed on a device by the hardware manufacturer, http://resources.infosecinstitute.com/10-popular-password-cracking-tools/, accessed December 10, 2014.
[18] CNET, Google Wallet PIN can be Cracked On a Rooted Android Device, February 9, 2012, http://www.cnet.com/news/google-wallet-pin-can-be-cracked-on-a-rooted-android-device/, accessed October 31, 2014.
[19] CNET, Latest Google Wallet Hack Picks Your Pocket, February 10, 2012, http://www.cnet.com/news/google-wallet-pin-can-be-cracked-on-a-rooted-android-device/, accessed October 31, 2014.
[20] Forbes, Apple Pay Rival and Walmart-backed MCX Hacked, User Emails Snatched, October 29, 2014, http://www.forbes.com/sites/ryanmac/2014/10/29/apple-pay-rival-and-walmart-backed-mcx-hacked-user-emails-compromised/, accessed October 31, 2014.

MITIGATION RECOMMENDATIONS

NFC developers, users, and security professionals share responsibilities for mitigating risks to NFC vulnerabilities. The following commonly practiced mitigation measures can be implemented to reduce risk to NFC-enabled devices and the access control and mobile payment systems that rely on this technology.

- Encrypt (i.e., AES 256 bit encryption) the NFC data stream and implement validation controls to help prevent data corruption, data disruption, data manipulation, and eavesdropping.
- Set up an active-passive communication mode and use a secure NFC communication channel to help detect and prevent unwanted third party data access.
- Install a reputable anti-malware program and maintain security software updates and password-protect PINs on NFC devices to help prevent mobile malware attacks.[21]

For more information, contact OCIA@hq.dhs.gov or visit our Website: www.dhs.gov/office-cyber-infrastructure-analysis.

[21] CSO Online, Near Field Communication—The Security Risks, November 1, 2012, http://www.cso.com.au/article/440741/near_field_communication_security_risks_/, accessed October 21, 2014.