Securing NFC Mobile Services with Cloud of Secure Elements (CoSE)

Pascal Urien[1] and Selwyn Piramuthu[2]

[1] Telecom ParisTech, UMR 5141,
23 Avenue d'Italie, 75013, France
[2] Information Systems and Operations Management,
University of Florida, Gainesville, FL 32611-7169, USA
pascal.urien@telecom-paristech.fr, selwyn@ufl.edu

Abstract. The availability of NFC smartphones has facilitated the development of a large number of related applications. Some of these NFC applications necessitate communication with other systems, which may not necessarily be secure, through communication channels and mechanisms that may be open to vulnerabilities. Security is therefore paramount to the success of these NFC mobile services. While Peer-to-Peer (P2P) communication mode is common in mobile NFC applications, it is vulnerable to security-related issues that arise from the use of untrusted devices for storage and to process applications. We propose the concept of a Cloud of Secure Elements (CoSE) where the secure services are hosted by servers rather than by smartphone Secure Elements. We discuss the use of CoSE for mobile payments. We also illustrate how an NFC smartphone may be efficiently used as a bridge between an NFC reader and an Internet server of secure microcontroller that hosts EMV applications.

Keywords: Cloud of Secure Elements, Secure Element, NFC, Security, Mobile Services.

1 Introduction

As the number of applications of smartphones with NFC increases, there is a concomitant need to secure these phones against vulnerabilities that arise from each additional application. Moreover, several applications together can expose the smartphone to new security weaknesses. We propose a new concept that we call the "Cloud of Secure Element" (CoSE) for securing NFC smartphones from vulnerabilities that are associated with the use of their Secure Elements or smartcards.

A smartcard is a tamper resistant micro-controller [1] whose security is enforced by multiple software and hardware countermeasures. It was invented in the 1980s to facilitate electronic payment in situations where both the merchant and the buyer were not connected. The BO' smartcard, used in France by the end of the 20th century generated cryptogram (based on a 3xDES algorithm), realizing the payment proof, and backed up every night via modem connections. Today's electronic payment technology deals with EMV [2] smartcards, that still generate cryptograms (based on

G. Memmi and U. Blanke (Eds.): MobiCASE 2013, LNICST 130, pp. 322–331, 2014.

the 3xDES algorithm) but in a context in which the merchant is connected while the buyer is offline. About 1.5 billion EMV bank cards are scheduled to be in service during 2013 [3]. Apart from the payment market, secure microcontrollers are used for access control purposes such as those that are used in transportation tickets or electronic keys.

Over the last several years, the EMV standard has supported contactless technology [4], named Near Field Communication (NFC [5]) based on inductive coupling at 13,56 Mhz. Furthermore, about one million NFC-enabled smartphones are manufactured every week; NFC modems are logically connected to a secure micro-controller (such as SIM modules) hosted EMV payment applications, and therefore able to perform payment transactions.

Because smartphones are more and more connected to the Internet, it becomes possible to remotely use secure microcontrollers by establishing a logical relay hosted in the mobile, between the NFC links (with a working distances of a few centimeters) and an Internet server hosting secure microcontrollers.

Relay techniques have been discussed in many research publications since 2005 [6][7][8]. Since relay techniques have the potential to create security threats, various countermeasures to such relay attacks have been studied, for example, based on signal round-trip measurements and evaluations [9].

We propose CoSE for mobile smartphones and illustrate this concept, using a platform that we developed using commercially available devices, for payment purposes. We illustrate how a mobile smartphone can be efficiently used as a bridge between a NFC reader and an Internet server of secure microcontroller hosting EMV applications. We also show how an (EMV) application may be downloaded and activated in the server and thereafter remotely used from the phone.

The rest of the paper is organized as follows: Since its introduction, NFC-enabled smartphones have been used in a wide variety of disparate applications. We discuss a select few NFC-enabled mobile smartphone applications in Section 2. NFC P2P applications constitute a majority among different available means. However, researchers and practitioners have identified several vulnerabilities in NFC P2P systems. We discuss some security issues associated with mobile NFC P2P applications in Section 3. We then present and briefly discuss the essentials of CoSE in Section 4. We conclude the paper with perspectives and future directions in Section 5.

2 NFC-Enabled Mobile Applications

With the availability of NFC-enabled mobile phones, both researchers and practitioners have been interested in exploring possible applications of these devices. NFC-enabled smartphones, for example, allows for automating processes (e.g., retail transactions, where these mobile phones provide secure interface between payment systems and retail systems).

Several researchers have considered the use of mobile phones with NFC for pervasive healthcare applications. For example, Sidén et al. [10] study tele-healthcare and assisted living where NFC-enabled mobile phones (Google Nexus S) interact with

RFID tags connected to appropriate sensors to automatically relay information such as the presence of new blood inside a bandaged wound, urine saturation in adult diaper, among others. Hancke and Opperman [11] consider remote monitoring and control systems using NFC and develop an interface that can be used with sensors (e.g., heart rate monitor). While Hancke and Opperman only develop an interface, Morak et al. [12] develop a prototype hardware platform for NFC-supported Bluetooth communication for acquisition and transmission of blood pressure and ECG. They use an analog ECG front-end and an off-the-shelf blood pressure monitor as sensors.

González et al. [13] propose and develop prototypes for the use of mobile phones with NFC and an NFC-phone-based interactive panel for learning environments through touching note, touching cabinet, and touching campus. These are used respectively for communication between teachers and students, increase ease of location of items in a cabinet, and interaction of students and campus buildings whereby the student can easily obtain information on a campus building that is in close physical proximity.

NFC-enabled mobile phones are also used for ticket payments. For example, Widmann et al. [14] discuss seamless integration of electronic ticketing system for public transportation using NFC mobile phones whereby the amount charged is computed based on entry and exit points registered when the NFC-enabled mobile phones are tapped at these points (check-in/check-out principle). They also discuss some issues or constraints with such use of NFC-enabled mobile phones for ticketing applications. For example, they lament the shortage of mobile phones that support card emulation mode and inaccessible secure elements due to issues with trusted service management.

Chaumette et al. [15] discuss the pros and cons of offline and online NFC-enabled mobile phone-based event-ticketing system in terms of user experience, security, economical aspects, reliability and speed of use. The online system requires the existence of Secure Element that stores and retrieves the static ticket identifier in the user's mobile device. In such an online system, no dynamic information (e.g., ticket) is stored in the mobile phone. The static ticket identifier is verified for successful user authorization by the back-end system that processes all dynamic information. The offline system, on the other hand, stores a copy of the ticket in digital format in the mobile phone and this ticket is transferred to the ticket verifier for successful authorization. Based on their evaluation, they find that both online and offline systems offer similar advantages, with a slight edge for the offline system in terms of speed of use and the online system providing a slight edge in terms of user experience.

There is an extensive set of literature on mobile payments using NFC-enabled mobile phones. For example, Mainetti et al. [16] observe the blocking of Secure Elements in mobile devices by smartphone and OS manufacturers and propose a peer-to-peer (P2P)-based framework for Android mobile phones that bypasses the need for special hardware. Monteiro et al. [17] also consider P2P mobile payment systems. Urien and Piramuthu ([18],[19]) present a suite of authentication protocols for NFC-based P2P retail store transaction processing. However, there are some issues in NFC P2P that need to be addressed. We discuss some of these in the next section.

3 Security of P2P Mobile NFC

Several vulnerabilities of P2P mobile NFC security have been identified over the past few years. These vulnerabilities range from relay attacks (e.g., [7]), eavesdropping attacks that are based on the weakness of applications that run in NFC, Denial of Service (DoS) attacks through saturation with communication requests when an on/off switch is not present, message modification attacks, implementation attacks (e.g., [20]), and attacks that are instantiated when the user loses the NFC device.

For example, Miller [20] performed fuzzing test and showed that (with high-level fuzzing) vulnerabilities in parsing of incoming message could be used to open a malicious web page, open an application, image, video, contacts, or documents without any interaction from the user. With a Nokia Meego, he initiated Bluetooth pairing, which allows for access of this device from farther away. Miller also showed that it is possible to take complete control of a mobile phone through NFC, resulting in stolen photos, contacts, as well as the use of this phone to send messages and make phone calls.

Although relay attacks are difficult to prevent using cryptography, this is an active area and we believe that there is some progress in this general area (e.g., [21])

Since NFC is a gateway to all associated devices, this too opens up opportunities for attacks from resourceful adversaries. For example, through fuzzing Mulliner [22] found a vulnerability in the processing of NDEF record payload length. He also discovered a means to spoof smart poster URI by inserting space, tab and newline characters into the title record. He observes that a man-in-the-middle attack can be easily mounted using a web-based proxy. He also created a proof-of-concept NFC worm, through the PushRegistry to intercept all URI NDEF messages, which is activated when a smart poster tag is read. A similar attack was illustrated at the 2012 RSA conference (e.g., [23]) with the modification of the NFC tag on a smart poster that resulted in the smartphone browser to open a phishing site. A variant of this attack was shown by [24] that allows an attacker to automatically execute USSD codes without the user's permission which could cause serious damage such as permanent kill of the SIM card, remote wipe, among others.

4 Cloud of Secure Elements

The experimental Cloud of Secure Elements platform comprises four elements.

- A service kiosk. It is a personal computer equipped with a contactless smartcard reader that is used to establish an NFC session in accordance with the reader/writer card-emulation paradigm. A free software (an EMV explorer tool) drives the reader and parses the content of a contactless EMV bank card
- A mobile. The smartphone is an NFC-enabled device (Nexus S), which supports the card emulation NFC mode. It runs a mobile application that establishes a logical relay between the kiosk and a remote grid of secure elements.

- A grid of secure elements (GoSE). It is a server (manufactured by [25]) that handles hundreds of smartcards. These secure microcontrollers host various trusted software, such as EMV payment applications.
- An administration console. It is a TCP/IP client that remotely manages the content of the smartcards hosted by the GoSE, thanks to protocols compliant with the Global Platform [26] standards

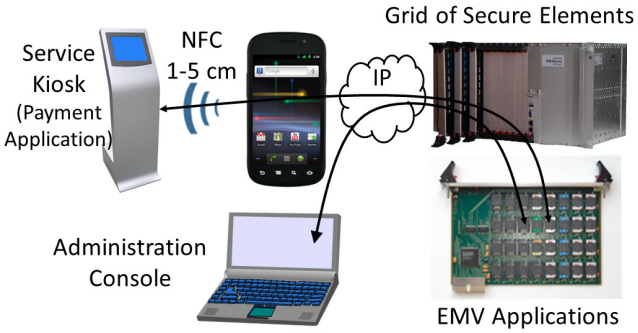

Fig. 1. A prototype of Cloud of Secure Elements

4.1 The Service Kiosk

The service kiosk is instantiated by a laptop equipped with a contactless smartcard reader. A free EMV explorer tool is used in order to parse and display the content of EMV NFC cards. This software works with physical PVC cards. It also transparently works with a mobile connected to the Grid of Secure Elements.

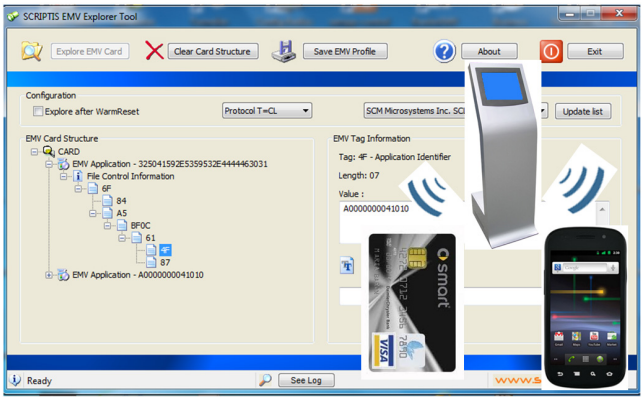

Fig. 2. The NFC service Kiosk

4.2 The Mobile

The platform works with an android smartphone (Nexus S), running the Gingerbread operating system. We use a software patch released by [27] providing software card emulation. It defines a new class, named "android.nfc.tech.IsoPcdA" that implements three procedures (connect, isConnected, and transceiver), similar to those available for the legacy android.nfc.tech.NfcA class.

A proxy application establishes a logical relay between the service kiosk and the GoSE. It is connected to the remote grid server, identified by its IP address and port number. Upon connection, it sends a hello-message, acknowledged by the server whose response packet may contain a request to setup a secure channel. This optional feature was not activated by the experimental platform.

When the mobile is tapped against the kiosk reader, a NFC link is established between the two devices. The kiosk (i.e. the EMV explorer tool) transmits ISO7816 [28] requests thereafter relayed by the proxy to a smartcard plugged in the GoSE, which returns ISO7816 responses.

Because this model of mobile supports NFC payment facilities (for example the Google Wallet), the service kiosk is generally not aware of the relay operations. However, counter measures based on round-trip time evaluations could possibly detect unusual computing latency when communication time dominates computing time by at least a few factors of magnitude, and is induced by heavy network traffic.

4.3 The Grid of Secure Elements

A Secure Element (SE) is a secure microcontroller, equipped with host interfaces such as ISO7816, SPI or I2C. The security is enforced by multiple logical and hardware countermeasures. Usually it runs a Java Virtual Machine (JVM) and therefore it is able to execute small applications (whose size is about a few 10KB) written in Java. The popular form factor for SE is smartcards, of which about 6 billion were produced in 2012 [3], for use in SIMs, bank cards, or passports.

Command	Topic
CONTENT	Return the list of used slots
USE	Select a slot
FREE	Release a slot
RESET	Reset a Secure Element
APDU	Send an ISO7816 request and get a response

Fig. 3. Summary of the SIM array commands

The grid of smartcards is a TCP/IP server that hosts a set of secure microcontrollers. Thanks to a dedicated Grid-Protocol, software running in these tamper-resistant devices may be handled from anywhere at any time.

Our server consists of a mother rack (SIM Array [25]) that manages up to 13 daughter boards, equipped with at most 32 smartcards. A single server holds a maximum of 416 SEs. Each SIM Array is connected to the Internet and has an IP address and manages a TCP server. An ASCII-oriented protocol, whose main commands are listed by figure 3, provides the functionalities needed for the grid inventory and the routing of ISO7816 commands toward a smartcard plugged in the server and identified by a number. Each SE is identified by its plugged slot number.

4.4 The Administration Console

During the grid lifecycle, it is required to download or remove applications in smartcards. The Global Platform committee [26] manages a set of standards to provide these services that include downloading applications, activation and deletion (see figure 4).

Commands	Topic
SELECT	Activate an embedded application. The Issuer Security Domain (ISD) is the application in charge of GP operations
INITIALIZE UPDATE	Initialize mutual authentication with ISD
EXTERNAL AUTHENTICATE	Ends mutual authentication with ISD
DELETE	Delete a package or an application
INSTALL	Allocate memory before package loading or instantiate an application
LOAD	Load a package

Fig. 4. Summary of the GP commands

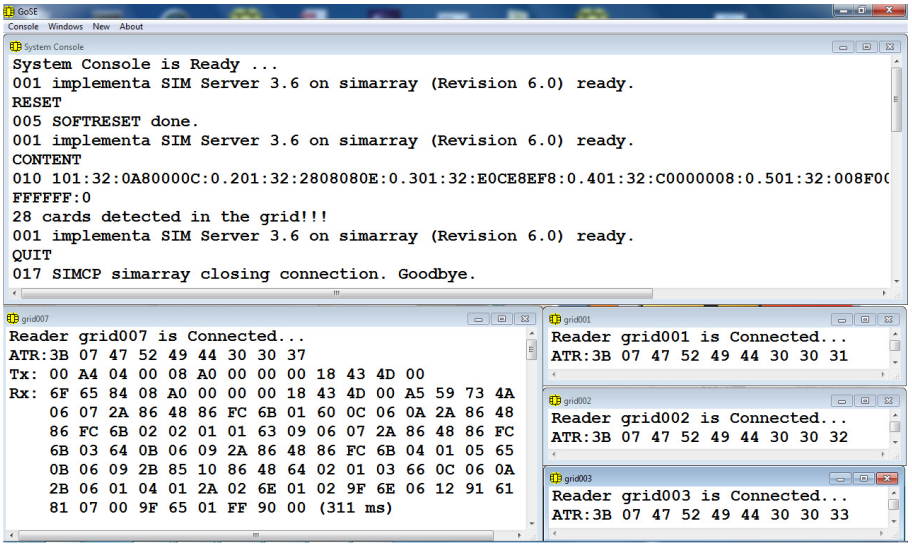

Fig. 5. The administration console

GPShell [24] is an open software running over the PC/SC API. It is a script interpreter that supports the main GP (version 2.0 and 2.1.1) facilities, illustrated by figure 5, and used to load, instantiate, delete, and list embedded applications in smartcards. The GPShell tool has been modified thanks to a logical bridge between PC/SC and the grid protocol. The administration console enables remote download, activate and delete embedded applications in secure micro-controllers. In the demonstration it is used for downloading or removing EMV software in the SIM array.

5 Perspectives and Future Works

This paper demonstrates that the Cloud of Secure Elements concept may work in the current technological landscape. Existing devices, such as NFC EMV cards, can be virtualized and readily migrated from consumer pockets towards the cloud.

NFC communications are not secure in terms of information privacy and integrity. As an illustration we are currently designing for NFC P2P a secure stack (named LLCPS [30]) based on the well-known TLS protocol.

Obviously there are no standards for data exchanges with the CoSE, both for service and management purposes. Furthermore the security of such sessions is a very sensitive topic. In a recent paper [31] we made a tentative list of issues that need to be solved in order to build and use secure cloud of secure elements. A first protocol (Remote APDU Call Secure – RACS) has been recently proposed in [34] in order to fulfill these requirements.

The CoSE technology could be used in the cloud, in order to provide a high trust environment, relying on tamper-resistant devices such as smartcards. This would offer an alternative to technologies based on Virtual HSM (Hardware Secure Module) described in [32].

European projects, like SecFuNet (Security for the Future Internet [33]), work toward this general direction.

References

[1] Jurgensen, T.M., et al.: Smart Cards: The Developer's Toolkit. Prentice Hall PTR (2002) ISBN 0130937304
[2] https://www.emvco.com/
[3] http://www.eurosmart.com/publications.html
[4] MasterCard® PayPass™, M/Chip, Acquirer Implementation Requirements, v.1-A4 6/06
[5] ISO/IEC 18092, Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1) (April 2004)
[6] Hancke, G.: A Practical Relay Attack on ISO 14443 Proximity Cards (January 2005)
[7] Francis, L., Hancke, G., Mayes, K., Markantonakis, K.: Practical NFC peer-to-peer relay attack using mobile phones. In: Ors Yalcin, S.B. (ed.) RFIDSec 2010. LNCS, vol. 6370, pp. 35–49. Springer, Heidelberg (2010)

[8] Roland, M.: Applying recent secure element relay attack scenarios to the real world: Google Wallet Relay Attack, technical report (August 2012)
[9] Reid, J., et al.: Detecting Relay Attacks with Timing-Based Protocols. In: Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security (2007)
[10] Sidén, J., Skerved, V., Gao, J., Forsström, S., Nilsson, H.-E., Kanter, T., Gulliksson, M.: Home Care with NFC Sensors and a Smart Phone. In: Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL), vol. 150, pp. 1–5 (2011)
[11] Hancke, G.P., Opperman, C.: A Generic NFC-enabled Measurement System for Remote Monitoring and Control of Client-side Equipment. In: Proceedings of the Third IEEE International Workshop on Near Field Communication, pp. 44–49 (2011)
[12] Morak, J., Kumpusch, H., Hayn, D., Modre-Osprian, R., Schreier, G.: Design and Evaluation of a Telemonitoring Concept Based on NFC-Enabled Mobile Phones and Sensor Devices. IEEE Transactions on Information Technology in Medicine 16(1), 17–23 (2012)
[13] González, G.R., Organero, M.M., Kloos, C.D.: Early Infrastructure of an Internet of Things in Spaces for Learning. In: Proceedings of the Eighth IEEE International Conference on Advanced Learning Technologies (ICALT), pp. 381–383 (2008)
[14] Widmann, R., Gruenberger, S., Stadlmann, B., Langer, J.: System Integration of NFC Ticketing into an Existing Public Transport Infrastructure. In: Proceedings of the 4th International Workshop on Near Field Communication, pp. 13–18 (2012)
[15] Chaumette, S., Dubernet, D., Ouoba, J., Siira, E., Tuikka, T.: Architecture and Comparison of Two Different User-Centric NFC-Enabled Event Ticketing Approaches. In: Balandin, S., Koucheryavy, Y., Hu, H. (eds.) NEW2AN 2011 and ruSMART 2011. LNCS, vol. 6869, pp. 165–177. Springer, Heidelberg (2011)
[16] Mainetti, L., Patrono, L., Vergallo, R.: IDA-Pay: An Innovative Micro-Payment System Based on NFC Technology for Android Mobile Devices. In: Proceedings of the 20th IEEE International Conference on Software, Telecommunications and Computer Networks (SoftCOM), pp. 1–6 (2012)
[17] Monteiro, D.M., Rodrigues, J.J.P.C., Lloret, J., Sendra, S.: A Hybrid NFC–Bluetooth Secure Protocol for Credit Transfer among Mobile Phones. In: Security and Communication Networks (2013), doi:10.1002/sec.732
[18] Urien, P., Piramuthu, S.: Framework and Authentication Protocols for Smartphone, NFC, and RFID in Retail Transactions. In: Proceedings of the 8th IEEE International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), pp. 77–82 (2013)
[19] Urien, P., Piramuthu, S.: LLCPS and SISO: A TLS-Based Framework with RFID for NFC P2P Retail Transaction Processing. In: Proceedings of IEEE International Conference on RFID, pp. 152–159 (2013)
[20] Miller, C.: Don't Stand So Close to Me: An Analysis of the NFC Attack Surface (July 25, 2012), http://www.blackhat.com/usa/bh-us-12-briefings.html#miller
[21] Urien, P., Piramuthu, S.: Identity-Based Authentication to Address Relay Attacks in Temperature Sensor-enabled Smartcards. In: Proceedings of the European Conference on Smart Objects, Systems and Technologies (Smart SysTech), Erlangen/Nuremberg (2013)
[22] Mulliner, C.: Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones. In: Fourth International Conference on Availability, Reliability and Security (ARES), pp. 695–700 (2009)

[23] Ries, U.: "Phishing via NFC," The H Security (March 2, 2012), http://www.webcitation.org/6BzrM8Qmp
[24] Borgaonkar, R.: USSD/Android Dailer vulnerability (June 2012), http://www.webcitation.org/6DW71H3uK
[25] http://www.implementa.com/products/sim-array
[26] http://www.globalplatform.org/
[27] Lee, E.: NFC Hacking: The Easy Way, DEFCON 20 (July 2012)
[28] ISO 7816, Cards Identification - Integrated Circuit Cards with Contacts
[29] http://sourceforge.net/p/globalplatform/wiki/GPShell/
[30] Urien, P.: LLCPS: A New Security Framework Based on TLS For NFC P2P Applications in the Internet of Things, IEEE CCNC 2013 (January 2013)
[31] Urien, P., Piramuthu, S.: Towards a Secure Cloud of Secure Elements Concepts and Experiments with NFC Mobiles. In Proceeding of the CTS 2013 Conference (May 2013)
[32] AWS CloudHSM Getting Started Guide, Kindle Edition, Amazon WEB Services (2013)
[33] SECFUNET, a research project funded by the European Commission's Framework Programme 7 and CNPq, the Brazilian National Council for Technological and Scientific Development, http://www.secfunet.eu
[34] IETF Draft, Remote APDU Call Secure (RACS), draft-urien-core-racs-00 (August. 2013)