INSO - Industrial Software
Institut für Rechnergestützte Automation | Fakultät für Informatik | Technische Universität Wien

Exposé zur Bachelorarbeit

Durchführung einer Relay-Attacke durch Interception der Android NFC-Schnittstelle

Betreuer: Thomas Grechenig

Michael Peyerl
1326027
033 534
Software & Information Engineering

25.01.2018

.....
Thomas Grechenig

Exposé zur Bachelorarbeit

1 Problemstellung

Seit der Einigung auf die Entwicklung von Near-Field-Communication (NFC) durch Sony und Philips im Jahr 2002 [6] hat sich die Technologie stark weiterentwickelt. Das NFC Forum [15] entwickelte zahlreiche Spezifikationen und die Frage nach Sicherheitsrisiken und -maßnahmen des neuen Kommunikationsmittels wurde vielfach behandelt [1, 4, 7, 10, 11, 14]. Im Jahr 2018 findet die NFC-Technologie Anwendung in zahlreichen unterschiedlichen Gebieten, von Autorisierung und Authentifizierung über mobile Haustürschlüssel bis zu bargeldlosem Bezahlen. Letztere ist höchstwahrscheinlich die bekannteste und am weitesten verbreitete Anwendung der relativ jungen Entwicklung. In nahezu jeder Debit- [1] oder Kreditkarte ist bereits ein NFC-Chip integriert, über welchen an Point-of-Sales (POS) - Terminalen bargeldlos bezahlt werden kann. Zusätzlich verfügt ebenfalls der Großteil der heutzutage benutzten Smartphones über eine NFC-Schnittstelle, welche von Anwendungen benutzt werden kann, um mit einer auf dem mobilen Gerät gespeicherten Debit- oder Kreditkarte zu bezahlen. Mit steigender Prominenz kontaktloser Zahlungen über NFC, wird die Frage nach den Sicherheitsrisiken der Bezahlmethode immer relevanter. Ein Risiko, welches bereits vielfach erforscht wurde, welches allerdings nicht vollständig verhindert werden kann, ist die sogenannte Relay-Attacke [2, 3, 5, 8, 9, 13, 16]. Bei diesem Angriff werden die NFC-Signale, die von einem POS-Terminal ausgehen, unverändert über einen zweiten Kommunikationskanal an ein weiteres Gerät (meistens werden hierfür Smartphones benutzt) gesendet. Dieses zweite Gerät befindet sich in unmittelbarer Nähe des Opfers und sendet diesem die empfangenen Signale über NFC. Die vom Opfer generierten Antworten werden wiederum unverändert an das erste Gerät gesendet, welches die Antwortsignale an das Terminal zurückgibt [11]. Auf diese Art und Weise kann die kurze Distanz von NFC-Kommunikation überbrückt werden und so beispielsweise mit fremden Karten bezahlt werden, ohne dass diese sich in der Nähe des Terminals befinden. Die Durchführbarkeit dieser Attacke wurde bereits vielfach bewiesen und auch Gegenmaßnahmen wurden in der Literatur diskutiert. Es ergibt sich allerdings die noch nicht behandelte Fragestellung, ob es möglich ist, das Gerät des Opfers selbst (die NFC-Schnittstelle) so zu modifizieren, dass die NFC-Antwortsignale selbständig an ein weiteres mobiles Gerät gesendet werden, welches sich in der Nähe eines Terminals befindet. Sollte diese Angriffsmethode erfolgreich durchgeführt werden können, stellt sich in weiterer Folge die Frage nach Gegenmaßnahmen, um diese spezielle Ausführung einer Relay-Attacke zu verhindern.

2 Zielsetzung/Motivation

Durch diese Arbeit soll untersucht werden, ob bzw. wie es möglich ist, die Kommunikation einer Zahlungsanwendung mit der NFC-Schnittstelle so zu manipulieren, dass, nachdem NFC-Signale empfangen wurden, die Antworten über eine zweite Verbindung an ein anderes Gerät gesendet werden. Dieses befindet sich in der Nähe eines POS - Terminals und leitet die empfangenen Signale weiter. Dies ist eine spezielle Art einer Relay-Attacke, bei der allerdings im Gegensatz zu den meisten anderen Anwendungen dieser Angriffsweise nur ein Angreifer-Gerät erforderlich ist. Es wird außerdem davon ausgegangen, dass Root-Rechte auf dem Opfer-Gerät genutzt werden können, um die beschriebene Modifikation durchzuführen. Darüber hinaus soll die Round-Trip-Time der NFC-Signale gemessen werden. Das ist "die Zeitspanne, die erforderlich ist, um ein Signal von einer Quelle über das Netzwerk zum Empfänger zu senden und die Antwort des

[1] http://www.kreditkarten.info/faq/was-ist-eine-debitkarte/

Empfängers wiederum über das Netzwerk zurück zum Sender zu transportieren."[12]. Das Signal, das über das Netzwerk gesendet wird (die sekundäre Verbindung) ist in diesem Fall die Application Protocol Data Unit (APDU) [2]. Ein Ziel der Arbeit ist daher die erfolgreiche Durchführung dieser speziellen Relay-Attacke bzw. die Modifikation des Opfer-Gerätes. Als weiteres Ziel sollen basierend auf Zeitmessungen der Signale Gegenmaßnahmen gefunden werden bzw. evaluiert werden, ob diese Attacke verhindert werden kann und wie eine Verhinderung möglich ist. Darüber hinaus kann durch die Ergebnisse dieser Arbeit ein Grundstein gelegt werden um in weiterer Forschung zu untersuchen, ob die vorgestellte Modifikation des Opfer-Gerätes für weitere Angriffe oder Malware verwendet werden kann. Die Ergebnisse sollen in erster Linie dazu dienen, schädliche Nutzung zu unterbinden.

3 Methodik

In einem ersten Schritt wird ein Prototyp einer Android Mobile Payment Applikation mithilfe von Host-based Card Emulation (HCE)[3] entwickelt. Dieser soll keine vollständige Zahlungs-Funktionalität zur Verfügung stellen, sondern in erster Linie in der Lage sein, mit einem POS-Terminal über die NFC-Schnittstelle des Smartphones zu kommunizieren. Das POS-Terminal wird durch einen Terminal Simulator[4] auf einem Windows PC emuliert. Eine weitere Android-Applikation soll für die Kommunikation zwischen dem Opfer- und dem Angreifer-Gerät sorgen, wobei als sekundärer Kommunikationskanal eine drahtlose Verbindung über Bluetooth, WLAN oder das mobile Internet denkbar ist. Diese Kommunikations-Anwendung soll darüber hinaus auf dem Opfer-Gerät die HCE-App aktivieren. Das Relay-Attack-Szenario ist in Abbildung 1 zur Veranschaulichung dargestellt.

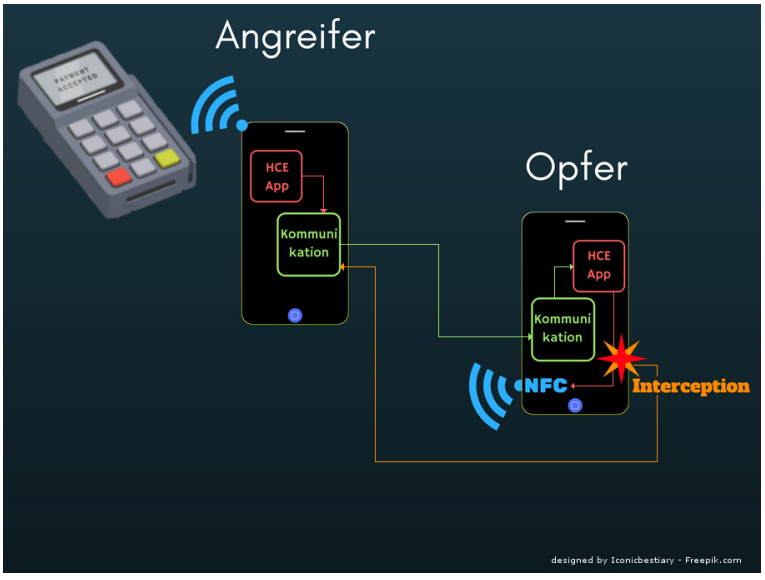

Abbildung 1: Relay-Attack-Szenario

[2]https://de.wikipedia.org/wiki/Application_Protocol_Data_Unit
[3]https://developer.android.com/guide/topics/connectivity/nfc/hce.html
[4]https://www.terminalsimulator.com/

Diese Anwendungen sollen nativ mithilfe der Programmiersprachen Java und/oder Kotlin entwickelt werden. Nach erfolgreicher Implementierung soll recherchiert werden, auf welche Art und Weise die Kommunikation zwischen Android-App und der NFC-Schnittstelle des Smartphones auf das Angreifer-Gerät umgeleitet werden kann, um mithilfe der generierten Antwort-Signale auf dem POS-Terminal zahlen zu können. Hierfür wird es möglicherweise notwendig sein, mit dem Android-Framework direkt zu arbeiten bzw. ein System-Service (möglicherweise in C++) zu entwickeln. Schlussendlich soll die beschriebene Relay-Attacke erfolgreich durchgeführt werden. Wurden diese Schritte abgeschlossen, wird evaluiert, wie ein derartiger Angriff verhindert werden kann. Um das zu erreichen, werden die Zeiten gemessen, die die NFC-Signale vom Opfer zum Angreifer und zurück benötigen. Basierend auf diesen Messungen kann festgestellt werden, ob es sinnvoll ist, zeitbasierte Protokolle zu entwickeln, welche diese Art von Angriff verhindern können. Falls der Rahmen der Arbeit dadurch nicht gesprengt wird, können weitere Gegenmaßnahmen getestet werden.

4 State of the Art

In zahlreichen Studien wurde bereits festgestellt, dass NFC Relay Attacken mit mobilen Geräten, die über eine NFC-Schnittstelle verfügen, einfach und ohne zusätzlichen Aufwand sowie ohne spezielles Fachwissen durchführbar sind und somit eine reelle und gefährliche Bedrohung für NFC-getriebene Services wie vor allem für mobile Zahlungen darstellen. Im Jahr 2005 zeigten Ziv Kfir und Avishai Wool in einer der ersten Arbeiten über Relay Attacken [16] "Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems"[13], wie es mithilfe selbstgebauter Geräte möglich ist, das Signal einer Smartcard über eine Entfernung von 50 Meter an den NFC-Reader zu senden. Darüber hinaus wird auch beschrieben, wie die Distanz der Smartcard zum Proxy-Gerät auf bis zu 50 cm (um einen Faktor 5) erhöht werden kann. Zur Entstehung dieser Arbeit war für die Durchführung einer Relay-Attacke noch zusätzliche Hardware sowie elektrotechnisches Wissen notwendig.
Ohne zusätzliche Hardware können die Autoren der Arbeit "Practical NFC Peer-to-Peer Relay Attack Using Mobile Phones"[8] 5 Jahre später zeigen, wie mithilfe von zwei NFC-fähigen Mobiltelefonen die Peer-to-Peer Verbindung zweier weiterer NFC-fähiger Mobilgeräte durch eine Relay-Attacke weitergeleitet werden kann. Die NFC-Verbindung wird dabei über MIDlets [5] realisiert. Darüber hinaus wird in dieser Arbeit diskutiert, wie Relay-Attacken verhindert werden können, wobei Gegenmaßnahmen, die auf dem Standort der Geräte basieren, näher betrachtet werden.
In Ihrem Artikel "Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones"[9] zeigen Lishoy Francis et al. ein Jahr später, wie mithilfe selbstentwickelter MIDlet-Applikationen eine Relay-Attacke über zwei handelsübliche Mobiltelefone durchgeführt werden kann. Nachdem ein mobiles Gerät als Proxy-Reader sowie das andere als Proxy-Token konfiguriert wurden, war es möglich die NFC-Signale in einem Test-Zahlungssystem sowie von einem e-Reisepass erfolgreich weiterzuleiten und in beiden Fällen wurden die Daten vom NFC-Reader akzeptiert.
Mit fortschreitender Entwicklung wurden Relay-Attacken zunehmend einfacher. Xiquing Chu beschreibt in seiner Masterarbeit [5] eine Relay-Attacke, die mit zwei Android Geräten durchgeführt wird, wobei keine zusätzliche Hardware und kaum zusätzliche Software benötigt wird. Zur Entstehung dieser Arbeit war die Android Version 4.4, welche Host Card Emulation einführt, soeben neu erschienen, weshalb der Autor noch eine ältere Android Version mit Cyanogenmod 9 verwendet. Zusätzlich wird die Zeit gemessen, die die einzelnen Kommandos benötigen und

[5] https://de.wikipedia.org/wiki/MIDlet

dabei wird festgestellt, dass die Relay-Attacke innerhalb der Frame Waiting Time (die maximale Antwortzeit nach Ende der Daten des Readers) [3] durchgeführt werden kann. Abgesehen davon kann die Frame Waiting Time von Angreifern manipuliert werden und ist somit nicht für die Verhinderung einer Relay-Attacke geeignet [3].
Darüber hinaus beschreiben D. Cavdar et al. in ihrer Arbeit Ä practical NFC relay attack on mobile devices using card emulation mode"[3], wie ein handelsübliches Smartphone ohne Hard- oder Software-Änderungen nur mithilfe einer selbstentwickelten App, die Host Card Emulation benutzt, verwendet werden kann, um Daten über NFC von einem anderen Gerät zu stehlen und diese bei einem NFC-Reader wiederzuverwenden, um sich unautorisierten Zugriff zu einem System zu verschaffen. Bemerkenswert hierbei ist, dass für die erfolgreiche Durchführung der Attacke nur ein einzelnes Smartphone ausreicht.
Eine ähnliche Arbeit liefern José Vila et al. [16], die eine Android-Applikation entwickelt haben, welche dem Gerät die Möglichkeit gibt, sowohl als NFC-Reader als auch als Smartcard zu operieren. Mithilfe dieser Anwendung gelang es den Autoren eine Relay-Attacke eines Zahlungssystems von New York nach Madrid über 5775 km durchzuführen.
Thomas Bocek et al. [2] führen ähnlich wie bereits zuvor beschrieben mithilfe zweier Android-Geräte, auf welchen Cyanogenmod installiert wurde, eine Relay-Attacke an öffentlichen POS-Terminals durch. Zusätzlich werden Gegenmaßnahmen wie Time Measurement und Distance Bounding diskutiert.

5 Inhaltsverzeichnis

Literatur

[1] Ali Alzahrani u. a. “NFC security analysis and vulnerabilities in healthcare applications”. In: *Communications, Computers and Signal Processing (PACRIM), 2013 IEEE Pacific Rim Conference* (2013). URL: http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=6625493 (besucht am 25. 01. 2018).

[2] Thomas Bocek u. a. “An NFC Relay Attack with Off-the-shelf Hardware and Software”. In: *10th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2016* (2016). URL: https://link.springer.com/chapter/10.1007/978-3-319-39814-3_8 (besucht am 15. 01. 2018).

[3] D. Cavdar und E. Tomur. “A practical NFC relay attack on mobile devices using card emulation mode”. In: *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (2015). URL: http://ieeexplore.ieee.org/document/7160477/?reload=true (besucht am 15. 01. 2018).

[4] Naveed Ashraf Chattha. “NFC — Vulnerabilities and defense”. In: *2014 Conference on Information Assurance and Cyber Security (CIACS)* (2014). URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6861328 (besucht am 25. 01. 2018).

[5] Xiquing Chu. “Relay attacks of NFC smart cards”. Magisterarb. Norwegian University of Science und Technology - Trondheim, 2014. URL: https://brage.bibsys.no/xmlui/bitstream/handle/11250/262988/742061_FULLTEXT01.pdf?sequence=1&isAllowed=y] (besucht am 15. 01. 2018).

[6] Sony Corporation und Philips. *PHILIPS AND SONY ANNOUNCE STRATEGIC CO-OPERATION TO DEFINE NEXT GENERATION NEAR FIELD RADIO-FREQUENCY COMMUNICATIONS*. 2002. URL: https://www.sony.net/SonyInfo/News/Press_Archive/200209/02-0905E/ (besucht am 24. 01. 2018).

[7] Gauthier Van Damme und Karel Wouters. *Practical Experiences with NFC Security on mobile Phones*. 2009. URL: https://www.esat.kuleuven.be/cosic/publications/article-1288.pdf (besucht am 25. 01. 2018).

[8] Lishoy Francis u. a. “Practical NFC Peer-to-Peer Relay Attack Using Mobile Phones”. In: *International Workshop on Radio Frequency Identification: Security and Privacy Issues* (2010). URL: https://link.springer.com/chapter/10.1007/978-3-642-16822-2_4 (besucht am 15. 01. 2018).

[9] Lishoy Francis u. a. *Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones*. 2011. URL: http://modsec.zimmerle.org/wireless-sec-papers/Practical%20Relay%20Attack%20on%20Contactless%20Transactions%20by%20Using%20NFC%20Mobile%20Phones.pdf (besucht am 15. 01. 2018).

[10] Ernst Haselsteiner und Klemens Breitfuß. *Security in Near Field Communication (NFC)*. 2006. URL: https://s3.amazonaws.com/academia.edu.documents/8360228/002%20-%20security%20in%20nfc.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1516912912&Signature=sib36KcnIO0AAbNxqdEjxuId6TY%3D&response-content-disposition=inline%3B%20filename%3DSecurity_in_near_field_communication_NFC.pdf (besucht am 25. 01. 2018).

[11] Infosec Institute. *Near Field Communication (NFC) Technology, Vulnerabilities and Principal Attack Schema*. 2013. URL: http://resources.infosecinstitute.com/near-field-communication-nfc-technology-vulnerabilities-and-principal-attack-schema/ (besucht am 24. 01. 2018).

[12] ITWissen.info. *RTT (round trip time*. 2014. URL: http://www.itwissen.info/round-trip-time-RTT.html (besucht am 25. 01. 2018).

[13] Z. Kfir und A. Wool. "Picking Virtual Pockets using Relay Attacks on Contactless Smartcard". In: *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)* (2005). URL: http://ieeexplore.ieee.org/abstract/document/1607558/ (besucht am 15. 01. 2018).

[14] Gerald Madlmayr u. a. "NFC Devices: Security and Privacy". In: *2008 Third International Conference on Availability, Reliability and Security* (2008). URL: http://ieeexplore.ieee.org/abstract/document/4529403/?part=1 (besucht am 25. 01. 2018).

[15] *NFC Forum*.

[16] José Vila und Ricardo J. Rodríguez. "Practical Experiences on NFC Relay Attacks with Android". In: *International Workshop on Radio Frequency Identification: Security and Privacy Issues* (2015). URL: https://link.springer.com/chapter/10.1007/978-3-319-24837-0_6 (besucht am 15. 01. 2018).