Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Formal security analysis of near field communication using model checking

Nikolaos Alexiou [a], Stylianos Basagiannis [b,*], Sophia Petridou [c]

[a] School of Electrical Engineering, KTH Royal Institute of Technology, Stockholm, Sweden
[b] Research Centre of United Technologies, Cork, Ireland
[c] Department of Applied Informatics, University of Macedonia, Thessaloniki, Greece

ARTICLE INFO

Article history:
Received 10 September 2015
Received in revised form 10 February 2016
Accepted 9 March 2016
Available online 15 March 2016

Keywords:
Near field communication
Probabilistic model checking
Relay attack
Security analysis
Wireless communication

ABSTRACT

Near field communication (NFC) is a short-range wireless communication technology envisioned to support a large gamut of smart-device applications, such as payment and ticketing. Although two NFC devices need to be in close proximity to communicate (up to 10 cm), adversaries can use a fast and transparent communication channel to relay data and, thus, force an NFC link between two distant victims. Since relay attacks can bypass the NFC requirement for short-range communication cheaply and easily, it is important to evaluate the security of NFC applications. In this work, we present a general framework that exploits formal analysis and especially model checking as a means of verifying the resiliency of NFC protocol against relay attacks. Toward this goal, we built a continuous-time Markov chain (CTMC) model using the PRISM model checker. Firstly, we took into account NFC protocol parameters and, then, we enhanced our model with networking parameters, which include both mobile environment and security-aware characteristics. Combining NFC specifications with an adversary's characteristics, we produced the relay attack model, which is used for extracting our security analysis results. Through these results, we can explain how a relay attack could be prevented and discuss potential countermeasures.

1. Introduction

Contactless radio communications, such as near field communication (NFC), have become popular short-range solutions for establishing secure ad-hoc connections. NFC allows low data rate links of 106, 212 and 424 Kbps to transfer data over short distance (up to 10 cm) (Anon., 2013a, 2013b). Due to its simplicity, the NFC technology is a suitable candidate for an increasing number of applications including mobile payments, e-ticketing, access control systems and in-vehicle communications (Almuairfi et al., 2014; Coskun et al., 2011; Kang et al., 2015; Madlmayr et al., 2008). The integration of NFC in smartphones, in particular, transforms user devices into mobile wallets (Google Wallet, 2013) and carriers of authentication and authorization proof that is exchanged via short-range NFC channels.

Just as in typical RFID communications, two NFC-enabled devices can be paired in peer-to-peer mode or, alternatively, operate in card emulation mode for mobile-to-infrastructure communications. However, NFC systems are susceptible to attacks leaving the security an open issue (Madlmayr et al., 2008). In particular, relay attacks are easy to deploy and pose a serious threat for security of NFC systems, as well as for the acceptability of the technology. During a relay attack, the adversary acts as a transparent intermediary between two distant

* Corresponding author.
E-mail address: basagis@utrc.utc.com (S. Basagiannis).
http://dx.doi.org/10.1016/j.cose.2016.03.002
0167-4048/

victim devices, i.e. an NFC reader and an NFC target, and maliciously *forces* an NFC link between them. This is achieved using a fast and transparent relay channel that connects the two victim NFC devices, which eventually believe they are in close proximity and can communicate directly with each other. The attack leverages on the absence of localization evidence of the NFC protocol, as well as on the fast relaying property of the adversarial channel, which eliminates the distance between the victim devices.

A prevalent countermeasure for relay attacks against NFC systems is the distance-bounding protocols (Drimer and Murdoch, 2007; Hancke and Kuhn, 2005). In a nutshell, they provide guarantees regarding the maximum distance between two communicating devices. Therefore, they prevent an attacker from faking the close-proximity property that is necessary to launch the relay attack. However, distance bounding has not yet been adopted to secure real world NFC systems, or is envisioned to do so in the near future. Although possible reasons are out of scope of this paper, we briefly mention the following:

1. Secure and reliable hardware implementations that can guarantee the tight timing constraints required by distance-bounding protocols come with additional cost. The cost of several hardware implementations has not been defined yet (Drimer and Murdoch, 2007). However, the technology's acceptability to new applications can be slowed down or, even worse, hindered by additional costs.
2. Software-only implementations of distance-bounding protocols sound promising, but suffer from a series of important issues like reliability and efficiency, not only in real world scenarios but also in lab environments. Thus, even if possible, software-only distance-bounding solutions will need extensive work in order to be adopted (Francis et al., 2011).

It is therefore obvious that we need methods to analyze and evaluate the security of real world NFC systems. Formal analysis techniques constitute the perfect candidate (Basagiannis et al., 2008, 2011) since they can be applied to analyze the security of systems in a rigorous manner. Model checking techniques offer the additional advantage of automated rigorous analysis, which is beneficial for proprietary systems and new communication technologies (Paparrizos et al., 2011), like NFC. In this paper, we propose a general framework that exploits formal analysis and especially probabilistic model checking to analyze the security of NFC protocol against relay attacks. Toward this goal, we firstly built a highly configurable continuous-time Markov chain (CTMC) model which takes NFC protocol specifications into account using the PRISM model checker environment (Kwiatkowska et al., 2011). Then, we enhanced our basic model with networking parameters, including both mobile environment and security-aware characteristics. In this way, we succeeded in combining an NFC transaction with the interference of an adversary, in order to construct our relay attack model. Based on this model, we extracted security analysis results, which can be exploited during protocol's design and implementation to evaluate the probability of a relay attack for a variety of protocol and adversary's characteristics and, thus, to explain how the attack could be prevented and to discuss potential countermeasures.

The remainder of this paper is organized as follows. Related work on relay attacks against NFC and the novelty of the proposed analysis are discussed in Section 2. Section 3 provides the NFC protocol specifications and describes the relay attack. Section 4 is a brief introduction to the probabilistic model checking preliminaries. The relay attack model along with security analysis details are presented in Section 5, while in Section 6 the results of the analysis are discussed. In Section 7 we set a market-wise NFC discussion and, finally, in Section 8 we conclude with remarks of the presented work as well as future directions.

2. Related work

There is currently a major push for adopting NFC technology and its security guaranties in general purpose mobile devices (Marketsandmarkets.com, 2013; Rebello, 2011). At the same time, proliferation of NFC technology has also attracted the attention of malicious users. To address these challenges, the current bibliography focuses on analysis and techniques related to the resiliency of NFC to attacks.

In 2005, Kfir and Wool studied relay attacks on contactless smartcard communications focusing on operating ranges issues (Kfir and Wool, 2005). They highlighted the fact that the nominal range of 10 cm between the reader and the target can be circumvented by exploiting the attackers' hardware, consisting of a proxy and a mole. In practice, they showed that an extension of 50 m is feasible in the reader-to-proxy range, while mole-to-target range can be also extended up to 40–50 cm. This entails that range limitations imposed by ISO/IEC 14443 standard can be overcome, increasing the attackers' probabilities.

The same year, Hancke designed a low-cost system and executed a relay attack up to a distance of 50 m, connecting a proxy and a mole through an UHF antenna (Hancke, 2005). His implementation was simple and cheap and introduced a small delay of 15–20 μs, which is possible because the communication is relayed as analog data. The alternative approach of encoding/decoding and buffering the data packets requires additional processing time causing longer delay.

Recently, Issovits and Hutter presented a practical relay attack which exploits a number of mechanisms of the ISO/IEC 14443 standard, i.e. the Frame Waiting Time (FWT), the Negative Acknowledges (NAKs) recovery functionality and the Waiting Time eXtensions (WTXs) (Issovits and Hutter, 2011). More specifically, they used an RFID-tag emulator with programming capabilities and a Nokia 6212 NFC mobile phone as proxy and mole correspondingly and a Bluetooth link between them as a relay channel. The legitimate parties, i.e. an ISO/IEC 14443 compliant reader and tag, exchange information using RFID links. The proposed attack reaches average delays of 85.3 ms. However, although they exploit protocol mechanisms for their attack and they propose some protection measures compliant with the standard, their approach is protocol dependable and restricted to their specific attack scenario. Moreover, the proposed countermeasures of checking the transmission parameters are not proven rigorously.

The practicability and complexity of relay attacks have been greatly facilitated due to the availability of NFC-enabled mobile phones. Francis et al. (2010) showed that it is possible to relay