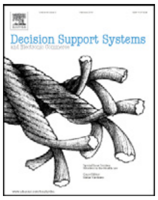
Decision Support Systems 59 (2014) 28–36

Contents lists available at ScienceDirect

Decision Support Systems

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



Elliptic curve-based RFID/NFC authentication with temperature sensor input for relay attacks

Pascal Urien [a], Selwyn Piramuthu [b,c,*]

[a] INFRES, TELECOM ParisTech, 75013 Paris, France
[b] Information Systems and Operations Management, University of Florida, USA
[c] RFID European Lab, Paris, France

ARTICLE INFO

Article history:
Received 21 June 2013
Received in revised form 28 August 2013
Accepted 16 October 2013
Available online 24 October 2013

Keywords:
RFID
Mutual authentication
Distance bounding protocol
Relay attack

ABSTRACT

Unless specifically designed for its prevention, none of the existing RFID authentication protocols are immune to relay attacks. Relay attacks generally involve the presence of one or more adversaries who transfer unmodified messages between a prover and a verifier. Given that the message content is not modified, it is rather difficult to address relay attacks through cryptographic means. Extant attempts to prevent relay attacks involve measuring signal strength, round-trip distance, and ambient conditions in the vicinity of prover and verifier. While a majority of related authentication protocols are based on measuring the round-trip distance between prover and verifier using several single-bit challenge–response pairs, recent discussions include physical proximity verification using ambient conditions to address relay attacks. We provide an overview of existing literature on addressing relay attacks through ambient condition measurements. We then propose an elliptic curve-based mutual authentication protocol that addresses relay attacks based on (a) the surface temperature of the prover as measured by prover and verifier and (b) measured single-bit round-trip times between prover and verifier. We also evaluate the security properties of the proposed authentication protocol.

1. Introduction

There is a continual trend for systems to gravitate toward automation in order to improve process efficiency as well as to reduce errors and vulnerabilities (e.g., [47,48]). Examples of such systems include mobile payment through Near Field Communications (NFC)-enabled smartphones and object identification with RFID tags. While the general efficiency and effectiveness in these systems are improved with automation, other challenges arise as a direct consequence. Among these, some of the pressing challenges include those related to privacy and security of the user in these systems as well as attacks from resourceful adversaries.

Several vulnerabilities have been identified in existing systems in a wide variety of applications such as automobiles, mobile payments. For example, in keyless start system, the driver does not need to insert a physical key to start the car. It was shown (e.g., [5]) that it is relatively easy to clone such a car key. In general, the inclusion of human in the loop (e.g., to open the car door) was assumed to reduce such vulnerabilities since starting a car without gaining entry to it is not of much use to the adversary. However, [19] show how both a keyless entry and start system in an automobile can be compromised. Several researchers have studied mobile payment systems with smartphones, and have shown that these transactions are vulnerable due to untrusted readers as well as the presence of adversaries who intermediate the transactions between smartphones and readers (e.g., [20,16,32]). While outright cloning accounts for some of these vulnerabilities, relay attacks play a significant role as well.

Relay attacks occur when an adversary simply relays signals between (honest) reader and tag without any modification. Since the signal content is not modified by the adversary, almost none of the extant cryptographic RFID authentication protocols are immune to such attacks. Relay attacks work equally well on mutual as well as one-way authentication protocols. Unless it explicitly participates in such an attack (e.g., mafia fraud attack, discussed below), a prover is generally unaware of a relay attack when it occurs. For example, an adversary can use relay attack to remotely start a car (e.g., [5]) or complete a mobile payment transaction (e.g., [20]).

Relay attacks and their variants have been discussed in the literature since at least a few decades ago (e.g., [10]: p.75; [14]), and there have been several attempts by researchers over the years to reduce the occurrence probability of such attacks. Among the most common are those that measure the round-trip time taken to transfer a single bit between the verifier and the prover with the assumption that gross deviation from a pre-calculated (based on the speed of light and the expected distance between prover and verifier) range is a cause for concern. This is also implemented in recently introduced MIFARE cards (e.g., MIFARE Plus X), which is an improvement over their earlier cards (e.g., [21]). However, the measurement of round-trip distance as a proxy for physical proximity determination is fraught with issues including the fact that it is difficult to identify relay attacks that are mounted from

[*] Corresponding author.
E-mail address: selwyn@ufl.edu (S. Piramuthu).

0167-9236/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.dss.2013.10.003

relatively short distances (e.g., a few kilometers) due to the inherent latency (e.g., default of 5 ms in ISO 14443 proximity cards) that is present in these transactions.

Almost all existing authentication protocols that use a variant of this idea also involve some, even if minimal, computation (e.g., to pop a stack or compare values to choose among several stacks). Any authentication protocol that measures the signal round-trip time is very sensitive to the relative time taken for computation vs. communication [36]. In other words, if computation at the receiver end is multiple orders of magnitude when compared with the round-trip signal travel time, it is difficult to measure the latency that is due only to round-trip travel times. Moreover, the computation time also depends on the ambient conditions of the RFID/smartcard processor and a large variation has the potential to wash away differences in signal round-trip times for prover and verifier that are anywhere from inches to miles apart from each other.

Signal strength has also been suggested as a means to verify physical proximity of prover and verifier. However, it is easy to modify signal strength. It is also easy to use a stronger signal to read from outside the expected read-range (e.g., BlueSniper 'rifle' [25]). Moreover, such skimmers are relatively inexpensive (≈$100) and can be assembled using off-the-shelf electronics hobbyist supplies and tools (e.g., [26,30]).

Since round-trip distance measurement and signal strength have their issues, researchers have resorted to identifying other means to address relay attacks. These include the use of environmental sensors and close coupling with another device (e.g., [7]) since these, unlike a request to the user to push a button for example, do not require any action on the user's part and therefore do not interfere with the automated authentication process between prover and verifier.

The premise that supports the use of ambient conditions to confirm the relative (physical distance) separation between prover and verifier is that their ambient conditions must be the same or close enough when these devices are in close physical proximity to each other. Ambient conditions are measured at the prover and verifier and the measurements are then compared against each other. Ambient conditions in this context include sound, light, temperature, among others. It is known that light and sound measurements are influenced significantly by the orientation of the measuring device with respect to the (light or sound) source (e.g., reflected, incident) and any existing interferences (e.g., standing waves). This necessitates the sensor-generated values to be appropriately compensated and normalized, which is extremely difficult due to the sensitivity of the readings to the relative reader and source orientations and the challenges in measuring the relative real-time orientations. We decided not to consider light or sound sensors due to these issues.

We consider the use of environmental sensors, specifically temperature sensors, to reduce the occurrence probability of relay attacks. We develop a mutual authentication protocol based on elliptic-curve cryptography that seamlessly integrates both authentication and a means to address relay attacks. We chose elliptic-curve cryptography because it's relatively lightweight when compared against most other public-key cryptography methods. Since the ambient condition near the verifier can be readily determined by a resourceful adversary, we use the prover's surface temperature instead. This is measured by an on-board temperature sensor on the prover and an appropriate sensor on the verifier. To reinforce the result based on temperature measurement, we also include a fast bit challenge–response part where round trip times are measured and validated. We believe that the simultaneous use of both temperature and round-trip travel time in our authentication protocol provides a relatively high degree of security. The proposed protocol is for mutual authentication — both the identity of the prover and verifier as well as the physical separation claimed by these parties are validated.

Throughout the paper, we interchangeably use NFC, RFID, and smartcard to represent the prover. We do this (a) to reinforce the fact that these devices are comparable from a relay-attack perspective and (b) since there's a strong overlap among the technologies and authentication protocols that are associated with these devices.

Based on the proposed mutual authentication protocol, the contributions of this paper are three-fold: (1) use of prover surface temperature for verifying claimed distance separation of prover and verifier in a mutual authentication protocol, (2) elliptic-curve based public key cryptography for mutual authentication to avoid the key distribution problem, and (3) multi-dimensional (based on both temperature and separation distance as measured by signal round-trip time) to reinforce results from each dimension to address relay attacks.

The remainder of this paper is organized as follows: We provide a brief discussion on relay attacks and their variants known as mafia attack and terrorist attack as well as their extensions in the next section. In Section 3, we provide an overview of published literature on the use of ambient conditions to address relay attacks. We present the proposed protocol in Section 4 and discuss its security properties in Section 5. We conclude the paper with a brief discussion in Section 6.

2. Relay attacks

Relay attacks operate by relaying signals between prover and verifier without any modification to these messages. By its very nature, these attacks necessarily involve a physical distance component. During the (one-way or mutual) authentication process between an actual prover and verifier, these entities (prover and verifier) are in close physical proximity to each other. On the other hand, when the rightful owner or bearer of the prover is unaware of its communication with a verifier, it's unlikely for this prover and verifier to be near each other. Researchers have used this observation to develop distance-bounding authentication protocols in which the physical separation of prover and verifier is determined through single-bit round-trip travel times between prover and verifier. The basis for distance-bounding protocols that address relay attacks is that no signal travels through space-time faster than light (e.g., [24]). Under this constraint, an adversary cannot increase the signal travel speed to claim a shorter physical separation from the verifier.

Relay attack comes in several flavors including the distance fraud, mafia (man-in-the-middle) fraud, and terrorist fraud attacks [13]. The mafia fraud attack needs two cooperating adversaries — a rogue prover $(\overline{T})$ and rogue verifier $(\overline{R})$. In this setup, the interactions between any pair of honest prover, honest verifier, rogue prover and rogue verifier occur as: $R–\overline{T}–\overline{R}–T$. Among the earliest of the distance bounding protocols, Brands and Chaum's [8] protocol includes a series of bit challenge–response exchanges. The round-trip times of these exchanges are then used to corroborate the claimed physical separation between prover and verifier. While the mafia fraud attack assumes honest prover and verifier, the terrorist fraud attack involves a dishonest prover and an honest verifier. The intention here is for the dishonest prover to convince the honest verifier that it is indeed present at a claimed location when it really is not. The dishonest prover accomplishes this by collaborating with an adversary. It should be stressed that this collaboration does not involve the prover sharing its secret (e.g., key) information with the adversary.

Over the years, researchers have developed protocols that are claimed to be immune to various forms of relay attacks. For example, Hancke and Kuhn [24] proposed a protocol that is secure against mafia fraud attack. This protocol has two phases (timed and un-timed). However, no attempt is made to ensure that the parties taking part in these phases are indeed the same. This exposes the protocol to terrorist fraud, where the dishonest prover can easily share necessary information to an adversary without revealing any secret. To address this vulnerability, Reid et al. [39] proposed a modified protocol with a strong link between the timed and un-timed phases. To discourage terrorist fraud attacks on this protocol, knowledge of necessary information for the timed (second) part of the protocol necessitates revelation of secrets.

Since the earlier protocols by Hancke and Kuhn [24] and Reid et al. [39], researchers have proposed several protocols that have attempted to improve on existing protocols in terms of their level of immunity against relay attacks. A majority of the protocols that were proposed