Journal of Network and Computer Applications 34 (2011) 877–887

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Design of a secure distance-bounding channel for RFID

G.P. Hancke *

ISG Smart Card Centre, Royal Holloway, University of London, Egham TW200EX, UK

ARTICLE INFO

Available online 4 May 2010

Keywords:
RFID
Contactless smart card
Distance bounding

ABSTRACT

Distance bounding is often proposed as a countermeasure to relay attacks and distance fraud in RFID proximity identification systems. Although several distance-bounding protocols have been proposed the security of these proposals are dependent on the underlying communication channel. Conventional communication channels have been shown to be inappropriate for implementing distance bounding, as these channels introduce latency that can be exploited to obscure attempted attacks. Distance-bounding channels for RFID tokens have been proposed but have failed to address distance fraud or have not been practically implemented in an RFID environment. This paper describes a near-field, bit-exchange channel design that minimizes latency and allows for more secure distance-bounding measurements, while still allowing for a resource-constrained prover. Results from a proof-of-concept implementation is also presented, which illustrates that a channel that is resistant to both relay attacks and distance fraud is feasible in current RFID systems.

1. Introduction

RFID technology is a prevalent method for implementing proximity-based services in systems that need to link a person or object to a specific location or operational context. These systems operate on the assumption that the token is in close proximity to the reader because of the physical limitations of the communication channel. Proximity, and the associated trust, is especially important in secure RFID systems implementing applications such as payment, identification and access control. For example, upon scanning a access card a door is unlocked or when presenting a contactless credit card the payment is authorized and goods handed to the customer present. However, using only the physical characteristic of the communication channel is not suitable for securely proving the proximity of a token. An attacker can use a proxy-token and proxy-reader to relay the communication between a legitimate reader and token over a greater distance than intended, or simply extend the range of his own device by modifying the communication channel parameters, e.g. amplify the response.

Distance-bounding protocols determine an upper bound for the physical distance between two communicating parties based on the round-trip-time of cryptographic challenge-response pairs. This distance can then be used as a cryptographic proof of proximity. Distance-bounding protocols are meant to detect any extra delay in the prover's expected response as an increase in the round-trip-time extends the distance bound. Distance-bounding protocols can therefore be an effective way to prevent relay attacks as the attacker introduces a delay, even if it is only the additional propagation time between the proxy devices. The attacker cannot decrease the round-trip-time by preemptively transmitting his response as he is forced to wait for the challenge, and as a result the probability of a successful distance fraud is reduced. Time-of-flight distance-bounding protocols must be integrated into the physical layer of the communication channel to accurately determine the distance between the prover and verifier. This means that the security of the distance bound depends not only on the cryptographic protocol itself but also on the practical implementation and the physical attributes of the communication channel. The communication channel used for the exchange must, therefore, not introduce any timing tolerances that the attacker can exploit to circumvent the physical distance bound. Communication channels used in HF RFID systems utilize error-correction and packet delimiters that introduce latency, and the physical transceiver architectures used have also been shown to be vulnerable to late-commit and clocking attacks, which allows the attacker to hide the extra time needed to relay data (Hancke and Kuhn, 2008; Clulow et al., 2006). The conventional channels currently used in RFID systems are therefore seen to be unsuitable for implementing secure distance bounding.

If distance-bounding is to be implemented in RFID systems then the ability of the underlying channel to generate an accurate and secure time measurement must considered. Any latency that could be exploited by an attacker would need to be identified and the resultant effect on security taken into account. The ideal situation would be to implement new distance-bounding channels that minimize latency and provide strong security properties, while still allowing for a resource-constrained RFID token. The

* Tel.: +44 1784 414423.
E-mail address: ghancke@ieee.org

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.04.014