UCI Beall
Applied Innovation
Research Translation Group

RFID Reader Revocation Checking Using Low Power Attached Displays

Tech ID: 20672 / UC Case 2010-102-0

CONTACT

Edward Hsieh
hsiehe5@uci.edu
tel: 949-824-8428.

INVENTORS

- Tsudik, Gene
- Uzun, Ersin

OTHER INFORMATION

CATEGORIZED AS

- **Communications**
  - Other
- **Computer**
  - Security
- **Security and Defense**
  - Cyber security

RELATED CASES

2010-102-0

BRIEF DESCRIPTION

A new RFID reader authentication protocol that allows efficient and timely check of revocation status of the reader’s certificate.

FULL DESCRIPTION

Revocation checking of RFID readers is a challenging problem due to the passive nature of RFID tags and cost sensitivity in RFID applications. The lack of constant power and online connection to a trusted server on RFID tags makes them vulnerable against readers with revoked privileges. Today, this problem becomes even more urgent with the use of RFID technology in privacy and security sensitive applications like RFID credit cards or e-passports.

The main challenge in solving the revoked reader problem in RFID systems is due to the fact that the RFID tags are passive devices without any self-sustaining power source. In other words, RFID tags are only alive when they are being read and they solely depend on the readers for their view of world (e.g., current time and date). However, this makes the revocation of readers challenging as the RFID tag relies on the reader itself to acquire the current date and be sure that, as of the day of reading, the presented certificate is not expired and it is not listed in the up-to-date revocation list. This opens the door for revoked reader attacks as an expired certificate and/or an old certificate revocation list (CRL) would not be noticed by any tag as long as the reader reports a time in history where both the certificate and the CRL was valid as the current time to the tag.

In this invention, a new way of authenticating RFID readers which allows efficient and timely check of revocation status in the process is proposed. The two differentiators of this invention compared to the existing techniques are two fold: (1) An efficient way of checking whether a given certificate is on a CRL or not, with constant communication overhead between a RFID tag and a reader. (2) a new protocol that allows the owner of an RFID tag to verify the current date reported to the tag by the reader is indeed correct. Achievement of the former advantage is made by way of using hash chains and cryptographic signatures and the latter advantage by attaching a low power, flexible and ultra-thin display to the RFID tag, which can easily be powered by the energy absorbed via a RFID antenna without a need for any secondary power source or change in current RFID specifications.

SUGGESTED USES

The invention can be used in many domains where RFID tags carrying private or valuable information. Immediate examples for such uses are RFID-equipped passports, and credit cards.

ADVANTAGES

Compared to traditional CRLs, which require communication overhead and storage, this invention has constant communication overhead between the tag and the reader. The invention solves the reader revocation problem that is left unsolved by the prior art. Compared to prior art, this invention provides solid and quantifiable security guarantees for a given time CRL issuance interval.

PATENT STATUS

Country	Type	Number	Dated	Case
United States Of America	Issued Patent	8,710,952	04/29/2014	2010-102

ADDITIONAL TECHNOLOGIES BY THESE INVENTORS

- Transaction Verification On Rfid-Enabled Payment And Transaction Instruments

UCI Beall
Applied Innovation

5270 California Avenue / Irvine,CA
92697-7700 / Tel: 949.824.2683