

Request Information

Permalink

Transaction Verification On Rfid-Enabled Payment And Transaction Instruments

Tech ID: 21364 / UC Case 2011-299-0

BRIEF DESCRIPTION

A new method that allows users to verify the transaction details (e.g., the amount being charged) and explicitly approve them on RFID enabled payment and transaction instruments.

FULL DESCRIPTION

RFID tags are commonly used as payment and transaction instruments (e.g., credit, debit, ATM and voting cards). In such settings, a malicious reader can easily mislead the tag into signing or authorizing a transaction different from the one that is communicated to, or intended by, the user. This is possible because there is no direct channel from a tag to its user (i.e., no secure user interface) on regular RFID tags and the only information a user gets (e.g., a receipt, or an amount displayed on the cash register) is under the control of a potentially malicious reader. Thus, it seems impossible for a user to verify (in real time) transaction details, e.g., the amount or the currency. This problem becomes especially important with current electronic credit cards.

UCI researchers have developed an approach to transaction amount verification that is designed to work with any RFID-enabled payment instrument. Its primary goal is to provide simple, secure and usable transaction verification at a Point-of-Sale (PoS).

The Protocol

Display enabled RFID tag (DERT) receives transaction details from the reader (seller/merchant). DERT verifies that the details (e.g., issuing bank, account number, etc.) match their counterparts in the reader PKC. Protocol is aborted in case of a mismatch.

DERT extracts and displays user-verifiable data, i.e, the amount and, optionally, the currency code. It then enters a countdown stage that lasts for a predetermined duration (e.g., 10 seconds).

User observes transaction information and, if the transaction amount and other details are deemed correct, presses accept button on DERT before the timer runs out. At this point, DERT signs the time-stamped transaction statement and sends it to the reader. This signed statement is then sent to the payment gateway and eventually to the financial institution that issued the payment DERT.

SUGGESTED USES

RFID enabled payment instruments

ADVANTAGES

This solution takes a proactive approach (instead of reacting to fraudulent transactions after they occur) and doesn't allow any transactions to go through without user's approval of its details (e.g, the amount for a credit card transaction). It is also important that users verify transaction details at the time of the transaction in our solution (not few days later).

CONTACT

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



INVENTORS

» Tsudik, Gene

OTHER INFORMATION

CATEGORIZED AS

- » **Communications**
- » Other
- » Wireless
- » **Computer**
- » Other
- » Security
- » Software

RELATED CASES

2011-299-0

PATENT STATUS

Country	Type	Number	Dated	Case
United States Of America	Issued Patent	9,443,240	09/13/2016	2011-299

RELATED TECHNOLOGIES

- ▶ [RFID Reader Revocation Checking Using Low Power Attached Displays](#)

ADDITIONAL TECHNOLOGIES BY THESE INVENTORS

- ▶ [RFID Reader Revocation Checking Using Low Power Attached Displays](#)

UCI Beall
Applied Innovation

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



© 2011 - 2016, The Regents of the University of
California
[Terms of use](#)
[Privacy Notice](#)