Security Analysis and Implementation of Relay-Resistant Contactless Payments

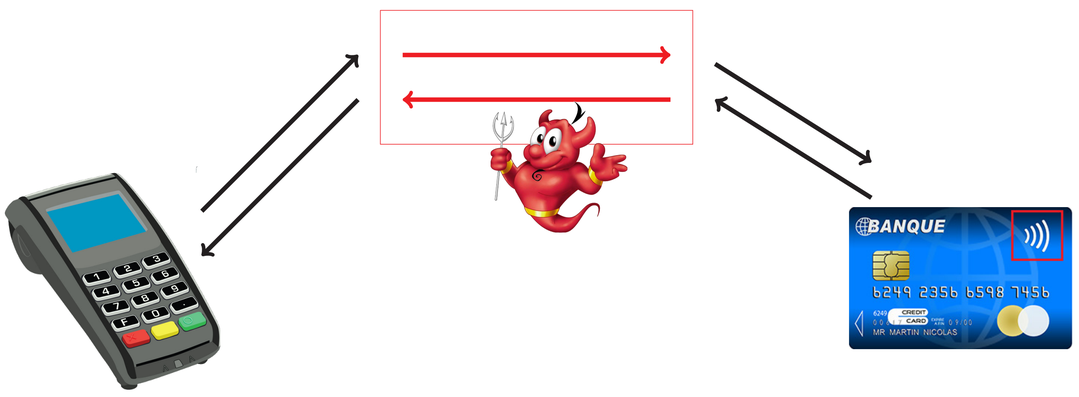
Ioana Boureanu[1], Tom Chothia[2], Alexandre Debant[3], and Stéphanie Delaune[3]

[1] University of Surrey, SCCS, UK
[2] University of Birmingham, UK
[3] Univ Rennes, CNRS, IRISA, France

Ensuring physical proximity becomes crucial when considering contactless payments. Specific protocols, namely distance bounding protocols, have been designed and recently formally analysed to achieve this goal. However, the latter has so far been conducted under the assumption that readers are honest; this is unrealistic for payment applications.

Contactless payment protocols

Entities = bank, reader, and card
Protocol = follows EMVCo's specification
Goal = ensure physical proximity of reader and card during transactions
Security concerns = subject to relay attacks...

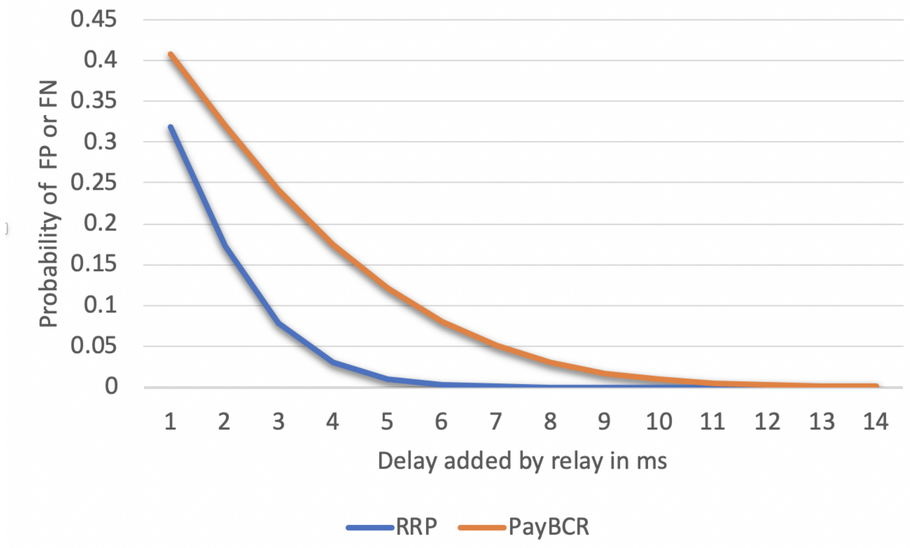


The PayBCR and PayCCR protocols

- two novel payment protocols which run close to the EMV standard
- rely on Trusted Platform Modules (TPM) onboard readers
- proximity check performed by the bank or the card

Practical contributions

- A collaboration with an EMV active company *Consult Hyperion*:
  - an implementation on the MasterCard PayPass-RRP protocol.
  - an implementation of the PayBCR protocol.
- A practical security analysis: both protocols actually stop relay attacks!



Symbolic verification in a nutshell

Messages are abstracted with terms (perfect cryptography assumption).
Protocols are described using a process algebra.
Intruder entirely controls the network: he is omniscient and omnipresent.

Tool support exists:

TAMARIN — Tamarin prover interactive mode

ProVerif

Main limitation: time is not faithfully modelled

Recent contribution for analysing distance-bounding protocols

- Few well-adapted frameworks:
  - Tamarin's approach: Mauw *et al.* - 2018
  - ProVerif's approach: Chothia *et al.* - 2018, and Debant *et al.* - 2018

Main restrictions:

- no agent mobility
- the time-check must be performed by the entity who initiates the challenge/response mechanism

Theoretical contributions

- A new symbolic model modelling time and agent mobility.
- A new security property dealing with malicious readers.
- A causality-based reduction to get rid of time and make possible the security analysis.
- First symbolic security proofs of protocols with remote proximity check.

Protocol	Role authentication	Time-bound authentication	Causality-based security
PayCCR*	✗	✓	✓
PayBCR	✓	✓	✓

* slightly modified

Authors




Alexandre.Debant@irisa.fr