Cryptology ePrint Archive: Report 2013/031

An Analysis of the EMV Channel Establishment Protocol

Christina Brzuska and Nigel P. Smart and Bogdan Warinschi and Gaven J. Watson

Abstract: With over 1.5~billion debit and credit cards in use worldwide, the EMV system (a.k.a. ``Chip-and-PIN") has become one of the most important deployed cryptographic protocol suites. Recently, the EMV consortium has decided to upgrade the existing RSA based system with a new system relying on Elliptic Curve Cryptography (ECC). One of the central components of the new system is a protocol that enables a card to establish a secure channel with a card reader. In this paper we provide a security analysis of the proposed protocol, we propose minor changes/clarifications to the ``Request for Comments" issued in Nov 2012, and demonstrate that the resulting protocol meets the intended security goals.

The structure of the protocol is one commonly encountered in practice: first run a key-exchange to establish a shared key (which performs authentication and key confirmation), only then use the channel to exchange application messages. Although common in practice, this structure takes the protocol out of the reach of most standard security models for key-exchange. Unfortunately, the only models that can cope with the above structure suffer from some drawbacks that make them unsuitable for our analysis. Our second contribution is to provide new security models for channel establishment protocols. Our models have a more inclusive syntax, are quite general, deal with a realistic notion of authentication (one-sided authentication as required by EMV), and do not suffer from the drawbacks that we identify in prior models.

Category / Keywords: applications /

Date: received 24 Jan 2013, last revised 19 Feb 2013

Contact author: nigel at cs bris ac uk

Available formats: PDF | BibTeX Citation

Version: 20130219:080543 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]