Bristol researchers work to secure next generation chip-card payment technology

November 5 2013

Current chip technology used for purchasing items via credit and debit cards in shops was developed in the mid-1990s. EMVCo, the standard body which manages, maintains and advances EMV Specifications, is in the process of designing the next generation payment technology to meet long-term industry requirements. The activity will establish a common, robust technology platform for supporting contact and contactless/mobile interfaces for both online and offline transactions.

Dr Gaven Watson from Bristol's Department of Computer Science will be presenting a paper at the prestigious Association of Computing Machinery's Conference on Computer and Communications Security (ACM-CCS) sharing the details of a study that validates the proposed protocol design to be used in future EMV chip cards.

This protocol was developed by EMVCo and then published on its website as a request for comments (RFC). University of Bristol researchers responded and proved mathematically that the protocol meets the security goals that it was designed to achieve.

The protocol sits at the heart of the new specification as it offers a key agreement system based on elliptic curve cryptography. Due to the constrained nature of payment cards, and some new requirements for protecting contactless transactions, the new protocol needed to be created.

Nigel Smart,Professor of Cryptology at the University of Bristol, said:

"This is an important step in validating the technology we will all start to use in the future. When the previous chip technology was designed people did not know how to mathematically prove that a protocol satisfied certain security goals. The science of cryptography has advanced and is now at a stage where this is possible and protocols that will be used in the real world can be fully analysed."

Christina Hulka, Chair of the EMVCo Board of Managers, added: "EMVCo welcomes the initiative of Professor Nigel Smart and his fellow researchers in developing a security proof of this key agreement protocol. EMVCo is of the view that the new cryptographic algorithms and protocols that will be used to secure billions of EMV payment transactions should not only offer optimum performance but also receive the best security analysis that modern cryptology can provide."

The paper represents joint work by the Bristol's Department of Computer Science and the Engineering Faculty of Tel-Aviv University.

More information: An analysis of the EMV Channel Establishment Protocol by Christina Brzuska and Nigel P. Smart and Bogdan Warinschi and Gaven J. Watson. eprint.iacr.org/2013/031
ACM Conference on Computer and Communications Security [ACM-CCS] 2013.

Provided by University of Bristol