Unleashing EMV Cards for Security Research

Tomáš Rosa, crypto.hyperlink.cz

EMV stands for payment cards standard developed jointly by renowned payment cards associations Europay, MasterCard, and VISA. It describes the common core which should be obeyed by any chip payment card regardless the particular association and-or the issuing bank behind it. Besides this standard – which provides several hundreds of pages of intensive technical reading by itself – there are thousands of pages of its particular proprietary extensions provided by the respective associations. These extensions are, contrary to the public EMV standard, held strictly confidential. They provide the specific details of the particular card processing in those parts, where EMV gives only a vague general description. Such a situation obviously discourages any attempt of public security research in this area. Perhaps, this is the main reason why there are just a few academic research papers on chip payment cards security worldwide.

The purpose of this talk is to encourage public academic research of payment cards security by showing that still a lot of things can be found by combining just the public EMV documents with certain feasible reverse engineering. We will show basic properties of the application protocol build over ISO 7816-3/4 and provide details on its practical invocation. This includes selecting the appropriate application, starting the payment transaction and processing its data. The main idea behind discovering the secrets of the protocol is this: When in doubt, use the CAP/DPA reader and listen to its communication with the particular card. It turns out, that these pocket smart devices, originally developed to allow card holder authentication for online banking services, are really valuable reverse engineering oracles. We will also note the most important parts where cryptographic operations are being used, together with showing the ways on how to approach practical experiments with them. This viewpoint is mainly inspired by side channel cryptanalysis.

Also touched will be the magnetic stripe of the card. Although the theme may seem a bit obsolete and unrelated, the aspects around possible cross-channel attacks deserve certain attention. We should emphasize that for properly configured cards and processing systems these attack are already defeated, but anyway – it is worth it knowing about them. Finally, we will also talk about the "2nd generation" contactless payment cards together with their relation to rising NFC interface for GSM phones.

Although the talk clearly cannot substitute those thousands of confidential pages, it can serve as a compass that will guide security researchers on their own ways to understanding and experimenting with this modern and challenging technology.

It shall be noted, however, that the talk by no means implies the payment cards are broken. This industry is really very broad and practically matured area of various technologies, techniques and administrative processes, all of them working tightly together. We cannot judge the whole system by only looking on a part of it. What we will do instead is just playing with that part, which is mostly interesting for us. The final judge is definitely to be left on risk analysts, who will, perhaps, also profit from the potential academic research promoted by this humble talk as well.