# Cryptographic API grammar

Zdeněk Kraus, xkraus00

October 19, 2011

### Abstract

As payment technology keeps improving constantly, we find ourselves using electronic cards and devices to manage our financial transactions more and more often. The currently most used worldwide payment method is EMV – Europay, MasterCard, and Visa. EMV is the global standard for IC (Integrated Circuit) cards.

EVM cards use secure cryptographic API. Cryptographic API is a set of functions that are used by entities to assure security of their interactions as intended by the designer. EVM cards provide the API on a chip as to prevent any attempt to compromise the cards. Typically, EMV card attacks focus on exploiting the hardware, such as altering account number stored on the magnetic stripe, or compromising the communication, e.g. the "Man-in-the-Middle" attack. Another type of attacks involves searching for vulnerabilities to misuse the cryptographic protocols. Because the API used for interaction with the chip is created by man, naturally, the interaction is not fully formally verified and the API and protocols may include other undiscovered vulnerabilities.

This problem can be solved by applying rules of formal languages. To achieve this, we can create a grammar, that corresponds to the API protocol. Then we are able to simulate API operation. By examining such grammar and its properties, we can acquire additional information about the protocol behaviour. That may discover ways to enhance security.