Emulator of Contactless Smart Cards in FPGA

Stanislav Jeřábek
Department of Digital Design
Faculty of Information Technology, Czech Technical University in Prague

jerabst1@fit.cvut.cz

Keywords. FPGA, Emulation, Contactless Smart Card, ISO/IEC 14443.

Abstract

This paper describes implementation of contactless smart card emulator compliant with ISO/IEC 14443 in FPGA. Systems using contactless smart cards are widely used and some of these systems are not secured properly. For example in many such systems UID (unique identifier) is used as the only one authentication mean. As the UID is not encrypted and is read from the card in plain, it is easy to make a copy of the smart card and use the clone as the original card. In this work we describe emulator of a smart card implemented in FPGA which is able to spoof some genuine smart card Emulator then can be used to spoof some other card successfully.

Emulator described in this work emulates protocol described in parts from 1 to 3 of ISO/IEC 14443 standard. So emulator is able to come through whole *card selection* process and so spoof the real smart card with given UID. This functionality was successfully tested on systems used at CTU in Prague, where the weak implementation of UID as the only one authentication mean is used. If the last part of the standard would be implemented, this device should be used as part of relay attack system. This is possible thanks to high efficient implementation in hardware and thus possibility to overcome proximity–check protection.

Acknowledgment

I thank to my master thesis supervisor Jiří Buček for everything related to the supervising.