ESP1836

Reverse Engineering the Communications Protocol of an RFID Public Transportation Card

Radio Frequency Identification (RFID) security has not been properly handled in numerous applications, such as in public transportation systems. In this paper, a methodology to reverse engineer and detect security flaws is put into practice. Specifically, the communications protocol of an ISO/IEC 14443-B public transportation card used by hundreds of thousands of people in Spain was analyzed. By applying the methodology with a hardware tool (Proxmark 3), it was possible to access private information (e.g. trips performed, buses taken, fares applied...),to capture tag-reader communications, and even emulate both tags and readers.