Security Analysis of Real-World Devices

Background

Research in the field of cryptology offered convenient algorithms and protocols to fulfill certain security goals. Even though there are no strict mathematical proofs for many algorithms, public scrutiny enables confidence in the schemes. In contrast, manufacturers of security-relevant devices sometimes tend to implement proprietary algorithms to create an “additional layer” of security or to save cost in terms of program size or performance. As shown multiple times, when the undisclosed mechanisms are reverse-engineered or leak to the public, the implemented schemes turned out to be insecure with respect to their claimed security features.

What can you do?

The goal of this thesis is to investigate the size of the gap between cryptographic research and what is implemented in real world. To this end, we have multiple widely deployed candidates available for a detailed analysis of the implemented proprietary security mechanisms. The first step here is to reverse-engineer the extracted program code running on the device. This enables an understanding of the used methods and the possibility to reason about the level of security. In the second step, you can exploit possible flaws by developing attacks or the required hardware to circumvent the claimed security.

The topic is well suited for students of ITS, ET/IT, and AI. To be able to understand the recovered program code, it is required that you are familiar with microcontrollers and at least one assembly programming language, e.g., AVR-asm. The underlying concepts can be quickly transferred to other devices and their corresponding instruction set. It is possible to find the most suitable target and to realize only a part of the whole project as a Studien- or Bachelorarbeit.

Contact

If this sounds interesting to you, please contact Falk Schellenberg (falk.schellenberg@rub.de).