Smart-card Security
Power analysis and Fault Injection Attacks

Daniel Cvrcek, Petr Svenda, Petr Hanacek, and others

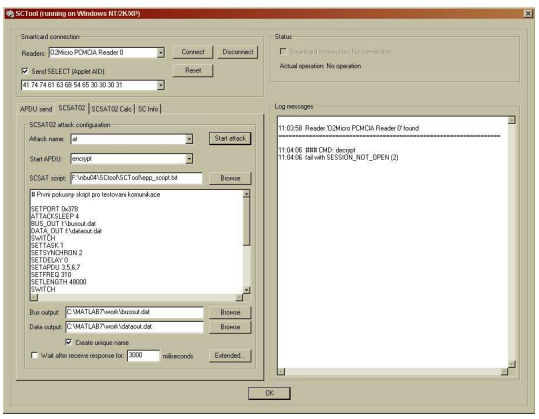
Dpt of Intelligent Systems
BUSLab

Smart-cards are used in number of applications. You can find a smart-card in your wallet as a credit/debit card, in your mobile phone as a SIM card, or you can be using it as an entry "key" to your workplace. Still, smart-cards must be considered as a low-cost device as a number of side-channel attacks is applicable on them.

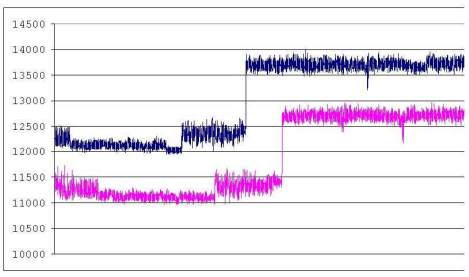
What is side-channel? Side-channel is a route one can obtain an information from e.g. a smart-cart. It is not used in usual operation with the device and if omitted during design, it can leak enough information for a complete compromise of the device security. We are talking about computational time, power consumption, electromagnetic emanation, when talking about smart-cards.

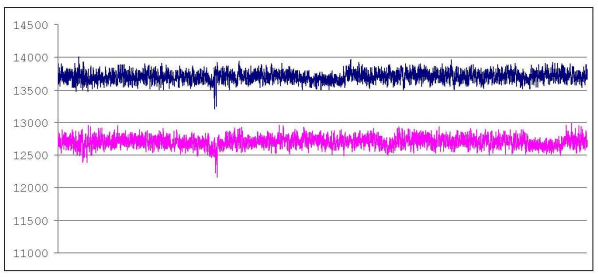
The research in the smart-card physical security targeted the vulnerability to timing attacks, leakage of information in the form of power consumption, and fault injection through changes of power supply. We have built a specialised measurement device (SCSAT02) that is able to sample power consumption with the frequency of 5 MHz. This maximum frequency is determined by DAM writing data into DSP processor memory. It is possible to use an external SDRAM memory but we have never finished an FPGA design of the driver.

Fault injection? If there are interfaces in the device, it is usually possible to use them for injection of unforseen inputs. These inputs might be of a form of a special data input (remember buffer overflow attacks) but they also may consist of changes in operational environment or physical properties of the data inserted into the device. Smart-cards are vulnerable to rapid changes in clock-signal or changes of the power-supply voltage (with duration in μs).



Although the amount of samples we are analysing does not reach the number of 100.000, it is not trivial to find a reasonable way of handling them. There is a special-purpose application able to communicate with the SCSAT device in an automated way – a number of measurement may be done in a single batch with operator intervention. The results saved as text files are processed in Matlab with functions we have written for the task. (Or maybe just OO Calc or MS Excel for rough results.)
Figures below depict initial phase before a DES encryption function is called. You can see an EEPROM writing (a pit in the left part of the left-hand figure) followed by a sharp increase in power consumption caused by starting a cryptographic coprocessor. The right hand figure shows DES encryption power consumption when the same key used on data with one bit flipped.





It all may seem to be just a game but these techniques may be used for discovering private keys used by smart-cards for signing e.g. your payment orders when using internet banking.
The project has not finished yet, and we have just built a new testing board that is much more universal and powerful. It has a 100 MHz system-on-chip processor with Linux OS, 300MHz PowerPC encompassed by FPGA, and 64MB of DDR SDRAM memory. Any analog input/output device can be deployed – A/D converters with laser diodes, sonar, high-speed light sensor, or even another processor.

The project is solved in cooperation with Faculty of Informatics, Masaryk University.