Research Seminar in Cryptography
Topics

Arnis Paršovs

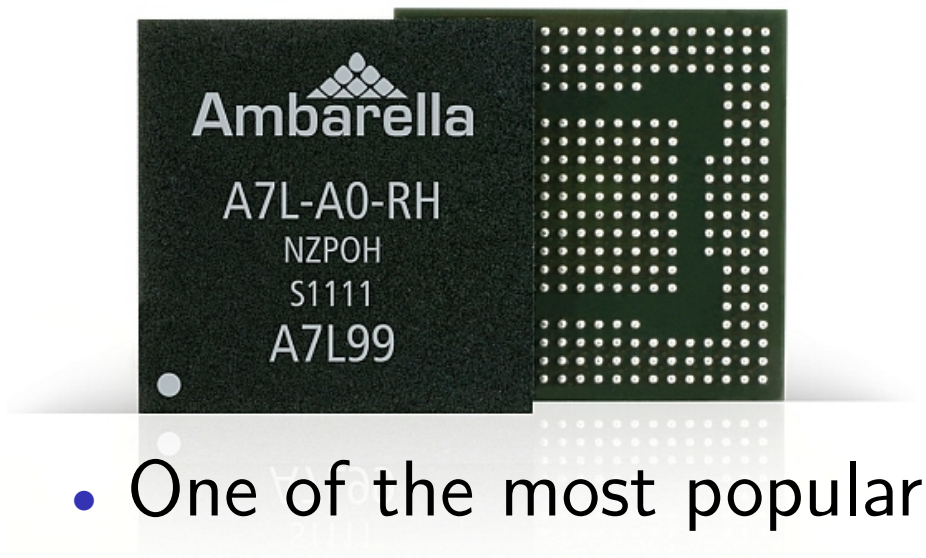
September 8, 2014

Encryption for Dashcams

- Privacy of the captured data ?!

Encryption for Dashcams

- No products providing encryption support
  - On-the-fly public-key encryption required
- No dashcam with open source firmware
  - Reverse engineering and patching required
- Target – Ambarella SoC firmware (ARM CPU)



  - One of the most popular dashcam processor
  - Used also in GoPro cameras

Encryption for Dashcams

Possible accomplishments:

- Research and document:
  - Firmware repackaging
    `http://chdk.setepontos.com/index.php?topic=5890.0`
  - Connection to debugging (UART/JTAG) port
    `http://dashcamtalk.com/forum/threads/mini0801-hacking-hardware-and-software.3157/`
  - Unbricking procedure
    `http://dashcamtalk.com/forum/threads/everything-you-need-to-recover-mini-0803.6302/`
- Patch firmware:
  - Find video stream saving breakpoint
  - Prepend dummy file header
  - XOR video stream with a fixed key
- 3 ECTS = 78 hours of workload

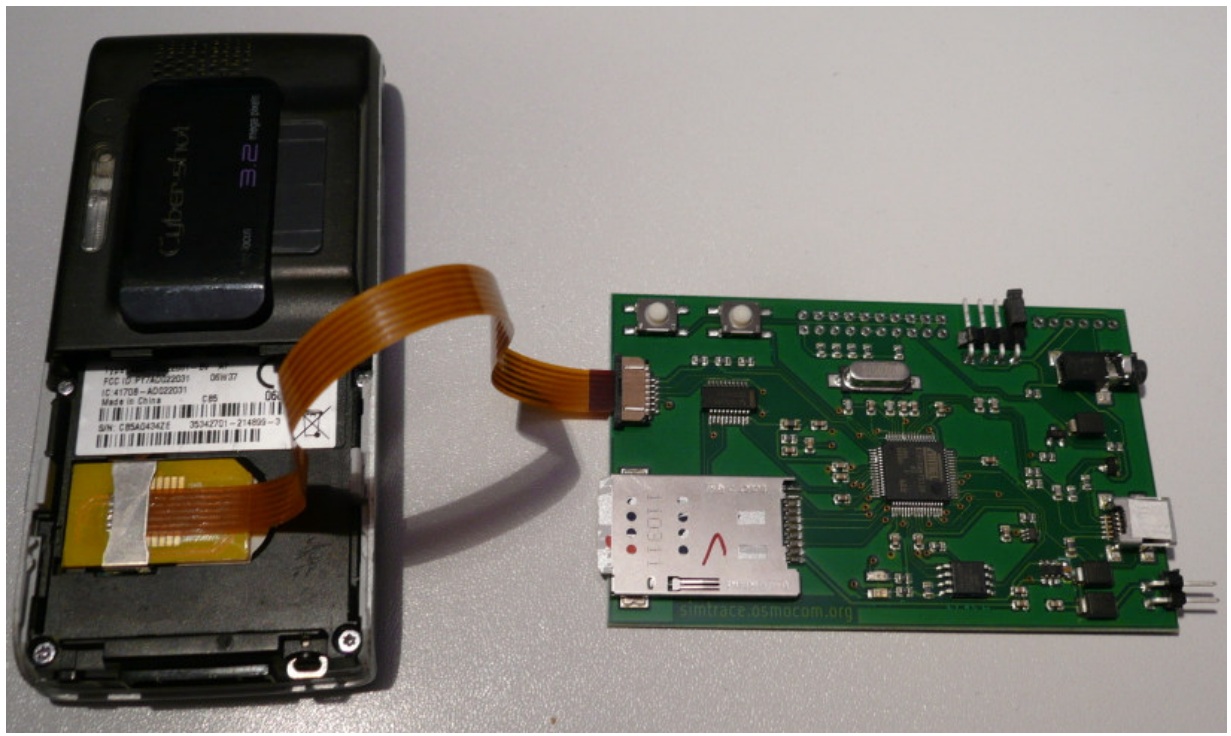
EMV (Chip & PIN) Protocol

Card for authenticating transactions in point of sale (POS) terminals and automated teller machines (ATMs).

EMV (Chip & PIN) Protocol

Questions to be answered:

- How EMV protocol works?
- What is stored in EMV card?
- Cross-check with a credit card you have:



`http://simtrace.osmocom.org`

Contacts

arnis@ut.ee