Oslobodimo hardware

reverse engineering protokola

Dobrica Pavlinušić
http://www.rot13.org/~dpavlin/
HULK, Knjižnica Filozofskog fakulteta u Zagrebu

DORS/CLUC 2009, 07.05.2009.

Reverse engineering?

- MDAP mrežni protokol
  - Update ADSL firmwarea

- AMV format zapisa
  - kineski MP4 video player

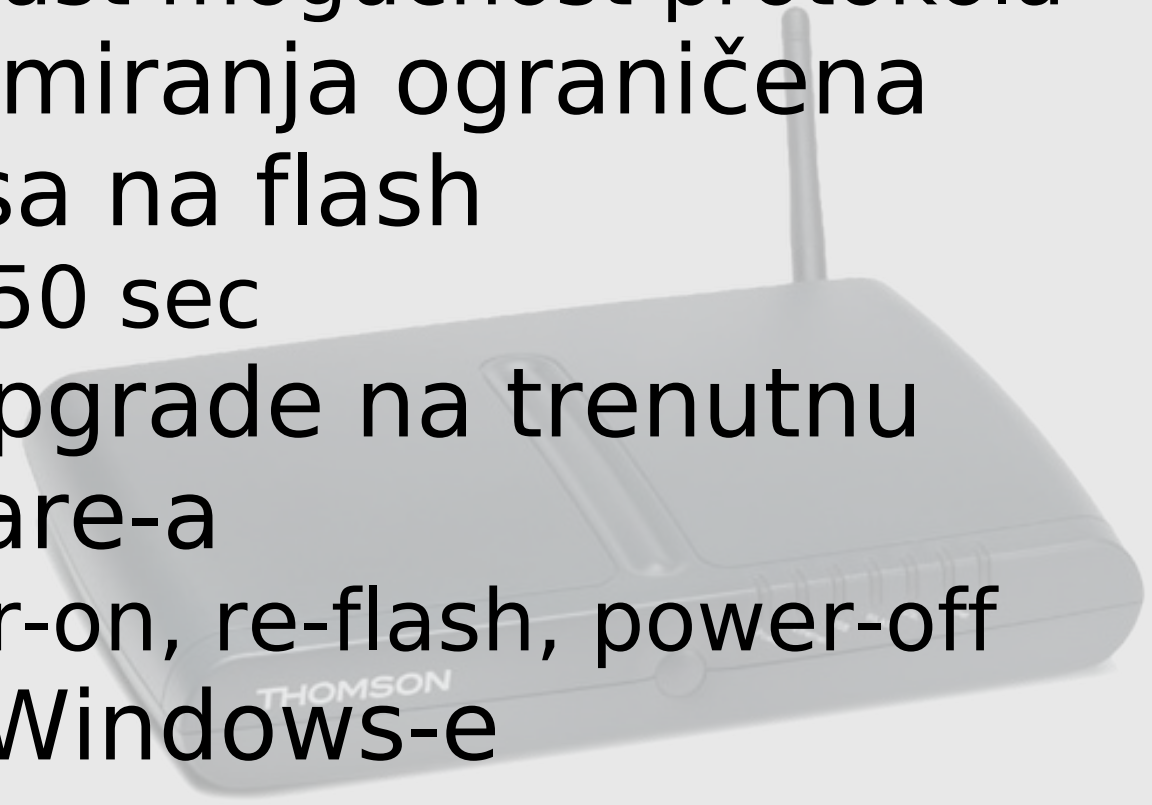
- 3M RFID protokol
  - USB serial

MDAP mrežni protokol

- Wireshark za snimanje prometa
  - Windows aplikacija u Qt-u
- Multicast za sve CPE-ove u segmentu
  - Malo sreće za checksum
- bootp
- tftp

Zašto vlastiti MDAP?

- Programiranje više uređaja istovremeno
  - Koristi multicast mogućnost protokola
- Brzina programiranja ograničena brzinom zapisa na flash
  - ~3 min -> ~50 sec
- Automatski upgrade na trenutnu verziju firmware-a
  - plugin, power-on, re-flash, power-off
- Ne zahtijeva Windows-e

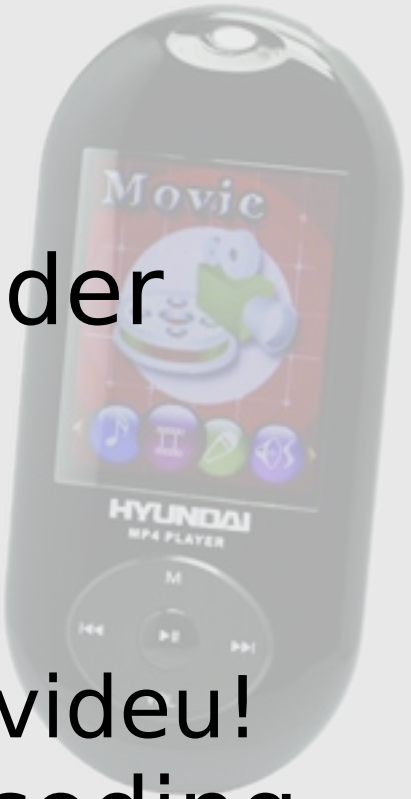


AMV video format

- S1MP3 arhitektura
  - Z80 + DSP on chip
- Audio
  - DSP: mp3, Z80: sučelje
- Video
  - DSP: mjpeg, Z80: adpcm
  - audio nije mp3!
- Windows Media Player
  - preskače frameove (load!)
  - video rezise bez interpolacije

Slobodan AMV!

- Video dekoder u perl-u
  - razumijevanje formata
  - otkrio da je audio ADPCM
- Zajednica razvila video encoder
  - samo dva mjeseca kasnije!
  - kao proširenje ffmpeg-a :-)
- Mnogo bolji resize (ffmpeg)
  - čitljivi titlovi na enkodiranom videu!
- Ne zahtijeva Windows za encoding
  - jpeq Q vrijednosti nisu savršene



3M RFID protokol

- 3M software za korisnike
  - Visual Basic iz 90-tih
  - Ne prikazuje SID-ove RFID čipova
  - Prikazuje 5 čipova istovremeno
  - Automatski copy/paste u drugu Windows aplikaciju
- USB serial protokol sa RFID čitačem

3M RFID protokol

- Portmon za pregled USB prometa
  - Windowsi pod KVM-om
- Otkriti sve mogućnosti
  - čitanje 25 čipova istovremeno
  - koliko podataka stane na RFID čip
  - kako funkcionira security
- Protokol ima CCITT checksum
  - StackOverflow korisnik **selwyn** rješio moj problem!

http://www.youtube.com/watch?v=ptWv4fFJ6Q8

Zvuči kompliciran o!

- Da li je reverse engeenering za mene?
  - Uređaj nije podržan pod Linux-om?
  - Da li bi mogao raditi bolje?
  - Želiš li pomoći ostalim korisnicima?
- Ako je jedan od odgovora **DA**
  - naučiti ćeš više o uređaju nego što si ikada želio znati!

Oslobodite i vi dio hardware-a!

Više informacija

- MDAP
  - http://blog.rot13.org/2007/11/cwmp_and_mdap_servers.html
  - http://svn.rot13.org/index.cgi/mdap
- AMV
  - http://www.s1mp3.org/en/
  - http://blog.rot13.org/2007/08/amv_free_decoder_works.html
  - http://svn.rot13.org/index.cgi/amv
  - http://blog.rot13.org/2007/10/amv_support_for_ffmpeg.html
  - http://code.google.com/p/amv-codec-tools/
- RFID
  - http://svn.rot13.org/index.cgi/RFID/
  - http://stackoverflow.com/questions/149617/how-could-i-guess
  - http://saturn.ffzg.hr/rot13/index.cgi?hitchhikers_guide_to_rfid
  - http://blog.rot13.org/2009/04/comet_experiment_rfid_reader_

Pitanja?
42