July 31, 2009

What The Hell Is Inside There?

Black Hat – Las Vegas

Christopher Tarnovsky
Flylogic Engineering, LLC.
chris@flylogic.net – http://www.flylogic.net

Black Hat Briefings

at&t
cingular
64K smartchip
SIM CARD
Nextel 600 Contcs & 25 Grps
Check nextel.com/sim for compatibility
PACIFIC BELL

Before

- Infineon SLE44 (8k), SLE66S (16/32k)
- Motorola 68HC05SC28 (12kb)
- ST ST16SF48 (8k), ST16SF4F (16k)

Note: There have been other unknown devices used around the world. These are just a few I have commonly found inside.

Were they secure?

- Short answer- NO!
- Easily probed
- Easily glitched

Now

- Infineon SLE66P/PE
- Infineon SLE88
- ST ST19NA18
- Philips (NXP) P5CC Series

Note: There are other unknown devices in use around the world. These are devices I have found to be in use currently.

Are they secure?

- Most are quite secure
  - Require FIB edits to prepare for probing
  - Feature size is below 250 nm.
  - Run at 1.8 - 2.5 volt core
  - Run as fast as 33 MHz
- Some are NOT!

In Conclusion

- Several manufacturers smartcard devices have been used
  - Companies using the devices have no idea about hardware security.
- Some of the devices are secure
- Some are considerably weak
- Latest Comp128 algorithm has been placed inside weak devices