February 2, 2010

Deconstructing a 'Secure' Processor

Black Hat – Washington D.C.

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

Black Hat Briefings

- Decapsulate
- Perform initial examination
- Identify device if possible
- Image layers
- Identify and understand challenges

- Remove silicon substrate from samples (decapsulate)
- Device analysis via microscopy to determine:
  - Is there a mesh present? If so, time will be spent to understand how to overcome challenge.
  - Understand bond pad layout .
  - Nomenclature on part to help identify better from public documentation.
  - Databus routing from memories.

- Prepare:
  - Small physical geometry on current architectures (<220nm, 4+ metals)
  - Lower internal operating voltage
  - Fast internal operating frequency
  - Runs asynchronous to outside world clock frequency
  - Only synchronization will be outside world reset signal
  - Memories will be encrypted. Will need to locate the central core of the CPU.
  - Find access to a Focused Ion-Beam workstation.

- Execute:
  - Mesh present over device?
    - Determine how to bypass
    - Most likely requires FIB edits
  - Find the ‘clear’ databus
  - Place probing needles down on the bus and examine running code
  - Determine CPU architecture from running code if not already known.
    - Today's CPU architectures are commonly found to be 6805 (ST), 8051 (Infineon, NXP) or AVR (Atmel) instruction sets.
  - Examine running logs from databus
    - Most developers trust these devices to execute code as was written
  - Glitch device momentarily to abuse CPU to spill code/data bytes
    - Capture code/data bytes via IO line or needles on bus

Mission accomplished, next chip!