[edit] Presentation Abstracts – Tuesday, 15 March

[edit] (S//NF) Differential Power Analysis on the Apple A4 Processor

(U) Presenters: [redacted], and [redacted] (U) The Apple A4 processor contains an on-board, AES cryptographic key called the Global ID (GID) that is believed to be shared across all current “iDevices”. This GID key is used to un-wrap the keys that decrypt the corresponding boot firmware code stored in system non-volatile memory. Currently, the only way to examine unencrypted boot code is to gain execution through an exploitable software security flaw. However, Apple is quick to address these flaws with each new release of firmware and hardware.

(S//NF) The Intelligence Community (IC) is highly dependent on a very small number of security flaws, many of which are public, which Apple eventually patches. The following presentation will discuss a method to noninvasively extract the GID key from the A4 silicon. If successful, it would enable decryption and analysis of the boot firmware for vulnerabilities, and development of associated exploits across the entire A4-based product-line, which includes the iPhone® 4, the iPod touch® and the iPad®.

(S//NF) Power analysis techniques have proven effective in extracting hardware resident cryptographic information, such as cryptographic keys, from secure processors noninvasively through side-channel methods. We have worked to develop an environment within the iPhone 4 that assists analysts in performing differential power analysis (DPA) attacks against the A4 processor while preserving the functionality of the device. We have studied electromagnetic (EM) emissions that occur during AES operations with the intent of extracting information about the on-chip AES keys. We will discuss the methods used to acquire various measurements from the system and the progress we’ve made in attempting to extract the GID key from the devices.