[edit] (S//NF) Secure key extraction by physical de-processing of Apple's 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 is highly dependent on a very small number of security flaws, many of which are public, which Apple eventually patches. This presentation will discuss a method to physically extract the GID key. 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) Apple relies on commercial and proprietary relationships with major integrated circuit (IC) manufacturers to supply the internal hardware for their leading-edge consumer products. Therefore, design and manufacturing information about the A4 is closely held intellectual property (IP). Some reverse-engineering reports have concluded that the A4 is manufactured by Samsung Ltd. for exclusive use in Apple products. Their data is compelling. They have shown that the Samsung Cortex A8 µProcessor core layout is used in the A4. If that is true, then it is possible that other Samsung IP, such as its non-volatile memory technology, may be used in this chip. Programmable non-volatile memory (NVM) offers the most design flexibility, reliability and security to store proprietary critical product information, such as the GID key.

(S//NF) Although, Samsung is a major supplier of flash memory chips it also holds IP in the area of CMOS-compatible, eFuse technology. The eFuse memory is thought to offer more immunity to random data upset, and a higher level of anti-tamper resistance. Therefore, this type of memory would be ideal as a secure repository of critical product information on the A4. We will use comparative examples of known Samsung product, versus the A4, in order to determine the type and location of NVM. In addition, we will discuss the progress made to date to determine where the GID key is located on the A4 IC, and how it can be recovered by physical de-processing of the chip.