iPhone 5c NAND mirroring attack

Sergei Skorobogatov, Markus Kuhn

UNIVERSITY OF CAMBRIDGE
Department of Computer Science and Technology, Security Group

Introduction

Apple iPhone devices are usually protected by a user passcode. Its security is designed in a way that prevents easy brute forcing. Inside the phone's CPU the passcode is combined with a secret and unique UID number, using a proprietary KDF algorithm to derive the system keys (Fig. 1). The number of attempts is usually limited to ten, with an increasing delay introduced after five unsuccessful guesses (Fig. 2).

The Apple iPhone 5c came under the spotlight soon after the FBI recovered one from a terrorist suspect in December 2015. In February 2016, the FBI announced that they were unable to unlock the recovered phone due to its advanced security features, including encryption of user data. Neither had they succeeded to persuade Apple to compile a modified version of iOS with unlimited passcode attempts. Later the FBI director dismissed the possibility of using NAND mirroring to help with getting the correct passcode.

"Mirroring" here refers to the process of copying the data into another storage device to create an exact copy of the original data. These copies can then be used multiple times to revert the system into that previous state. The iPhone 5c stores all non-volatile information inside a NAND flash memory chip located on its main board.

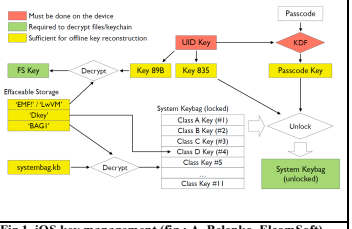

Fig.1. iOS key management (fig.: A. Belenko, ElcomSoft)

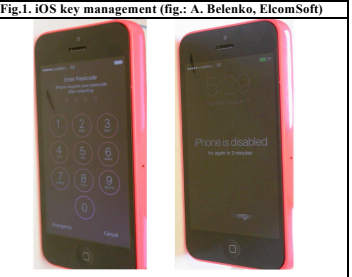

Fig.2. Passcode security of iPhone 5c

Experimental results

This work was carried out to investigate whether NAND mirroring is possible on the iPhone 5c. For that we ordered samples of used phones from Ebay and carefully disassembled them to gain access to the main board. Then we desoldered the metal shields above the CPU and the NAND with a hot-air gun, allowing us access to the components (Fig. 3). The NAND flash chip was not only soldered to the PCB but also glued to it with epoxy. This complicated the removal process by requiring insertion of a thin razor between the chip and the PCB during hot-air desoldering. Then the NAND chip was wired back to the board to make sure that the phone is still functional. Some cutting in the shielding and the case were made to allow the wiring out (Fig. 4). After that, an intermediate board was built to assist with eavesdropping on the NAND communication (Fig. 5). Once the proprietary NAND access protocol was understood it became possible to Read, Erase and Write the data. In order to speed up the process, a special microcontroller based test board was built (Fig.6). That way the whole 8 GB memory storage was copied in less than an hour using a simple software written in C (Fig. 7). However, cloning the NAND into another similar chip was complicated by the shadow areas implemented inside the NAND. Once the protocol for accessing those areas was found with the help of an oscilloscope (Fig. 8), it became possible to create exact copies of the original NAND chip. The protocol was using command packets at 500 MB/s hidden within slower 20 MB/s communication.

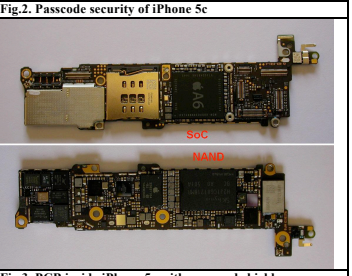

Fig.3. PCB inside iPhone 5c with removed shields

In order to restore the NAND to the original state with ten passcode attempts, it was necessary to only restore a few hundred 16 kB blocks. This takes less than a minute. After that the NAND needs to be inserted into the powered-down phone before switching it on. Then the next set of passcodes can be entered before the delay is introduced after 5 incorrect attempts. Then the process had to be repeated again. This successfully proved that NAND mirroring works for iPhone 5c. For a 4-digit passcode the recovery process would take about 20 hours, assuming several NAND chips being programmed in parallel. However, for a 6-digit passcode the process would take about 3 months.

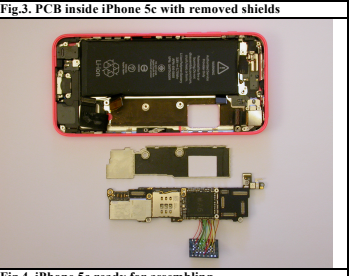

Fig.4. iPhone 5c ready for assembling

We also looked at the iPhone 7. A sample phone was carefully disassembled and the NAND chip was desoldered and then wired to a connector (Fig. 9). However, initial signal analysis revealed that, instead of parallel communication, a more sophisticated serial interface was used, similar to PCIe. Any experiments with eavesdropping and emulation would require special hardware to be used or built.

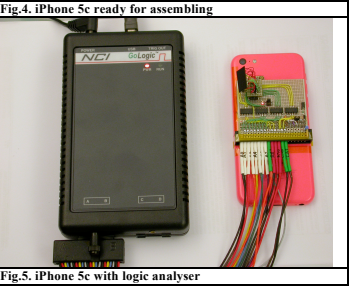

Fig.5. iPhone 5c with logic analyser

Future work

Although the above experiments worked well and proved the possibility of using NAND mirroring to recover the user passcode, it is not practical to manually swap programmed NAND chips. Ideally a hardware emulator of the NAND chip should be used. Also, instead of manually entering the passcodes, the process of brute forcing them could be automated, by plugging a keyboard emulator into the Lightning connector. This would reduce passcode recovery times to about 10 hours for 4 digits and to less than 2 months for 6 digits.

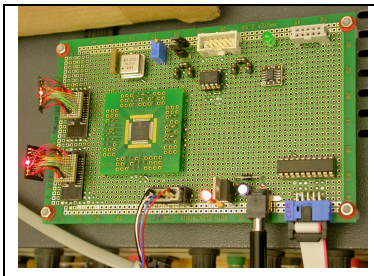

Fig.6. Special test board for copying NAND chips

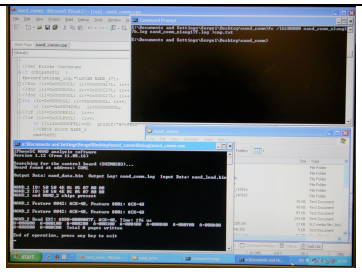

Fig.7. Software used for NAND mirroring

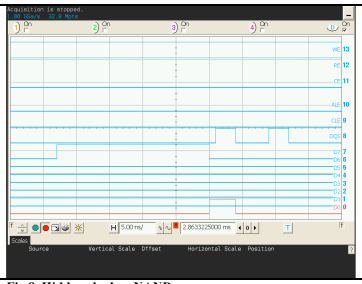

Fig.8. Hidden shadow NAND access

Fig.9. iPhone 7 with NAND wired to connector