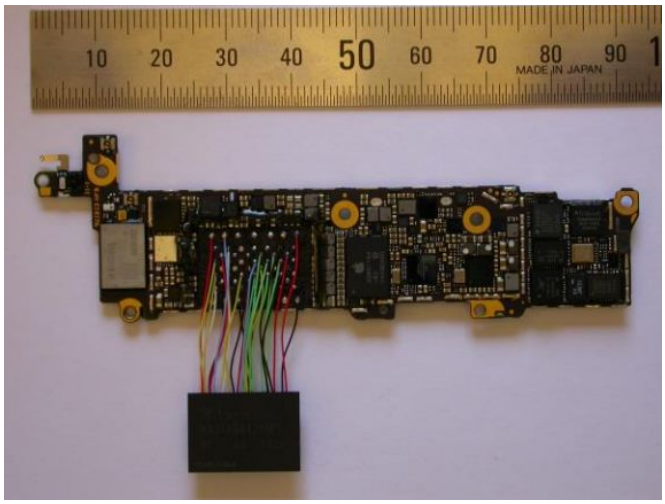
Computer scientist shows how to crack Apple iPhone 5c passcode for less than $100

20 September 2016, by Bob Yirka



iPhone 5c with wired up NAND. Credit: arXiv:1609.04327 [cs.CR]

(Tech Xplore)—University of Cambridge computer scientist Sergei Skorobogatov has figured out a way to gain access to an Apple iPhone 5c without having its password. He has written a paper outlining the technique, which he uploaded to the *arXiv* preprint server and has posted a video demonstrating how it works on YouTube.

Earlier this year, it was widely reported that the FBI paid an unknown company $1 million to crack the password of an iPhone used by terrorists known as the San Bernardino shooters. Now it appears they could have saved a lot of money if they had contacted Skorobogatov instead—he has found a way to crack the password of an iPhone using off-the-shelf parts that cost under $100.

The technique was simple: Skorobogatov simply mirrored the iPhone's Nand chip and then reprogrammed it to allow for resetting the counter that keeps tabs on how many times someone attempts to enter a password—the iPhone only allows six tries and if the user persists to 10 tries, the phone erases device data—this allowed him to manually try every possible combination of a four number password until he hit upon the one that was correct—a process he says that would take 40 hours on average.

In practice, the technique was a little more complicated than it sounded—Skorobogatov had to use a solder gun to heat the glue holding the chip in place to remove it without causing damage. He also had to reverse-engineer the communications system to learn how to get the mirrored chip to talk to the iPhone. After that, it was simply a matter of typing in a password up to five times—then refreshing the Nand chip—over and over again, until he found the right code. Skorobogatov acknowledges that his technique was rudimentary—someone employing more resources could likely have automated parts of the process, such as refreshing the counter and typing in passwords, greatly reducing the time it would take to come up with the correct password.

Skorobogatov suggests the same technique would likely work on other iPhones, though it would take longer to run in cases where the password has more digits.

More information: The bumpy road towards iPhone 5c NAND mirroring, arXiv:1609.04327 [cs.CR] arxiv.org/abs/1609.04327

Abstract
This paper is a short summary of a real world mirroring attack on the Apple iPhone 5c passcode retry counter under iOS 9. This was achieved by desoldering the NAND Flash chip of a sample phone in order to physically access its connection to the SoC and partially reverse engineering its

proprietary bus protocol. The process does not require any expensive and sophisticated equipment. All needed parts are low cost and were obtained from local electronics distributors. By using the described and successful hardware mirroring process it was possible to bypass the limit on passcode retry attempts. This is the first public demonstration of the working prototype and the real hardware mirroring process for iPhone 5c. Although the process can be improved, it is still a successful proof-of-concept project. Knowledge of the possibility of mirroring will definitely help in designing systems with better protection. Also some reliability issues related to the NAND memory allocation in iPhone 5c are revealed. Some future research directions are outlined in this paper and several possible countermeasures are suggested. We show that claims that iPhone 5c NAND mirroring was infeasible were ill-advised.

APA citation: Computer scientist shows how to crack Apple iPhone 5c passcode for less than $100 (2016, September 20) retrieved 23 February 2019 from https://techxplore.com/news/2016-09-scientist-apple-iphone-5c-passcode.html