Apple phones are AES-tough, says forensics expert

August 14 2012, by Nancy Owano

(Phys.org) -- Monday's *Technology Review* carries a glowing tribute to Apple iPhone security according to its author, Simson Garfinkel, a contributing editor who works in computer forensics and is highly regarded as a leader in digital forensics. He says Apple has passed a threshold "Today the Apple iPhone 4S and iPad 3 are trustworthy mobile computing systems that can be used for mobile payments, e-commerce, and the delivery of high-quality paid programming," thanks to Apple's heavy investment in iPhone security. That is where "threshold" comes in.

Apple has crossed it. Even law enforcement cannot perform forensic examinations of Apple devices seized from criminals, he said.

iPhone has a security architecture that is so sturdy and so tightly woven into its hardware and software that it is easy for consumers to use encryption on their phones and difficult for someone else to steal the encrypted information, he stated.

The key to Apple's security architecture strengths is the Advanced Encryption Standard algorithm (AES), a data-scrambling system adopted as a U.S.government standard in 2001. After over ten years of exhaustive analysis, he said, AES is still widely regarded as unbreakable.

(In August last year, AES was cracked, by a team of researchers from Microsoft, Research, KU Leuven and ENS Paris. It was a theoretical, or "academic" crack, with no practical implications. Despite being four times easier than other methods, the number of steps required to crack AES-128 was an 8 followed by 37 zeroes, said one of the team members."To put this into perspective: on a trillion machines, that each could test a billion keys per second, it would take more than two billion years to recover an AES-128 key," the Leuven University researcher added. Still, their attack unsettled some assumptions about AES.)

Nonetheless, the algorithm is so strong that no computer imaginable for the foreseeable future, even a quantum computer, said Garfinekel, would be able to crack a truly random 256-bit AES key. The National Security Agency has approved AES-256 for storing top-secret data.

A white paper from Apple dated earlier this year about its security features explained that the device's unique ID (UID) and a device group ID (GID) are AES 256-bit keys fused into the application processor during manufacturing. "Burning these keys into the silicon prevents them from being tampered with or bypassed, and guarantees that they can be

accessed only by the AES engine."

Apple is no doubt fortunate that this security threshold information is circulating, as Garfinkel is a solid authority on the subject of security.

The timing is excellent for Apple branding, considering the exposure another report had recently, where a Wired journalist's digital life was changed in one day which involved Apple and Amazon. The hackers didn't use any sophisticated algorithms or brute-force attacks to gain access to Mat Honan's online information. They simply called Apple, pretending to be the victim and convinced the Apple specialist to reset the AppleID password. Apple subsequently said it would review its-over-the-phone verification system to prevent such incidents from happening again.

More information: images.apple.com/ipad/business … S_Security_May12.pdf
www.technologyreview.com/news/ … -security-threshold/

Citation: Apple phones are AES-tough, says forensics expert (2012, August 14) retrieved 3 February 2023 from https://phys.org/news/2012-08-apple-aes-tough-forensics-expert.html