30C3: SD card tricks can deliver MITM attacks

1 January 2014, by Nancy Owano

Credit: bunniestudios

(Phys.org) —This year's 30th Chaos Communication Congress (30C3) in Hamburg from December 27 to December 30 carried numerous informative presentations, including a reverse-engineering story about SD cards, which two investigators explored for malware potential. The presenters were identified as "bunnie" and "xobs," taking center-stage to discuss their work. The presentation was titled " The Exploration and Exploitation of an SD Memory Card." (SD cards are the small flash-memory cards used to store data on phones, digital cameras and other portable devices.) As *Gizmodo* put it, "the next time you plug in an SD card, just remember that it's actually a tiny computer of its own." In short, some cards' embedded microcontrollers can be exploited. The two found that some SD cards contain vulnerabilities that allow arbitrary code execution—on the memory card itself. They talked about reverse-engineering and loading code into the microcontroller within a SD memory card.

"All "managed FLASH" devices, such as SD, microSD, and SSD, contain an embedded controller to assist with the complex tasks necessary to create an abstraction of reliable, contiguous storage out of FLASH silicon that is fundamentally unreliable and unpredictably fragmented. This controller is an attack surface of interest."

In bunnie's blog he wrote more on the topic, and said, "From the security perspective, our findings indicate that even though memory cards look inert, they run a body of code that can be modified to perform a class of MITM attacks that could be difficult to detect; there is no standard protocol or method to inspect and attest to the contents of the code running on the memory card's microcontroller." (The "MITM" refers to the man in the middle attack, where, they said, the card may seem to be behaving one way, but in fact does something else.) "Those in high-risk, high-sensitivity situations should assume that a "secure-erase" of a card is insufficient to guarantee the complete erasure of sensitive data. Therefore, it's recommended to dispose of memory cards through total physical destruction (e.g., grind it up with a mortar and pestle)."

At the same time, they said, understanding the inner workings of the controller enables opportunities for data recovery in cards that are thought to have been erased, or have been partially damaged. "Bunnie" is Andrew "bunnie" Huang. He has a Ph.D in electrical engineering from MIT and authored the book, *Hacking the Xbox: An Introduction to Reverse Engineering*. Xobs is Sean Cross.

The Chaos Communication Congress is described as an annual meeting of the "international hacker scene," organized by the Chaos Computer Club, where computer experts gather for lectures and workshops.

More information:
www.bunniestudios.com/blog/?p=3554

APA citation: 30C3: SD card tricks can deliver MITM attacks (2014, January 1) retrieved 28 January 2022 from https://techxplore.com/news/2014-01-30c3-sd-card-mitm.html