1000 - Breaking Bitcoin Hardware Wallets

Sunday at 10:00 in Track 3
20 minutes | Demo, Exploit
Josh Datko*Principal Engineer, Cryptotronix LLC*

Chris Quartier*Embedded Engineer, Cryptotronix, LLC*

The security of your bitcoins rests entirely in the security of your private key. Bitcoin hardware wallets help protect against software-based attacks to recover or misuse your key. However, hardware attacks on these wallets are not as well studied. In 2015, Jochen Hoenicke was able to extract the private key from a TREZOR using a simple power analysis technique. While that vulnerability was patched, he suggested the Microcontroller on the TREZOR, which is also the same on the KeepKey, may be vulnerable to additional side channel attacks.

In this presentation we will quickly overview fault injection techniques, timing, and power analysis methods using the Open Source Hardware tool, the ChipWhisperer. We then show how to apply these techniques to the STM32F205 which is the MCU on the Trezor and KeepKey. Lastly, we will present our findings of a timing attack vulnerability and conclude with software and hardware recommendations to improve bitcoin hardware wallets. We will show and share our tools and methods to help you get started in breaking your own wallet!
Josh Datko
Josh Datko is the owner of Cryptotronix, an embedded security consultancy. As a submarine officer, he was sent to Afghanistan to ensure that the Tailiban did not develop a submarine force—mission accomplished! He wrote a book on BeagleBones and crypto hardware which not many people have read, talked about embedded security at Portland BSides and HOPE, and presented a better way to make a hardware implant at DEF CON 22 which hopefully helped the NSA improve their spying.
Chris Quartier
Chris is the lead embedded hacker at Cryptotronix. He has worked at both big companies and IoT startups as an embedded developer working on bare metal and embedded linux board bring up, driver development, and trying to get those little logic analyzer clips to stay connected to a target. He's hacked on radios, rail guns, and fitness trackers but not all at the same time.

#defcon25/by_track/track3/sunday #defcon25/By_Day/_Sunday