1100 - Secure Tokin' and Doobiekeys: How to roll your own counterfeit hardware security devices

Saturday at 11:00 in Track 2
45 minutes | Demo, Tool
Joe FitzPatrick*SecuringHardware.com*

Michael Leibowitz*Senior Trouble Maker*

Let's face it, software security is still in pretty bad shape. We could tell ourselves that everything is fine, but in our hearts, we know the world is on fire. Even as hackers, it's incredibly hard to know whether your computer, phone, or secure messaging app is pwned. Of course, there's a Solution(tm) - hardware security devices.

We carry authentication tokens not only to secure our banking and corporate VPN connections, but also to access everything from cloud services to social networking. While we've isolated these 'trusted' hardware components from our potentially pwnd systems so that they might be more reliable, we will present scenarios against two popular hardware tokens where their trust can be easily undermined. After building our modified and counterfeit devices, we can use them to circumvent intended security assumptions made by their designers and users. In addition to covering technical details about our modifications and counterfeit designs, we'll explore a few attack scenarios for each.

Sharing is Caring, so after showing off a few demonstration, we'll walk you through the process of rolling your own Secure Tokin' and Doobiekey that you can pass around the circle at your next cryptoparty.
Joe FitzPatrick
Joe is an Instructor and Researcher at https://SecuringHardware.com. Joe has spent over a decade working on low-level silicon debug, security validation, and penetration testing of CPUS, SOCs, and microcontrollers. He has spent the past 5 years developing and leading hardware security related training, instructing hundreds of security researchers, pen testers, hardware validators worldwide. When not teaching Applied Physical Attacks training, Joe is busy developing new course content or working on contributions to the NSA Playset and other misdirected hardware projects, which he regularly presents at all sorts of fun conferences.

@securelyfitz
Michael Leibowitz

Michael has done hard-time in real-time. An old-school computer engineer by education, he spends his days hacking the mothership for a large semiconductor company. Previously, he developed and tested embedded hardware and software, dicked around with strap-on boot roms, mobile apps, office suites, and written some secure software. On nights and weekends he hacks on electronics, writes DEF CON CFPs, and contributes to the NSA Playset.

@r00tkillah

#defcon25/by_track/track2/saturday #defcon25/By_Day/_saturday