Joe Grand's Hardware Implants and Espionage Workshop Agenda

Last updated: May 21, 2020

This one-day workshop focuses on the risks and realities of hardware espionage and supply chain compromise. It is a hands-on environment where students will detect and analyze various forms of surreptitious hardware. Each section provides details of the threat, real-world examples, and recommendations for detection/mitigation.

Prerequisite: Joe Grand's Hardware Hacking Basics two-day training (www.grandideastudio.com/portfolio/hardware-hacking-training/)

A. Espionage Overview

B. Hardware Implants

- Hands-on exercise: Build a keystroke-injection hardware implant, experiment with various payloads

C. Covert Channels/Data Exfiltration

- Hands-on exercise: Discover multiple methods of covert channel on a custom circuit board, capture/decode exfiltrated data

D. Component-Level

- Hands-on exercise: Identify functional difference between a known-good and modified device, determine resulting effect/weakness, reverse engineer the modification

E. Printed Circuit Board (PCB)

- Hands-on exercise: Physical delayering of an intentionally-modified custom circuit board, identify differences in layout against known-good version, determine effect of modifications