Hardware Implants and Espionage
Workshop Agenda

Last updated: November 22, 2018

This one-day workshop focuses on physical hardware implants, supply chain weaknesses, and data exfiltration methodologies. It is a hands-on environment where students will detect and analyze various forms of surreptitious hardware. Each section provides details of the technology, real-world examples, and tools/recommendations for detection.

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

A. Hardware Espionage Overview

B. Implants

C. Component-Level

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

D. Covert Channels/Data Exfiltration

- Hands-on exercise: Discover covert channel on a custom circuit board, build optical receiver circuitry, capture/decode exfiltrated data

E. Printed Circuit Board (PCB)

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