GRAND IDEA STUDIO

Hands-On Hardware Hacking: Hardware Espionage
Training Course Agenda

Last updated: October 14, 2016

This one-day class focuses on detecting, reverse engineering, and analyzing various forms of physical hardware implants and data exfiltration methodologies. Consisting of part lecture (2-3 hours) and part group exercises/open lab (5-6+ hours), students will have the opportunity to explore and experiment with different facets of surreptitious hardware. Students should have completed Grand Idea Studio's Hands-On Hardware Hacking and Reverse Engineering training course (www.grandideastudio.com/portfolio/hardware-hacking-training/) or have prior hardware hacking knowledge and experience.

A. Hardware Espionage Overview

1. Common themes and prevalent areas of attack
2. General examples, including credit card skimmers, access control, routers, PCs, keyboards/mouse, USB cables

B. Component

1. Overview and examples
2. Tools and techniques for detection
3. Hands-on: Identify behavioral differences between a known-good and modified device, detect the modification, determine the outcome

C. Side/Covert Channels

1. Overview
2. Tools and techniques for detection
3. Hands-on: Discover timing and optical side channel weaknesses on a custom circuit board, build optical receiver circuitry, identify and decode exfiltrated data

D. Printed Circuit Board (PCB)

1. Tools and techniques for deconstruction and detection
2. Hands-on: Physical delayering of a custom circuit board, identify differences in layout against known-good version, determine functionality/effect of modifications