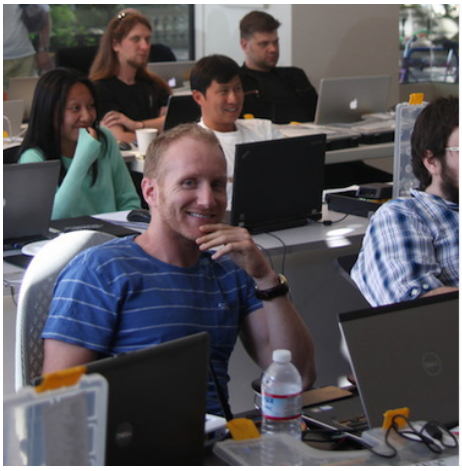
xipiter.com/training

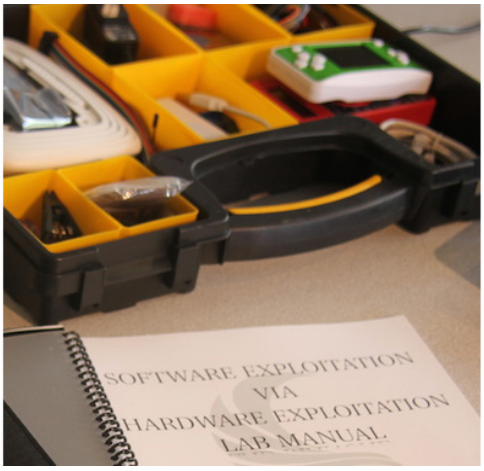
Software Exploitation Via Hardware Exploitation Training

November 10 - 13th 2014

Bechtel Conference Center / Reston, Virginia

Register today. Seats Limited





Overview:

Software Exploitation Via Hardware Exploitation teaches how to reverse engineer and exploit software on embedded systems via hardware. It teaches all this against real-world Commercial Off The Shelf (COTS) products such as routers, game systems, and other appliances. This course has an intense focus on results oriented vulnerability discovery (not just hardware hacking and tinkering for fun).

Who Should Attend:

Penetration Testers, Forensic Investigators, reverse engineers, software security auditors/analysts, software exploitation engineers, “Makers”, Tinkerers, Developers, IT Professionals, Mobile Developers, Hackers, jail breakers, and anyone interested.

About Xipiter:

This course is taught by Xipiter, a information security team that specializes in software exploitation, embedded systems and software reverse engineering. In addition to this course, Xipiter’s trainings have sold out 3 years in a row at the BlackHat USA security conference and has been privately taught at companies like Samsung, Google, and government security agencies. Members of Xipiter’s team regularly speak and present research internationally at industry conferences and have co-authored books on exploitation, reverse engineering, and embedded systems.

To register visit xipiter.com/training

Team discounts available. Email info@xipiter.com

Concepts taught (hands-on) in the course include:

- Bus spying, tampering, spoofing, injection (UART, SPI, I2C, USB, etc.)
- All you need to know about simple serial interfaces (UART, SPI, I2C)
- Finding Pinouts (JTAG, Serial, etc)
- All about JTAG: Using JTAG surreptitiously for reverse engineering, attacks, and exploit development, also: “JTAG Fuzzing”
- Stealing Firmware non-destructively (JTAG, direct interface, serial interfaces, etc.)
- Stealing Firmware destructively (pulling chips from the board and reading them)
- Parsing Firmware images and disassembling them
- Firmware analysis
- Simple Side Channel Attacks: how they work and how to use them in the real-world.
- Power Analysis and Power Side Channel attacks.
- “Glitching Attacks”
- ARM Exploitation via hardware debuggers
- Attacking Low-power RF devices (Zigbee, etc)

Students will get hands on experience with tools like:

- JTAG Adapters
- IDA, OpenOCD, GDB
- BusPirate, BusBlaster
- CPLDs (in lieu of FPGAs)
- Oscilloscopes
- Multimeter (Ammeter, Voltmeter, etc)

Details:
Length: 4 days
Format: Lecture and Lab

Location:
Bechtel Conference Center
1801 Alexander Bell Drive
Reston, Virginia 20191

To register visit xipiter.com/training
Team discounts available. Email info@xipiter.com