TROOPERS TRAININGS Make the world a safer place.

HMTS HM Training Solutions

Training:

Hacking the USB World with FaceDancer & USB-Tools

Date of the training: **March 16-17, 2020** in Heidelberg, Germany

Book now using the voucher code: **TR20_HMTS** and save an additional 5% of the current valid rate of any package!

Overview

USB connectivity has become ubiquitous: the sheer variety of USB-connected devices - ranging from computers and game consoles to resource-constrained embedded systems - has resulted in a wide variety of vendor-specific protocols and custom USB software stacks - presenting a unique and omni-present attack surface. The ability to able to fuzz, monitor, MITM, or emulate USB can often be a foot in the door for working with black box systems; whether your goal is to build tools that work with existing hardware and software, find vendor interfaces or vulnerabilities to execute custom code, or to play NSA.

This exercise-driven training covers the basics of USB and explores the role of USB in attack and defense using open-source hardware and software, including ViewSB, FaceDancer, numap, GreatFET, and Rhododendron. Over the span of two days, you'll explore the tools and techniques relevant to modern USB security, learn how to craft and defend from real-world exploits, and explore the depths of the USB security model. Course instructors will share real-world experience developing both USB tools (including FaceDancer, ViewSB, and USBProxy) and USB exploits (including the Tegra RCM exploit that completely compromises devices using NVIDIA's embedded processors, such as the Nintendo Switch).

In this training, we'll teach you what you need to get into USB hacking– including:

- Fundamentals of USB: how USB hosts and devices communicate, from the physical layer to the basics of enumeration and standard device classes;
- Understanding existing USB devices: how you can use open-source software and hardware tools to reverse engineer and understand existing USB devices;
- Understanding the USB attack surface: understanding the (lack of a) USB trust model, and understanding how misbehaving hosts and devices can wreak havoc;
- Rapid construction of new USB devices: how to use the FaceDancer toolkit to rapidly create new USB devices– including creation of misbehaving USB devices;
- Manipulation of existing USB devices: including using USBProxy to man-in-the-middle USB communications to tamper with target hosts and devices;
- Using USB skills offensively and defensively: using the skills developed thus far to attack USB hosts and devices, and understanding the challenges of securing USB hardware;
- **New this year**: automating USB security techniques; including using our tools - and building your own tools - for automatic fuzzing;
- Advanced USB techniques: including discussion and demonstration of real USB attacks developed by the trainers.

This is the fourth content iteration of Great Scott Gadgets' open-source USB training. All course materials, and all tools used in the course, are fully open source and intended to be as accessible as possible. The vast majority of the tools used and demonstrated in the course – both hardware and software (e.g. GreatFET, FaceDancer, USBProxy, ViewSB, Rhododendron) – are developed and maintained by the course trainers; providing a unique opportunity to receive training and perspective directly from the tool creators.

The course is nearly entirely exercise driven – interspersed lectures, talks, and demonstrations serve to provide context and guidance for the lab exercises. Exercises are presented in a CTF style: students log into an online CTF system and view course materials, tutorials, and challenges from the interactive portal. The web system tracks student process through both core exercises (for which time is allocated) and bonus exercises (which may be completed during any free time or outside of the training context). The CTF portal remains online after the course is complete, allowing students to continue attempting challenges on their own time.

Each student will receive a full set of all hardware necessary to complete the course (beyond the laptop they'll be required to bring), and all hardware will be theirs to take home, afterwards - allowing them to continue using their tools for both further learning and in practice.

Prerequisites

Attendees should have basic proficiency in a scripting language, with a casual familiarity with python preferred. Course exercises will involve simple python development, but a very basic familiarity with a scripting language should be sufficient.

Requirements

A laptop with at least three USB ports (or a USB hub), and which has the free VirtualBox hypervisor and extension pack installed.

About the Trainers

Kate Temkin is a seasoned USB researcher, and maintains a variety of open-source hardware and software tools, including FaceDancer, ViewSB, and GreatFET. She's discovered a number of well-known USB vulnerabilities– including CVE-2018-6242, which famously allowed full exploitation of the Nintendo Switch.
In addition to significant experience with USB, Kate has significant educational experience, having previously taught and developed university-level engineering course.

Mikaela Szekely is an open source software and hardware enthusiast with a long-standing interest in USB and embedded systems; as well as an embedded software engineer for Great Scott Gadgets. She develops for various projects including GreatFET and ViewSB. When not maintaining such tools, Mikaela contributes to a variety of open source projects, makes truly terrible puns, and hones her computer science skills in scenic Colorado.

Booking

Recommended online booking of trainings through:
https://troopers.de/tickets/

Voucher code: TR20_HMTS
Using this voucher code automatically gives you an additional 5% off the current valid price! You can register with this code until seats have run out.

Contact

Need assistance? Don't hesitate to call us. We are fluent in English and German. +49 151 16228365 or info@troopers.de

Booking is also possible offline through your trusted partner:

HM Training Solutions, Falkenstrasse 6, 63820 Elsenfeld, Germany
+49 6022 508200 / info@hmtrainingsolutions.com
+49 6022 5089999 / www.hmtrainingsolutions.com