TROOPERS19: Approximate* Schedule

Day I: Overview and First Steps

9:00-10:00	Whirlwind Tour of USB	Lecture
10:00-10:10	USB Protocol Analysis & Lab Environment Bring-up	Demo, Lab
10:10-10:30	Core Exercise 1: sniffing secrets from a packet exchange	Lab
	Bonus Exercise 1: in-depth protocol analysis	
10:30-11:00	BREAK	
11:00-11:30	Enumeration and Configuration, class drivers	Lecture
11:30-11:45	Core Exercise 2: enumeration of real devices	Lab
	Bonus Exercise 2: scoping out a system via packet capture	
11:45-12:00	MiTM'ing USB Devices with USBProxy	Demo
12:00-12:30	Core Exercise 3: bypassing USB whitelisting	Lab
	Bonus Exercise 3: bypassing software checks	
12:30-13:30	LUNCH	
13:30-14:00	USB Transfer Types and how they're used	Lecture
14:00-14:10	Communicating with USB Devices	Demo
14:10-14:30	Core Exercise 4: finding hidden USB commands	Lab
	Bonus Exercise 4: digging deeper into command arguments	
14:30-14:40	Fuzzing Embedded Systems with libusb/FaceDancer Host	Demo
14:40-15:00	Core Exercise 5: using USB hosts to attack devices	Lab
	Bonus Exercise 5: *breaking in to embedded devices via USB*	
15:00-15:30	BREAK	
15:30-16:00	Real world example: "breaking all security" on the Nintendo Switch	Demo
16:00-16:10	Emulating USB Devices: it's fun *and* good for you	Lecture/Talk
16:10-16:20	Cool Demonstrations of FaceDancer Emulation	Demo
16:20-17:00	Core Exercise 6: emulating devices to steal secrets	Lab
	Bonus Exercise 6: advanced secret stealing	

Day II: Exercises and Real-World Applications

9:00-9:30	Refresher, Waking Up, Caffeination, and USB Driver Classes	Lecture
10:00-10:10	Class driver demos: cool things with emulated devices	Demo
10:10-10:30	Core Exercise 7: attacking a system with a class driver	Lab
	Bonus Exercise 7: scoping out a target with class drivers	
10:30-11:00	BREAK	
11:00-11:30	The USB Threat Model, Common USB Mistakes, and USB Security	Talk + Demos
11:30-12:30	Core Exercise 8: building a malicious device	Lab
	Bonus Exercise 8: breaking into a host with a USB device	
12:30-13:30	LUNCH	
13:30-13:50	MiTM'ing to fuzz/attack complex devices	Talk + Demos
13:50-14:40	Core Exercise 9: MiTM'ing a synthetic system	Lab
	Bonus Exercise 9: MiTM'ing software on the host	
14:40-15:00	Advanced USB Techniques: side-channel, glitching, etc.	Talk + Demos
15:00-15:30	BREAK	
15:30-17:00	Final Challenge: low-guidance attacks on black-box systems (CTF style)	Lab