HS.T 2018: Approximate Schedule

Day I: Overview and First Steps

8:30-9:00	Arrival, Settling in, and Caffeination	Set-up
9:00-10:00	Whirlwind Tour of USB	Lecture
10:00-10:15	USB Protocol Analysis	Demo
	Lab Environment Verification	Lab
10:15-10:30	BREAK	
10:30-10:40	Core Exercise 1: sniffing secrets from a packet exchange	Lab
	Bonus Exercise 1: in-depth protocol analysis	
10:40-11:10	Enumeration and Configuration, class drivers	Lecture
11:10-11:25	Core Exercise 2: enumeration of real devices	Lab
	Bonus Exercise 2: scoping out a system via packet capture	
11:25-11:35	MiTM'ing USB Devices with USBProxy	Demo
11:35-12:00	Core Exercise 3: bypassing USB whitelisting	Lab
	Bonus Exercise 3: bypassing software checks	
12:00-1:30	LUNCH & TECH TALK Samy Kamkar – RF Attacks in the Analog Domain [12:20-1:20]	
1:30-1:50	USB Transfer Types and how they're used	Lecture
1:50-2:00	Communicating with USB Devices	Demo
2:00-2:20	Core Exercise 4: finding hidden USB commands	Lab
	Bonus Exercise 4: digging deeper into command arguments	
2:20-2:30	Fuzzing Embedded Systems with libusb/FaceDancer Host	Demo
2:30-3:00	Core Exercise 5: using USB hosts to attack devices	Lab
	Bonus Exercise 5: breaking in to embedded devices via USB	
3:00-3:15	Real world example: finding USB irregularities on the Nintendo Switch	Demo
3:15-3:30	BREAK	
3:30-4:00	Emulating USB Devices: it's fun *and* good for you	Lecture/Talk
4:00-4:15	Cool Demonstrations of FaceDancer Emulation	Demo
4:15-5:00	Core Exercise 6: emulating devices to steal secrets	Lab
	Bonus Exercise 6: advanced secret stealing	
5:00-5:20	Real world example: "breaking all security" on the Nintendo Switch	Demo
5:20-5:30	Wrap-up for first day and Q&A	Talk

This course schedule is intended as a template to deviate from–we'll adjust the course pacing to fit our students. There's a lot of depth possible in these topics: so, typically, we have more "potential material" than time.

Day II: Exercises and Real-World Applications

8:30-9:00	Arrival, Settling in, and Caffeination	Set-up
9:00-9:30	Refresher, Waking Up, and USB Driver Classes	Lecture
9:30-9:45	Class driver demos: cool things with emulated devices	Demo
9:45-10:15	Core Exercise 7: attacking a system with a class driver *Bonus Exercise 7: scoping out a target with class drivers*	Lab
10:15-10:30	BREAK	
10:30-11:00	The USB Threat Model, Common USB Mistakes, and USB Security	Talk + Demos
11:00-12:00	Core Exercise 8: building a malicious device *Bonus Exercise 8: breaking into a host with a USB device*	Lab
12:00-1:30	LUNCH & TECH TALK Mike Ryan-- Bluetooth RE Tools/Techniques [12:20-1:20]	
1:30-1:45		
1:45-2:00	MiTM'ing to fuzz/attack complex devices	Talk + Demos
2:00-3:00	Core Exercise 9: MiTM'ing a synthetic system *Bonus Exercise 9: MiTM'ing software on the host*	Lab
3:00-3:15	Advanced USB Techniques: side-channel, glitching, etc.	Talk + Demos
3:15-3:30	BREAK	
3:30-5:30	Final Challenge: low-guidance attacks on black-box systems (CTF style)	Lab

Cheat Sheet
<forthcoming>