BOSTON CYBERNETICS INSTITUTE

Vulnerability Assessment for Embedded Systems

4-Day Course

I. Course Description

This course is intended for engineers who need to perform assessments and then actually demonstrate vulnerabilities on embedded systems, IoT devices or similar systems. Students learn how to find vulnerabilities, demonstrate them by writing exploits, and communicate the nature and severity of vulnerabilities to a non-technical audience.

This is a majority hands-on course, with theory and lectures as needed. Exercises focus on embedded Linux and ARM but other architectures are mixed in for perspective. This course balances application of skills with fundamental knowledge so no one is just "going through the steps" but rather is engaging in a creative problem-solving experience, just like in the real world.

A. Learning Objectives

- Students will be able to identify vulnerabilities in embedded products
- Students will be able to bypass multiple exploit mitigations
- Students will know the pros and cons of different approaches
- Students will be able to communicate findings to management

B. Target Audience

This course is intended for the engineers and scientists who are in the weeds assessing tactical platforms for cyber vulnerabilities.

C. Prerequisites

Students are expected to be familiar with reading and writing programs in C and Python We are experienced teachers and are prepared for a variance in backgrounds in each class. We specifically address this through our exercises and environment. For the best experience, you should have a licensed copy of IDA Pro, although it is not required.

D. Class Format

Each student will receive a virtual machine which contains all the tools, exercises, and documents needed for the class. Students are encouraged to save all materials to take with them for future reference.

II. Course Schedule

Each session of each day is recorded and uploaded directly after the session is over. So even if students cannot make all the times listed, they can still review videos at their convenience.

A. Week Schedule

Day	Theme	Topics
1	Reversing Embedded Architectures	• Remote debugging with IDA Pro and QEMU • Extract, parse, and analyze firmware • Architecture specific challenges • Reversing ARM/MIPS/PowerPC binaries • Overcoming anti-analysis techniques
2	Vulnerability Analysis	• Bug classes • Source and binary auditing • Stack and heap-based memory corruption • Information disclosures
3	Exploitation	• Writing and using shellcode • Abusing stack and heap semantics • Manufacturing Information disclosures • No-execute bit, ASLR, stack canaries • Return oriented programming
4	Comprehensive	• End-to-end exploitation of an embedded device • Extract target filesystem to emulate applications • Identify vulnerabilities in software • Exploit vulnerabilities to gain control of target

B. Daily Schedule (times in EDT / UTC-04:00)

Begin	End	Length	Type
8:30 AM	10:00 AM	1:30	Session 1
10:00 AM	10:15 AM	0:15	BREAK
10:15 AM	11:30 AM	1:15	Session 2
11:30 AM	12:30 PM	1:00	Lunch
12:30 PM	1:45 PM	1:15	Session 3
1:45 PM	2:00 PM	0:15	BREAK
2:00 PM	3:15 PM	1:15	Session 4
3:15 PM	3:30 PM	0:15	BREAK
3:30 PM	4:45 PM	1:15	Session 5
4:45 PM	5:00 PM	0:15	BREAK
5:00 PM	6:00 PM	1:00	Office hours

III. Instructors

Evan Jensen is the cofounder and CTO of BCI, where he splits his time between performing assessments, creating capabilities for clients, and teaching. He is an experienced instructor in reverse-engineering and exploitation. Evan has taught seminars and courses at BU, RPI, NYU, MIT, Tufts, West Point, MITRE, and Lincoln Laboratory. Before cofounding BCI, Evan worked for Lincoln Laboratory's Cyber System Assessments Group and Facebook's red-team. He was an instructor for NYU's weekly Hack Night from 2011 to 2014, covering reverse-engineering, exploitation, and various other cybersecurity topics. He developed nearly all of the lessons for Trail of Bits' CTF Field Guide, covering vulnerability discovery, exploitation, forensics, and operational tradecraft. Jensen was heavily involved in teaching cybersecurity in the NYU Polytechnic community. He was co-instructor with Dan Guido for the course Penetration Testing and Vulnerability Analysis during Fall 2012 and Fall 2013, and was a teaching assistant for Neil Daswani for the course Application Security during Spring 2013. Passionate about enabling others to learn via the medium of repeated failure, he was CTF captain of Brooklynt_Overflow from 2012 to 2014 and founding member/captain of Lab RATs from 2014 to 2016 which placed 10th in the 2017 DEFCON CTF finals. He has a Bachelor's in computer science from NYU Tandon School of Engineering.