ENGR-E399/599
Indiana University Spring 2022
Prepared by: Austin Roach January 13, 2022

Syllabus

This course provides an introduction to embedded systems reverse engineering. Its focus is the practical exploration of the process of reverse engineering using tools and techniques relevant to embedded systems. This course will give experience with:

- Analyzing embedded systems architectures
- Identifying and interacting with debug interfaces and external communication interfaces
- Extracting information for analysis from nonvolatile memories and firmware update files
- Disassembling, decompiling, and analyzing executable code for various microcontrollers and microprocessors
- Emulating firmware
- Identifying appropriate points for analysis given a reverse engineering goal

The course will explore a range of embedded systems architectures, from those based on 8-bit microcontrollers to those based on microprocessors running embedded multitasking operating systems.

---

1 Instructor

Austin Roach
ahroach@iu.edu

2 Schedule

Lecture: Thursday 4:55PM-7:25PM, 4012 Luddy Hall
Lectures will be recorded to allow students to view lectures for which they are absent and to review lecture content as needed.

Office hours: Thursday 7:30PM-8:30PM, 2032 Luddy Hall

If students are unable to attend office hours, appointments with the instructor on Zoom can be scheduled upon request.

A tentative schedule of lecture topics is:

Date	**Topic**
01/13/22	Course introduction and overview; introduction to Ghidra
Online	ARM ISA; ARM disassembly and code analysis
01/20/22	Identifying standard library functions: manual and automated techniques
01/27/22	ELFs; RE hints from linking and loading
02/03/22	Embedded Linux systems hardware/software architecture; analyzing filesystem images; reverse engineering using operating system abstractions
02/10/22	Dynamic analysis of embedded Linux systems; emulation
02/17/22	AVR architecture and ISA; AVR disassembly
02/24/22	AVR I/O interfaces; automating interaction with I/O interfaces
03/03/22	Microcontroller emulation
03/10/22	Serial protocols and interfaces: discovery and interaction
03/24/22	JTAG; interacting with debug access ports
03/31/22	STM32F4 architecture; analyzing object-oriented code
04/07/22	Firmware update files
04/14/22	Advanced analysis and RE approaches
04/21/22	Security threats and evaluation techniques
04/28/22	ENGR-E 599 student presentations: embedded systems RE case studies

3 Prerequisites

While there are no official prerequisites, students will benefit from some familiarity with:

- electronics
- programming in C and Python
- assembly language in at least one architecture
- microcontroller or bare-metal microprocessor programming
- operating systems

Background in these areas will be provided as needed for the assignments. If a student needs more background information in a particular topic area than is provided during lecture, they should inform the instructor so that additional resources or instruction can be provided.

4 Textbooks

This course has no official textbook. Some generally useful references are listed below. References relevant to particular topic areas will be presented during class.

Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation
Bruce Dang, Alexandre Gazet, Elias Bachaalany, and Sébastian Josse
John Wiley & Sons
ISBN-13: 978-1-118-78731-1
https://iu.skillport.com/skillportfe/main.action?assetid=62680

Reverse Engineering for Beginners
Dennis Yurichev
Self-published
https://beginners.re/

Hacking the Xbox: An Introduction to Reverse Engineering
Andrew "bunnie" Huang
No Starch Press
ISBN-13: 978-1-59327-029-2
https://bunniefoo.com/nostarch/HackingTheXbox_Free.pdf

The Ghidra Book
Chris Eagle
No Starch Press
ISBN-13: 978-1-71850-102-7

The IDA Pro Book
Chris Eagle
No Starch Press
ISBN-13: 978-1-59327-289-0
https://iu.skillport.com/skillportfe/main.action?assetid=43616

Practical IoT Hacking
Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, and Beau Woods
No Starch Press
ISBN-13: 978-1-71850-090-7

5 Lectures

Lectures will be recorded for later viewing. Lecture materials, including slides and any other resources used during the lecture, will be shared in a course git repository.

6 Assignments

Assignment submissions should include a written description of the techniques that the student used to complete the assignment and the details that were learned through the analysis. Assignment submissions may either be flat text files or PDFs. Some assignments may also require the submission of supporting artifacts, such as analysis files from the disassembler or source code for programs that were written to interact with a system.

Late portions of an assignment will be accepted, but the points awarded for any late portions will be reduced by 50%. Even if an assignment is incomplete, students are strongly encouraged to submit whatever they have completed by the due date in order to maximize the awarded points.

7 Policy on working together

Cooperation on the assignments is accepted and encouraged. Any collaborators must be acknowledged on assignment submissions, and assignment reports and source code must be written independently. **Duplication of another student's work is not permitted, and will result in a score of zero points for the assignment.**

8 Hardware

Students will be provided with hardware to support some of the assignments. Students should plan to return the hardware kits by the date of the final class.

9 Class participation

Class participation accounts for a small fraction of the final score. Students can show their continued engagement with the course material in a variety of ways, such as by attending lectures, participating in discussions, attending office hours, or corresponding with the instructor about assignments or course topics.

For students in the ENGR-E 599 version of the course, full participation will also include the delivery of a 10-15 minute presentation on an embedded systems reverse engineering topic of the student's choice during the final class period. This could be a summary of a research paper, details of a project found online, or a description of a project undertaken by

the student outside the course. More information about the presentations will be provided mid-way through the semester. If students would like help choosing a topic for presentation, they are encouraged to contact the instructor.

10 Grading

Grading will be calculated from a combination of assignment grades and class participation. There are no exams.

Assignments	**Participation**
95%	5%

In the event that alterations to the course plan require changes to this weighting, any changes will be communicated on Canvas.

The cutoffs for assigning letter grades are as follows:

Percentage	**Letter grade**
93%	A
90%	A-
87%	B+
83%	B
80%	B-
77%	C+
73%	C
70%	C-
67%	D+
63%	D
60%	D-
<60%	F

The instructor reserves the right to decrease the grade cutoffs during the course. In other words, the scale above represents the *minimum* letter grade that will be assigned, and the instructor may choose to restructure the scale to assign better grades at their discretion. Any changes to the grading scale will be communicated with a post to the course Canvas site.

Grades of A+ will be assigned for extraordinary achievement during the course.

11 Communications

Official announcements, course materials, and descriptions of labs and assignments will be posted to Canvas. Students will also submit their assignments on Canvas.

If a collaborative discussion forum (a Slack workspace, for example) would be of interest to the class, one may be established with details for joining posted to Canvas.

Please e-mail the instructor for any discussions related to personal matters, grades, or course administration.

12 Disability services for students

If a student needs an accommodation for a disability, they should inform the instructor during the first three weeks of the semester. Some aspects of this course may be modified to facilitate the student's participation and progress. Once the instructor is aware of a student's needs, they can work with the Office of Disability Services for Students (DSS) to help determine appropriate academic accommodations. Any information that a student provides is private and confidential.