University of Michigan Electrical Engineering and Computer Science — Handout 2
EECS 598-008: Medical Device Security — January 9, 2013
Instructor: Kevin Fu

Course Information

Instructor: Prof. Kevin Fu
Room BBB 4628, 616–594–0385, kevinfu@umich.edu
Office Hours Mondays: 12:00–1:00PM or by appointment
(Please CC calendar requests to Quinn Stewart, qunstwrt@umich.edu)

Web page: http://eecs.umich.edu/courses/eecs598-008/

1 Overview

This graduate-level course teaches students the key engineering concepts and skills for creating more trustworthy software-based medical devices ranging from pacemakers to radiation planning software to mobile medical apps. Topics span computer engineering, human factors, and regulatory policy. Students will master technical skills such as reverse engineering, static analysis, fuzz testing, hazard analysis, validation, requirements engineering, radio-frequency communication, physiological sensing, and fundamental concepts from system engineering that lead to safer and more effective medical devices that are increasingly interconnected and wirelessly controlled.

Students will apply the newly learned concepts and skills by analyzing the security of a real-world medical device in a hands-on term project. Interdisciplinary teams (when possible) will consist of students from complementary backgrounds to mimic the composition of teams at medical device manufacturers and regulatory bodies. Occasional guest speakers from medical device manufacturers, hospitals, and government will complement the classroom activities with critical lessons from the front lines.

Intended audience. This 3-credit course is designed for graduate students in Computer Science and Engineering and upper-level undergraduates with appropriate computing background (e.g., excellent grades in EECS 280, EECS 370, or EECS 388 would suffice). Students from ECE, Informatics, BME, and IOE are especially welcomed, as are medical students with appropriate computing experience. Students without computing experience are welcome to audit the course after registering for visiting credit.

Prerequisites. Students are expected to have graduate-level standing or permission of the instructor. There are no other formal prerequisites because this course is highly interdisciplinary. No one would have all the prerequisites across all the skill sets!

Time and location. Lectures are held in Dow 1010 on Mondays and Wednesdays from 10:30 AM to 12:00 PM. Note that the room number is decimal, not binary. Don't get lost like the instructor. A schedule of topics is posted on the Web site.

2 Textbook: A Course Reader

There is no textbook for this course. Instead, we have arranged for a course reader that provides excerpts from several hard-to-find and out-of-print sources. The course reader is $57.09 available via Dollar Bill Copying (`dollarbillcopying.com`). You may order the book online for shipment, or order online for pickup at their store near Central Campus (Dollar Bill Copying, 611 Church Street, Ann Arbor, MI).

Copyright licensing is the primary cost of the reader. To keep costs low, we have not printed the documents that are already available online. We were unable to secure copyright licenses to provide electronic copies of the course reader, but please let the instructor know if you find any freely available versions online.

If you have a financial hardship that makes it difficult to purchase the course reader, please ask the instructor about other options.

3 Grades and methods of evaluation

Students will be evaluated based on a group term project, individual problem sets, in-class exams, and class participation. The assignments will involve a balance of team and individual work ranging from hands-on labs to technical writing. Grading is weighted as follows:

Group project	40%
Individual homework/labs	30%
Two in-class exams	20%
Class participation	10%

Passing the class is not possible without completing the final project and participating in class, regardless of your other grades.

3.1 Exams

There will be two in-class exams during the semester. Exams are **closed book**. The intent of each exam is to test your understanding of the material from the readings and lectures. Each exam is not intended to be a comprehensive or cumulative exam, but you may need to understand past material to answer exam questions that build on past material.

If you miss an exam for reasons other than a documented medical or personal emergency, you will receive a zero for that exam. If you anticipate a conflict with an exam time, talk to the instructor at least one month before the exam date to schedule an oral exam. Exam dates are given at the beginning of the semester so you can avoid scheduling job interviews or other commitments on those days. Outside commitments are not considered a valid reason for missing an exam.

3.2 Homework

Individual homework will consist of both technical essays responding to research papers, and hands-on homework assignments related to technical problem solving. Due dates will appear on the Web site.

Technical essays are one-page responses to a technical question relating to assigned reading material. The essay should follow strategies for effective technical writing. The essays will be graded on both the quality of writing as well as the effectiveness of the technical argument. Your responses should fit comfortably on one page, and have no more than 400 words. Paper responses are due *before* the start of lecture. At 10:40 AM, a homework assignment will be considered late. Submit your PDF responses (no Word docs allowed) via CTools.

Absolutely no collaboration is allowed on the essays; see the plagiarism policy later in this document to avoid failing the course.

3.3 Group project

Medical devices are created by interdisciplinary teams. Thus, this course has a group project. We will assign you team partners and will attempt to balance various constraints such as scheduling and ensuring a team of diverse technical skills.

Each team will have 3–4 members. You will be responsible for organizing team meetings around your many schedule constraints. Effective teamwork is essential. We will spend class time discussing how to be a good team partner. Similar to other EECS courses, we expect all group members to contribute their fair share, and we expect to assign the same project grade to all members of a group. To help ensure this, group members will evaluate the contributions of other group members after each project. Members who contribute less than their share may receive a lower grade on the project; non-contributing members will receive a zero. In case of disputes regarding contribution, an instructor may interview group members.

You're fired. Students may be fired from a group by the majority vote of the remaining members. The procedure for this is as follows: (1) documented "gentle warning" of risk of firing in e-mail, with CC to all group members and to `kevinfu@umich.edu`, with cause and specific work required to remain in group; (2) allow at least 72 hours for compliance; (3) if the problems persist, e-mail statement of firing to the group and to `kevinfu@umich.edu`. Fired group members may join another group; students who cannot find a group must complete the remaining project by themselves.

Managing group dynamics and using each group member's time and talents effectively can be difficult. If there are problems with your group, please see the instructor as soon as possible. Be open and candid with your group about potential problems early on so your group can plan around those problems and not fall behind. A sure way to make your group upset at you is not finishing your work at an agreed-upon deadline and not informing them about the problems early enough for them to help. We encourage everyone to read "Coping with hitchhikers and couch potatoes on teams" by Barbara Oakley.

Options for group projects.

1. Reproduce the results of a medical device security research paper (e.g., run your own experiment or run your own simulation). Suggested venues from which to draw papers include the USENIX Security, IEEE Symposium on Security & Privacy (aka Oakland), ACM CCS, NDSS, SIGCOMM, and USENIX HealthSec/HealthTech. Check with the instructor if you have a passion for a different venue and seek permission to use a paper for your project.

2. Thoroughly analyze the security and privacy of a medical device. I presently can provide access to a large collection of both implantable and bedside medical devices for analysis. I can also provide binaries and source code to a few interesting medical devices. This choice is much more open ended. The advantage is that there is more room for creativity, but the danger is that the problem is very open ended and could result in disaster if the project does not work out in the end. A team should come to office hours to discuss this option.

No two teams may choose the same project. Don't worry—there are enough to go around.

Components and milestones. Project milestones will be spaced throughout the semester to make sure everyone keeps up. The best possible outcome of a class project is a publishable research artifact. You may not, however, receive credit for the same project twice, e.g. by undertaking an independent study for the same outcome.

There are four components to your project grade: a project proposal, a midterm status report, a final project report, and a project presentation. The due dates for each of these milestones will appear on the course Web page. You cannot pass the project unless each is completed.

Communicate with your teammates! Lack of communication could result in a dysfunctional team that risks failing the class. If you have tried repeatedly to communicate with an unresponsive team member, contact the instructor before the problem becomes unmanageable.

Project proposal due February 4 (20%). Your proposal should explicitly state the problem your project will address, your project's goal and motivation, related work, the methodology and plan for your project, and the resources needed to carry out your project. Be sure to structure your plan as a set of incremental milestones and include a schedule for meeting them. Part of the grade will involve peer review; we will pseudorandomly assign another team to provide a constructive critique of your proposal.

In-class mini oral report due February 27 (5%). Team will give in-class, oral presentations (5 minutes max) explaining the outputs and outcomes so far, the wrong turns, and the changes in response to the proposal feedback.

Status report due March 25 (25%). Your status report should contain enough data and analysis to show that your project is on the right track. You should append a copy of your original proposal with instructor comments, along with any surprising results or changes in direction, schedule, etc. You should also have a refined version of the problem statement and goals, as well as a more developed related work section. Part of the grade will involve peer review; a different team will provide a constructive critique of your status report.

Final report and Presentation due April 22 (50%). A final report describes your research problem, contributions, results, and analysis. You will present your research problem, analysis, and results in a brief presentation. The presentation may include a system demo if appropriate. The final report must include a paragraph explaining, for each team member, their contributions and duties in the project. Part of the grade will involve peer review; students will provide a constructive critique of presentations.

Peer Rating of Team Members (weighting factor) To encourage team members to contribute to the success of the project, individual grades will take into account peer ratings from each team member. Ratings are excellent, very good, satisfactory, ordinary, marginal, deficient, unsatisfactory, superficial, and no show. The course staff will use the peer feedback as a weighting factor for individual grades for the team project. We provide the following examples of weighting factors. A student receiving all "excellent" or "very good" ratings would receive a 100% weighting factor for the team grade. A student receiving all "ordinary" ratings would receive a 75%. A student receiving all "deficient" ratings would receive a 50%. Universal ratings of superficial or no show would result in a zero for the team project.

Your report should follow the structure of a research paper. Your presentation should follow the structure of a research talk. We will discuss how this is done in class.

3.4 Class participation

Students can participate in class in several ways. At the beginning of class, students will have the opportunity to present a 5-minute talk on a research-worthy, intellectually-stimulating topic in medical device security that is thematically related to the topic of the day (but not the assigned reading). The material could draw upon one of the optional papers, or a paper that you find. You may sign up for a time slot. Students can also engage in discussion during class and on the class discussion forum. Quality rather than quantity counts most in this subjective evaluation. One can also gain class participation credit by signing up to "shepherd" other teams' projects. That is, you can provide feedback on write-ups.

4 Policies

4.1 Lateness

Each student is granted one "penalty free" late pass for turning in a homework assignment. You need not provide any excuse. A free late means you may turn in the homework by **10:40 AM** on the day of the **next class** without penalty. We will strictly enforce the deadline; we do not want to encourage lingering on old assignments that delay new assignments. Homeworks will be accepted **only as emailed PDF files**. The turn in date is when we receive the message, not when you send it. Any late homework beyond your one freebie will result in a zero grade. Late freebies may **NOT** be used for any of the term project assignments. A late final project assignment (i.e., the proposal, status report, or final report) will have a **20% grade reduction** for each late weekday (10:41 AM).

4.2 Ethics, Law, and University Policies

This course shares the same ethics guidelines as EECS 588 (Computer and Network Security).

To defend a system you need to be able to think like an attacker, and that includes understanding techniques that can be used to compromise security. However, using those techniques in the real world may violate the law and the university's computing practices, or may be unethical. You must respect the privacy and property rights of others at all times, or else you will fail the course. Under some circumstances, even probing for weaknesses may result in severe penalties, up to and including civil fines, expulsion, and jail time.

Before engaging in any security analysis, carefully read the Computer Fraud and Abuse Act (CFAA),[1] a federal statute that broadly criminalizes computer intrusions. This is just one of several laws that govern hacking. The EFF provides helpful advice on vulnerability reporting[2] and other legal matters[3]. Contact the instructor if you have any concerns.

Please also review CAEN's policy document[4] on rights and responsibilities for guidelines concerning use of technology resources at U-M. As members of the university, you are required to adhere to these policies.

4.3 Collaboration and plagiarism

All projects in this course are to be done by your own group and in accordance with the College of Engineering Honor Code[5]. Violation will result in a zero on the project in question and initiation of the formal procedures of the Engineering Honor Council. We will use automated programs and manual checks to correlate projects with each other and with prior solutions. (obviously this year there are no prior solutions.)

You may discuss material with others, but your writing must be your own. When in doubt, contact the instructors about whether a potential action would be considered plagiarism.

When discussing problems with others, excluding projects, do not show any of your written solutions to others, including code. Do not take notes about the solution other than to jot down publicly available references. Use only verbal communication.

Using someone else's code or API is forbidden. You may use publicly available code (libraries and open source material) if code was published before we assigned the work. If you find code that trivially solves some problem we have assigned, we expect you'll tell us where so that we learn the homework assignment is moot.

If you do discuss material with anyone besides the instructors, acknowledge your collaborators in each write-up. If you obtain a key insight with help (e.g., through library work or a friend), acknowledge your source, briefly state the insight, and write up the solution on your own. In most of your write-ups, we expect to see citations.

We cannot emphasize enough that **you MUST cite all your sources** properly. You must remove any possibility of someone else's work from being misconstrued as yours. We consider the facilitation of plagiarism (giving your work to someone else) as plagiarism as well. If we detect two homework assignments that share text, both persons will be disciplined.

Investigating plagiarism is a pleasant experience for neither instructor or student. Please help us by avoiding any questionable behavior. Please come see us anytime if you are unable to keep up with the work for any reason and we will work something out. We want to see you succeed and will do everything we can to help you out!

[1] http://www.law.cornell.edu/uscode/18/1030.html

[2] https://www.eff.org/issues/coders/vulnerability-reporting-faq

[3] https://www.eff.org/pages/grey-hat-guide

[4] http://www.engin.umich.edu/caen/policies/

[5] http://www.engin.umich.edu/students/honorcode/code