Security Lab

An interdisciplinary minor at the Rotterdam University of Applied Sciences

Maintainers	Arne Padmos (padam@hr.nl), Diederik de Vries (vried@hr.nl)
Institute	School of Communication, Media, and Information Technology
Start date	2016.08.29
ECTS	30
Language	English
Abstract	Are you a designer or a techie? Do you want to become a security analyst? We will teach you how to test a system for vulnerabilities.

Summary

Security plays an increasingly important role in today's world as our society grows more and more interconnected. To gain assurance of the security of things like connected cars and pacemakers, it is essential that such systems be adequately evaluated. In our minor, students learn how to evaluate the security of connected devices. Building on a creative capacity or a technical background, we challenge students to become security analysts. We teach students the security mindset: the ability to spot problems in complex systems and how these problems can be exploited. This mindset is applied to a holistic security evaluation, where different targets of evaluation are inspected from multiple angles.

Justification

Security is a focus areas of CMI. We extend the curricula by taking on security evaluation from an interdisciplinary angle. This enables students to tackle future security concerns. Building up to the same learning objectives, students attack problems from two points: techies deepen their knowledge while designers apply their craft in novel contexts. The security mindset is nurtured by applying evaluation strategies and methods in a context of connected medicine, intimate devices, and communication platforms for civil society.

Objectives

Our competence profile is that of the security analyst, with a focus on the cryptography, computer security, network security, and human factors layers within the testing phase. After the minor, students can spot common errors, select and execute fitting evaluation strategies, write reproducible audit reports providing actionable advice, and responsibly disclose their findings. In terms of types of evaluations, students can apply red and blue teaming, laboratory testing, and field study research methods in a security context.

Prerequisites

Students do not need to study a specific major, but they need to have in-depth technical knowledge of computer systems and/or in-depth knowledge of human factors (HCI/UX). Given the workload, students should not have retakes or similar availability constraints.

Content

Students start with a focus on theory, consisting of classic cases, theories, and hands-on exercises in cryptography, computer security, network security, and the human factor. Subsequently, students in the technical track construct safety-critical connected devices, audit open source projects, and perform web app penetration tests. Alternatively, in the human track, students architect privacy-respecting intimate products, test the usability of encrypted email and chat, and run a phishing campaign to raise employee awareness.

Format

Days with a theory focus start with a news recap, followed by a demo hack, case studies, conceptual abstractions, theoretical questions, and a class discussion. For the afternoon, a toy system is presented which students try to break in groups. Everyone hands in their lab journal by 08:30 on paper. The following morning at 09:00 a short quiz is given and selected individuals present hacks and answer critical questions. Project days are free-form: they start with a stand-up, give support as needed, and end with a status update. Projects consist of phases (e.g. exploration, orientation, exploitation/experimentation, reporting). A phase starts on Monday, has a deadline of 14:00 on Friday, and closes with lightning talks. The first project is done in pairs, the second as a group, the last alone.

Assessment

Theory is given in the first four weeks through cases and exercises. A literature survey and knowledge sharing in the projects ensures a proper balance of theory and practice. Assessment in theory weeks is based on active participation (assessed through selective presentation of answers), daily quizes, and lab journals. In all project weeks, formative feedback is given that must be integrated in the final report and presentation for a pass. Retakes take place in week 20, consisting of portfolio-based criteria-guided assessment interviews. Assessment of projects happens only if enough engagement has been shown by the student. The same goes for the retake. A failed retake means a failed minor. The final grade is the mean project grade, provided that three-quarter of all quizes has been passed. Grading of projects is done intersubjectively by a minimum of two lecturers.

Reading

Theoretical and practical background is given in class, and there are specific books for further reading. A list of all books used for the different parts of the minor is given at http://roselabs.nl/links/, including links to audits reports. An open source course book (ISBN 9789082436808) is being developed at https://github.com/arnepadmos/book.

Planning

The minor runs from week 1 in Q1 to week 10 in Q2. Full-time attendance is required. Students are expected to arrive at the security lab by 09:00 (WN.05.023). The day ends around 17:00. One day consist of 3 contact hours and 5 hours of group work; each week has 15 contact hours. The total workload is 840 hours, which is equivalent to 30 ECTS.