Software Security - spring 2015 (old page)

This is a joint (4 credit) course between Aalto University Department of Computer Science & University of Helsinki Department of Computer Science in spring 2015. The course code for Aalto University is T-110.6220 and for University of Helsinki is 582708. Lectures will be held by Antti Vähä-Sipilä from F-Secure Corporation.

Course staff

- Antti Vähä-Sipilä (lecturer, avs on IRC, avs_at_iki.fi, Twitter)
- N. Asokan (professor responsible for the course, n.asokan_at_aalto.fi)
- Ravishankar Borgaonkar (local organization, ravishankar.borgaonkar_at_aalto.fi)
- Hien Truong (local organization, hien.truong_at_cs.helsinki.fi)

Course staff can be reached by email.

The course IRC channel is #tkt-swsec on IRCnet, which was inherited from the 2014 course at the University of Helsinki. You are welcome to join here to meet other course participants! If you have any questions about content and want to chat, feel free to contact the lecturer on IRC (I'll react if I'm awake and online).

The course uses Moodle for returning weekly exercises, lecture notes, and for public lecture Q&A.

Thanks

I'd like to thank F-Secure, nSense and Microsoft for their support in making the course possible.

News

- No news at the moment. Please read the course email list.

Course Overview

This is a basic course on software security. The target group are software developers and generalists who are not necessarily security specialists. However, the course provides a lot of practical insight to those contemplating security related career options. The content of the course is geared towards practical and commercial software development.

The course will explain how software breaks in the security sense, and how to determine whether software is broken. We look at the variety of activities and strategies available for software developers and organizations to create more secure software. We learn how to perform security and privacy threat modelling (architectural risk analysis and privacy impact assessment), and how to apply language-theoretic approach to security engineering. We conclude with economics of software security, its regulation (mainly from a Finnish and EU viewpoint), and relationship to society.

Prerequisites

Students need to be familiar with operating system basics such as the concepts of processes and memory allocation, fluent in at least one programming language, understand the concept of a protocol stack, know how HTTP works, and be comfortable on the command line on GNU/Linux, Mac OS X, or Windows. Prior information security knowledge is not a requirement.

For some of the weekly exercises, you need access to a computer (GNU/Linux, Mac OS X or Windows) with a Java JRE.

Grading and passing the course

Weekly exercises

The course has no exam, but has six weekly graded home exercises, whose average score will be the final grade. Students must complete at least four of the six exercises in order to get a final grade. A skipped exercise will be evaluated as zero. Grading guidelines are available from Moodle.

Each exercise deadline is one week after the lecture. Exercises are returned on the course Moodle page.

Responses to weekly assignments can be written in either English or Finnish. Writings must be returned in plain text (including Moodle text fields), HTML or PDF formats. Images (diagrams drawn in some assignments) must be returned in PDF, JPEG or PNG formats. If using lossy compression, please use maximum quality settings.

Weekly exercise support sessions

In addition to the lectures, we have an optional support meeting each week where we can discuss any challenges you might face with the weekly exercises. This is where you can get face-to-face support or discuss your ideas. If nobody has any problems, we will discuss the weekly lecture topic in more depth - typically real life experiences and other unstructured discussion as long as we have something interesting to share. As said, these sessions are fully optional. You can also ask lecture and exercise specific questions on the course Moodle page.

Lectures

Although lectures do not, strictly speaking, have mandatory attendance, we would ask you not to enroll on the course unless you really also plan to attend the lectures. The course has limited space and there *will* be someone else who wants to attend. If you are looking for a completely virtual course, have a look at Coursera's Software Security course instead.

Lecture notes

Each course participant is required to write lecture notes for one of the lectures that they'll attend (pick the week you want here). These lecture notes are shared with all of the other course participants and may be published on this course wiki page. This means that several people will write lecture notes for a single lecture.

Lecture notes deadline is one week after the lecture. They are not graded, but need to be written. Lecture notes are returned through the course Moodle page.

Lecture notes must be written in English, as they will be shared with other students who might not speak Finnish.

Concept inventory tests

This course is also an experiment in computer security education. We will measure the participants' knowledge of some key concepts immediately before and after the course using a 15-minute multiple choice test. This test is pseudonymous; it will not affect your grade, and we are not interested in the identity of any single responder. The only thing we require is that we can correlate the responses before and after the course.

Course Registration

Registration is now closed.

Schedule

- Lecture Room: T6 room of Aalto CS building, Konemiehentie 2, Espoo
- Time: Lectures on Monday (08 to 10) and Exercise session on Wednesday (08 to 10)

Date	Lecture topic	Lecture notes	Weekly Assignment Support & Discussion Meeting (Optional)	Exercise and deadline (all deadlines 23:55 UTC+3)
Mon 13 Apr	• Concept inventory test • Introduction • How software breaks (low level)	(Removed, see 2016 page)	15 Apr • More advanced fuzzing concepts (demos and discussion possible)	(Removed, see 2016 page)
Mon 20 Apr	• How software breaks (web apps) • Concepts of language theoretic security	(Removed, see 2016 page)	22 Apr • Deeper dive into Burp Suite Professional	(Removed, see 2016 page)
Mon 27 Apr	• Security in a software project • Visitor: A consultant's view - Henri Lindberg from nSense	(Removed, see 2016 page)	29 Apr • Modern software development processes and security activities	(Removed, see 2016 page)
Mon 04 May	• Threat modelling (architectural risk analysis) 1	(Removed, see 2016 page)	None; if you have challenges, post a question on Moodle.	(Removed, see 2016 page)
Mon 11 May	• Engineering for privacy • Threat modelling (architectural risk analysis) 2	(Removed, see 2016 page)	None; if you have challenges, post a question on Moodle.	(Removed, see 2016 page)
Mon 18 May	• Software security in the society • Economics of software security • EU and national regulation • Concept inventory test	(Removed, see 2016 page)	20 May • Case studies of real threat modelling that were interesting or lead to architectural changes	(Removed, see 2016 page)

Books

Neither book is a strict requirement for passing the course, but will support your learning as follows: If you have no previous exposure to software or application security, you would be strongly recommended to obtain the Secure Coding book, and if you are planning to work in information security, I recommend getting the Threat Modeling book.

1. Mark G. Graff, Kenneth R. van Wyk: Secure Coding: Principles and Practices. O'Reilly, 2003. The book is out of print, but it is still available to buy directly from O'Reilly as a DRM free PDF: http://shop.oreilly.com/product/9780596002428.do. (Hint: O'Reilly regularly has 50% off days, at least on "the day against DRM" on May 6th)
   Note: Aalto students can loan E-book copy (DRM protected) for 1 to 7 days from Alli. Link https://alli.linneanet.fi/vwebv/holdingsInfo?searchId=910&recCount=25&recPointer=0&bibId=673820
2. Adam Shostack: Threat Modeling: Designing for Security. Wiley, 2014. http://threatmodelingbook.com/
   Note: E-book copy is available for 14 days for Aalto students. Link - http://site.ebrary.com/lib/aalto/detail.action?docID=10837601

Other

This course was lectured for the first time in 2014 at the University of Helsinki. You can find the old course pages on their wiki. Please don't copy their answers.

This course is not a CYBERsecurity course.