Introduction
TDDC90 – Software Security

Ulf Kargén
Division for Database and Information Techniques (ADIT) at the Department of Computer and Information Science (IDA)
Agenda

• Why study software security?
• Organization of the course
  • Course contents
  • Prerequisites
  • Lectures overview
  • Labs
  • Paper presentation
  • Reading material

Examiner
Nahid Shahmehri

Course leader
Ulf Kargén
Why study software security?

1. What kind of software is security critical?
2. Why do people try to hack software?

15 years ago

1) Mostly server software
2) Fun

Today

1) Pretty much all software
2) Profit

- Hackers increasingly target end-user equipment
- Break-ins happen increasingly by exploiting client-side software (document viewers, media players, browsers), not by attacking central infrastructure
- “Everything” is connected to the internet
Why study software security?

Software is everywhere …
Developing secure software requires…

- Security-aware developers
  - Know about common vulnerability types
  - Know common attacks
  - “Think like a hacker”
  - The devil is in the details…

- Adequate software engineering processes
  - Methods for eliciting security requirements
  - Security in the specification, architecture and design
  - Secure coding guidelines and patterns

- Software security assurance methods and tools
  - Many methods:
    Code reviews, formal methods, static analysis, fuzzing, etc.
Organization of the course
Organization

- 9 lectures
- 3 mandatory labs
  - Pong – the insecure ping
  - Static analysis
  - Web security
- Mandatory oral presentation
  - Read a paper on web security and present at end of course
- Examination:
  - Written exam (3 hp)
  - Labs + presentation (3 hp)
Prerequisites

• Required:
  • Basic computer security course
  • Programming experience
  • Course in software engineering

• Recommended:
  • Operating systems and assembly programming basics
  • Some prior experience with C-programming
  • Basic course in logic
  • Basic web programming
    (HTML, JavaScript, some server-side language)
For those unfamiliar with C

Google these things (in this order):
✓ C pointers
✓ Pointer arithmetic
✓ Pointers and arrays
✓ C dynamic memory allocation
✓ C sizeof operator
Lectures

• Secure software development (1 lecture)  
  Given by Ulf Kargén
  • Secure software development processes
  • Secure design patterns
  • Modeling and risk analysis

• Vulnerabilities and exploits (2 lectures)  
  Given by Ulf Kargén
  • Common vulnerabilities in C/C++ programs
  • Known attack techniques
  • OS and compiler mitigations
Lectures (continued)

• Web security (1 lecture)
  Given by Ulf Kargén
  • Common vulnerabilities in web applications
  • Attack techniques and protections

• Code reviews (1 lecture)
  Given by Kristian Sandahl
  • Software inspections and other techniques
Lectures (continued)

• Static analysis (2 lectures)
  Given by Ahmed Rezine
  • Introduction to static analysis
  • Abstract interpretation
  • Symbolic execution

• Security testing and course wrap-up (1 lecture)
  Given by Ulf Kargén
  • Fuzzing, concolic testing
  • Course wrap-up
Labs

• Pong – the insecure ping
  • Perform a code review to find vulnerabilities
  • Exploit a buffer overflow to gain root
  • Fix all vulnerabilities

• Static
  • Study common static analysis techniques described in the lectures

• Websec
  • Deliberately vulnerable web app
  • Study common weaknesses and understand attack techniques
Labs

- One group for all students
  - Different assistants for each lab – see lab page on course web

- Webreg signup deadline **November 15th**
  - Unregistered students not allowed to sign up!

- Students are required to work in pairs
  - If you sign up alone, we may randomly group you with another student.

- **Hard** deadline for handing in solutions is **December 20th**
  - Complete all labs **at least one week before this** to allow time for corrections and re-submission
  - Hand in solutions continuously during the study period – don’t save everything for the last week!
  - Start with labs **as early as possible**, especially Pong!
Presentation

• Mandatory oral presentation
  • Done in pairs (same as for labs)
  • Read paper on web security and present on seminar
  • Both students must participate in presentation and contribute equal parts
  • Detailed instructions on web page (TBA)
• Presentations seminar at **December 14**
  • Presentations are 10 – 15 minutes + plus questions
  • Several other milestones prior to that (see web page)
Reading material

- No course book (no one book covers all topics in the course)
- Mandatory reading:
  - Papers/articles, web resources, and lecture slides
  - Lectures don’t cover all articles, and vice versa
- Also a list of extra reading for interested students
  - Not needed for exam
Questions?