Introduction

TDDC90 – Software Security

Ulf Kargén

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

LiU EXPANDING REALITY

Agenda

- Why study software security?
- Organization of the course
  - Course contents
  - Prerequisites
  - Lectures overview
  - Labs
  - Reading material
  - Course evaluation

Examiner
Ulf Kargén

Lecturer
Ahmed Rezine

Lecturer
Kristian Sandahl

Lab assistant
Alireza Mohammadinodooshan

Why study software security?

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

20 years ago

1) Mostly server software
2) Fun

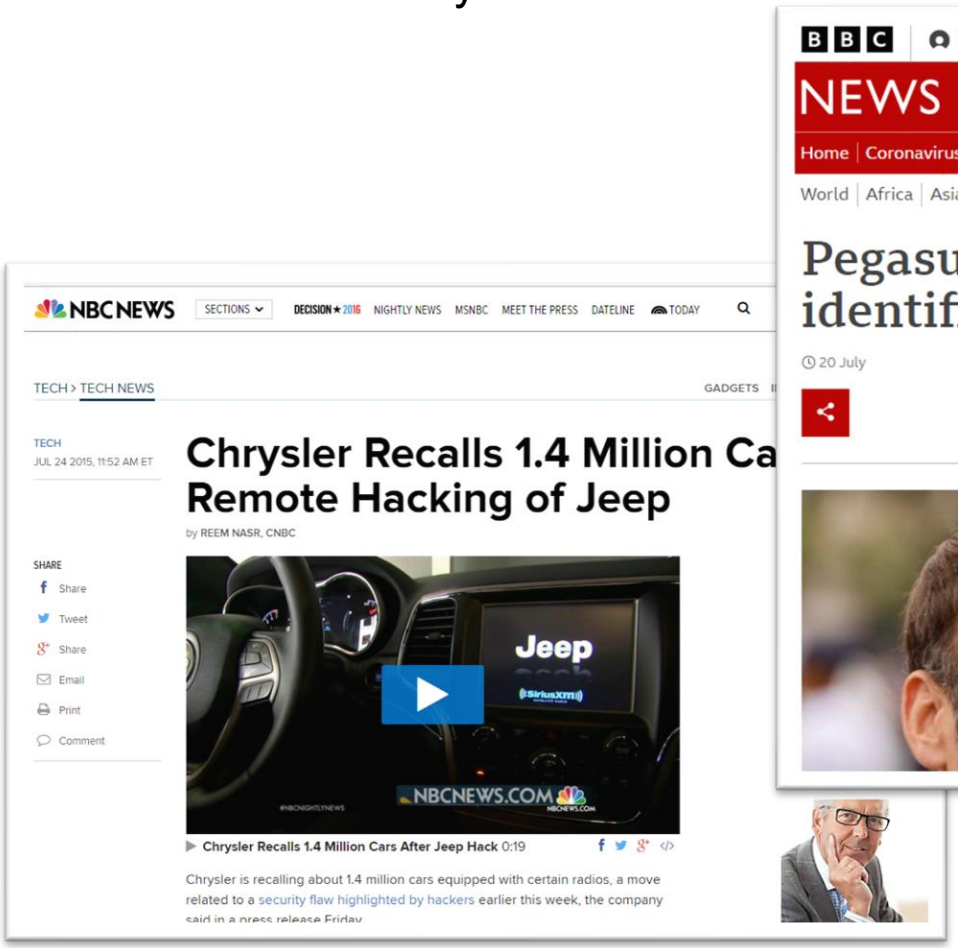
Today

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 – attacks against poorly secured IoT targets are very common

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
  - Web security
  - Static analysis
- Examination:
  - Written exam (3 hp)
  - Labs (3 hp)

Detailed information on course organization, lecture slides, lab instructions, etc., is available on the course web site:

https://www.ida.liu.se/~TDDC90/index.en.shtml

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
  - Pay special attention to the difference between sizeof on pointers and arrays!

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
  - **Requires considerable time and effort, especially if you don't posses all recommended prerequisite knowledge**
- Websec
  - Deliberately vulnerable web app
  - Study common weaknesses and understand attack techniques
  - Typical time needed: 1-2 lab sessions
- Static
  - Study common static analysis techniques described in the lectures
  - Typical time needed: 1-2 lab sessions
  - **Note:** Requires demoing for me or Ahmed.
    The other labs do **not** require demos.

Labs

- Different assistants for some labs – see lab page on course web
- Webreg signup deadline **November 8th**
  - Unregistered students not allowed to sign up!
- Labs are meant to be done in pairs
  - *Might* be possible to do labs alone if you have a good motivation, **however:**
  - If too many sign up alone, we may randomly group lone students.
- **Hard** deadline for handing in solutions is **December 16th**
  - 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!

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

Previous year's course evaluation

- Overall score last year was 4.56 (of 5)
- Scores of all evaluation items available at: https://admin.evaliuate.liu.se/search?lang=en

Suggestions on improvements from students:

- "Want more interactivity during lectures"
  - **Comment**: Interactivity is more challenging when lectures were given online. Hopefully some more interactivity this year,
- "The PONG lab was a lot of steps"
  - **Comment**: Possible to hand in each step separately for grading.
- "I wish it would be more about web security."
  - **Action:** Web security part will be updated this year to better reflect current trends. Roughly same scope and scale though.
- "I wanted more examples of when to use static analysis in practice"
  - **Comment**: This is something we are considering, e.g. as a lab, but must fit time-wise, which is a bit challenging.

Previous year's course evaluation

Suggestions on improvements from students (cont):

- "As always in this course, students have a really different level. Solutions has to be found on this"
  - **Comment**: Quite heterogenous intake to course – not much we can do about this
- "Want answers for old exams"
  - **Comment**: Old exams are provided to give an idea about exam structure and what topics to focus on when studying for the exam. My philosophy is that it's better to not provide answers to exams, as this prevents "overfitting" to answers, and fosters (forces) learning by true understanding. (I.e., by reaching internal consistency in your understanding of the topic.)

Previous year’s course evaluation

Positive remarks:

- Good that the examiner engages students during lectures by doing show of hands, asking questions, etc.
- The web lab was very fun and interesting!
- I liked that the slides had a lot of info, and that there were booth material online to read and additional reading available. Also, having recordings available afterwards was great for my learning and for repetition. I like the lab assistant doing a thorough job and giving us examples to demonstrate how things should/should not be done.
- The PONG lab was very instructive.
- The help during labs is really helpful, maybe a bit more time for this would be better.
- Good that labs gave practical experience.

Questions?