Course Wrap-up

TDDC90 – Software Security

Ulf Kargén

Department of Computer and Information Science (IDA)

Division for Database and Information Techniques (ADIT)

Course topics

- **Secure software development**
- **Vulnerabilities in C/C++ programs**
- **Web security**
- **Code reviews**
- **Static analysis**
- **Security testing**

The Exam

- 38 points total
- Grading: Pass (3): 19p – 4: 27p – 5: 32p
- No aids (except English dictionary in book format)
- Points per subjects will *roughly* correspond to the number of lectures given for the subject.
  - See previous years' exams to get an idea

What to expect on the exam?

Secure software development and **Code reviews**

- Methods:
  - Be able to describe methods and processes
  - Be able to apply modelling and analysis methods on small examples
- Design patterns:
  - Be able to describe design patterns in course literature and their *motivation* and reason about *where they are applicable*
    - Descriptions may require both UML-diagrams and Pseudo code

What to expect on the exam?

Vulnerabilities in C/C++ programs

- Vulnerabilities:
  - Be able to describe all vulnerability types mentioned in the lectures – What is the reason for the vulnerability and how to avoid it?
- Attacks:
  - Be able to describe the stack-buffer overflow exploit in detail
  - Conceptual understanding of the other exploit methods
- Mitigations
  - Conceptual understanding of the mitigation techniques described in the lecture – and attacks that circumvent them
  - Be able to reason about which attacks could be mitigated using a particular method

What to expect on the exam?

Vulnerabilities in C/C++ programs

- Exam questions:
  - Will generally emphasize understanding over knowledge of details.
  - Will typically require reading some code:
    - Spotting simple bugs in code examples, etc.

What to expect on the exam?

Web security

- Vulnerabilities:
  - Be able to describe all vulnerability types in the lecture – What is the reason for the vulnerability and how to avoid it.
- Attacks:
  - Be able to describe basic ideas behind attacks
- Exam questions:
  - Will be more conceptual than code-oriented, but you should be able to
    - Show simple (and syntactically correct) SQL-injection attack inputs
    - Write some pseudocode to explain different vulnerabilities and mitigations

What to expect on the exam?

Static analysis

- Important properties of methods
- You should be able to apply the techniques explained in the lectures on simple toy examples (see old exams to get a good idea of what to expect)

What to expect on the exam?

Security testing

- Understand challenges of security testing in general
- Conceptual understanding of methods
  - Penetration testing
  - Mutation based fuzzing
  - Generation based fuzzing
  - Concolic testing
  - Greybox fuzzing
- Compare strengths and weaknesses of said methods
- Explain whether a method is suitable for a given use case
- Questions will again focus on understanding rather than details

Final words

Remember:

- Hard hand-in deadline for labs 17th of December (23:59)
- Register for exam!
- Fill out course evaluation!

Where to go from here?

- TDDE62, TDDE63
- Master’s thesis opportunities