Course Wrap-up

TDDC90 – Software Security

Ulf Kargén

Department of Computer and Information Science (IDA)

Division for Database and Information Techniques (ADIT)

Course topics

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

The Exam

- 40 points total
- Grading:
  - Pass (3): 20p
  - 4: 29p
  - 5: 35p
- No aids (except English dictionary in book format)
- Points per subjects will *roughly* correspond to the number of lectures given for the subject.
  - The two lectures on C/C++ vulnerabilities and the part about secure software development are central to the course, and will be given higher weight.

What to expect on the exam?

Vulnerabilities in C/C++ programs

- 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 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 possibly 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

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
    - Descriptions may require both UML-diagrams and Pseudo code
- No questions on accreditation in this year's course

What to expect on the exam?

Static analysis

- Emphasize on conceptual understanding of the methods described in the lectures, rather than the mathematical formalisms.
- Important properties of methods
- Soundness and completeness

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
- Compare strengths and weaknesses of said methods
- Understand fundamental challenges of concolic testing
- Questions will again focus on understanding rather than details

Final words

Remember:

- Hard hand-in deadline for labs 17th of December
- Register for exam!
- Fill out course evaluation!

Where to go from here?

- TDDD17 – Information security, second course
- Master’s thesis opportunities at ADIT

Good luck on the exam!

The End