LiTH, Linköpings tekniska högskola
IDA, Institutionen för datavetenskap
Nahid Shahmehri

Written exam

TDDC90 Software Security

2008-12-20

Permissible aids

Dictionary (printed, NOT electronic)

Teacher on duty

Shanai Ardi, 013-282602, 0762-105806

Instructions

The exam is divided into two parts with a total of ten questions. You should answer all questions in all parts. In order to get the highest grade you will need sufficient points in the second part.

You may answer in Swedish or English.

Grading

Your grade will depend on the total points you score on the exam. The following grading scale is preliminary and might be adjusted during grading.

Grade	3	4	5
Points required	18	24	30

Important
In order to get the highest grade you must have scored at least six points in part 2.

Part one

Question 1: Exploits (2 points)

Explain how a simple stack-based buffer overflow can be exploited on a typical computer.

Question 2: Fuzz testing (2 points)

Explain what “fuzz testing” is.

Question 3: The Common Criteria (2 points)

Explain what a protection profile is and how it is used.

Question 4: Capability Models (2 points)

What are capability levels in SSE-CMM and what do they mean?

Question 5: Static analysis (4 points)

Explain, using an example, the concept of path sensitivity in static analysis. What are the consequences, typically, when a static analysis tool is not path sensitive?

Question 6: Exploits and vulnerabilities (4 points)

a) Explain what a return-to-libc attack is.
b) Explain why attackers prefer return-to-libc (or similar techniques) over more traditional methods of exploiting buffer overflows.
c) How can return-to-libc attacks be prevented?
d) Analyze or discuss the effectiveness of the prevention mechanism you proposed. Is it always effective? Can it be circumvented? How difficult is it to circumvent? Are there other issues of importance?

Question 7: Security processes (4 points)

What is the “security touchpoint process”? Briefly explain each part of it.

Question 8: Type qualifiers (4 points)

Type qualifiers, like the ones used by `cqual`, are effective at finding certain kinds of (potential) security problems. Explain how type qualifiers work, what kinds of problems they find, and what problems and/or limitations they have.

Part two

In order to score well on these questions you will need to show that you understand not only the technical issue or concept at hand, but also its context and its interactions with its context (e.g. processes, methods, techniques, technology, people, risks, threats, and so on). We *think* that good answers to these questions will require at least one or two handwritten pages (more or less may be required depending on how you write).

Question 9: Model-based methods (6 points)

Many proposed methods for software security use models in some way, such as misuse cases, attack trees, vulnerability cause graphs, formal specifications, etc. Discuss the strengths and weaknesses of model-based approaches, how they relate to other approaches to software security.

Question 10: (6 points)

Explain what threat modeling is and what its role in software security is. Show how threat modeling can be performed through an example.