CHALMERS UNIVERSITY OF TECHNOLOGY
Department of Computer Science and Engineering
Examination in Computer Security EDA263 (DIT641) for the International Master's Program in Computer Systems and Networks, Saturday 17 March 2018, 08:30—12:30

Examiner: Associate professor Magnus Almgren, Ph.031-772 1702,
email: magnus.almgren@chalmers.se

- Some questions are about knowing the material. For these, there is a reference to where the answer is discussed.
- Some questions are about being able to think and reason about the material. For these, there is a draft of the solution and what we are looking for in your answer.
- Some questions are supposed to be quite easy if you have taken the course: lab, previous exam, lots of time in lecture, partly memory-based. These will form the basis for getting a 3 ("pass") in the course.
- Other questions are supposed to be much more difficult and require a good understanding of the material, able to reason and draw new conclusions, or know the terminology well. These are to examine for higher grades, 4—5 ("pass with distiction").
- This copy is released as-is and may contain typos and other mistakes. Please ask if a certain answer seems wrong so it is updated.

1 Defences against attacks (20p)

a) Explain what a packet-based firewall is and what type of information it uses for its decision logic. Give an example rule and explain what it could do. (4p)

see page 311 and page 312 in the book.

b) Explain what the SQL injection attack is and give an example. (3p)

see page 386 and page 387. There is also a slide show on the attack, and a lab.

c) Explain what the TOCTOU attack is and give an example. (3p)

see slides on TOCTOU and Kerberos

d) Explain how efficient the packet-filtering firewall (positioned in A) can be in the following scenarios. Be concrete and use the answer for (a) to structure your answer. When applicable, explain what type of rule you would create for the firewall. (10p)

The answer should reflect understanding of security mechanisms and how they can be used to improve security. There is no single “right” answer, but we are looking for the reasoning in the answer.

-- Against SQL injection attacks on the DMZ.

In this case, there is a mismatch between the type of attack we would like to detect (b) and the information used (a). From (a), we can block hosts based on their IP address for example, but as any client need to access our web server in the DMZ (see hints), it is unlikely we can make an effective rule.

-- Against SQL injection attacks on the internal network.

See (d-1). The difference is that no system here should be reached by any outside host (see hints), and we are not worried about insiders (see question text). Thus, we can use the firewall to block all outside access to the web server and the database, and thus also block any sql injection attacks.

-- Against TOCTOU attacks on the internal network.
See (d-1).

(exam continued on the next page)

2 Defensive Programming (10p)

In the lectures, we used the program snippet shown in Listing 1 to discuss attacks and defences.

a) Explain what a buffer overflow is from a general perspective. (1p)

see lectures, videos, or book

b) Use the code shown in Listing 1 to demonstrate specifically how a buffer overflow would work. Your answer should include *a figure* of the stack when the program enters the echo function, *a description* of what the attacker would do, and *how* this affects the stack (as a second figure). (6p)

see slides about buffer overflow, as well as book page 345

c) We discussed three main system defences against buffer overflows. ***Choose one*** of these system defences and explain how it works. Then explain in detail using the specific code from Listing 1 how an attacker might still be able to perform her attack even if the stack is protected by this particular defence mechanism. Please be concrete and include a figure of the stack in your answer. (3p)

Mostly use lecture notes for canary, address space randomization, and no-execute bit; see book page 364-366. The attacks are also included in the slides.

3 Security and dependability concepts (4p)

a) In the course, we spoke about three main security objectives. Name them and briefly explain their meaning. (3p)

CIA, lecture 1 slides + page 33 (also repeated in other lectures)

b) Some in the security field feel that additional concepts are needed to present a complete picture. Name and explain one such additional concept. (1p)

For example, p34 and/or attributes from the Crypto lectures

(exam continued on the next page)

4 Authentication (20p)

a) Define what is meant by authentication. (1p)

b) Describe the four steps of an authentication procedure. (4p)

c) The information used for authentication can be of three (or potentially four) fundamentally different kinds. Describe and exemplify those. (3p)

d) What is two-factor authentication? (1p)

(a)—(d): See L2 and L3, book p95, 128-129.

e) UNIX passwords are … (9p)
- usually not stored in clear text. Explain what is stored and how security is improved.
- usually combined with a SALT. Explain the SALT and how security is improved.
- usually not stored in the file /etc/passwd. Why? What is the added security?

Discussed during L2/L3. See book page 96 and forward. Hash, SALT, and shadow password file.

f) What is a rainbow table and how is this relevant to your answer in (e)? (2p)

See page 100 or discussion L2/L3 on how to build UNIX password system

5 Miscellaneous questions (6p)

Give a short (i.e. less than ca. 10 lines) but exhaustive answer to each of the following questions: (The answer must include not only the function, usage, principle etc., but also the (security) context into which the object of the question would be applicable.)

a) Explain the *side-channel attack*. Give an example. (2p)

Slides/DL lecture 9 + lecture 5 when discussing Spectre

b) Explain briefly how *speculative execution* was used in the Spectre attack. What side-channel attack was used in this attack and how? (4p)

Slides lecture 5