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 18 March 2017, 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 Malware Defence (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. (4p)

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

c) Explain what the tracker attack is and give an example. (4p)

see page 179--180 and slides from the database lecture

d) Explain how well the packet-filtering firewall positioned in A can protect systems in the DMZ against the SQL injection attacks. Be concrete and explain what type of rule you would create (use the answer for (a) to structure your answer) and how well it would work (false positives, false negatives). (4p)

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. 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.

e) Explain how well the packet-filtering firewall positioned in A can protect systems in the internal network against SQL injection attacks. Be concrete and explain what type of rule you would create (use the answer for (a) to structure your answer) and how well it would work (false positives, false negatives). (4p)

See (d). 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.

2 Denial of Service Attacks (10p)

The book discusses two similar but different types of denial-of-service attacks: the SYN Spoofing attack and the TCP SYN Flood attack.

a) Explain the attacks separately and then discuss the difference between them and how that might influence whether an attacker would prefer to use one attack over the other. (5p)

see book page 248-, 252. One targets a structure in memory used to setup connections and the other one targets network bandwidth.

b) In both attacks, the attacker should spoof the source address.
Give at least two reasons why. (2p)

see book page 246—247: more difficult to block during the attack (esp. if you change continuously), attacker's system not getting all the traffic back, more difficult to track down afterwards for legal reasons

c) If the attacker had a choice, would she choose an existing or non-existing host for the source of the attack (the spoofed address)? Motivate your answer. (2p)
   a. The SYN Spoofing attack
   b. The TCP SYN Flood attack

see book page 247: real host = will add additional traffic with responses, error packets, etc. This is good for a flooding attack (b) as you get even more traffic (see section 7.5). For (a), it is important the host does not report back a RST packet as this will free up entries in the memory structure = should be a non-existant host or a host that cannot answer (also under DoS?).

d) In this context, what is backscatter traffic and what can it be used for? (1p)

see book page 248

3 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. Describe these briefly by stating what they do and why this makes it harder for the attacker to perform the attack. (3p)

Mostly use lecture notes for canary, address space randomization, and no-execute bit; see book page 364-366.

4 Security Models (10p)

a) What is the primary goal of the Chinese Wall Model? We are not looking for terms from the CIA, but a related concept. (1p)

Conflict of Interest, book page 457

b) Draw a figure, showing how this (general) model would look in the specific example for this law firm. Show in the picture the three levels information is organized into and explain them with a concrete example. (3p)

slides, example during lecture, or book Figure 13.6.

c) Define the simple security rule formally in the following way: (2p)
Simple Security Rule: A subject S can read object O only if ...

book page 457, or lecture on security models

d) Alice and Bob work for the law firm. State whether the following *read* accesses (performed in the order shown here) will be accepted or denied. Use your answer in (b+c) to explain your reasoning. Structure your answer in the following way:
Answer: x) Accepted/Denied, because … (2p)

1) Accepted Alice reads a document outlining which new offices will open in 2018 for Bank of Wales.
2) Denied Alice reads a document outlining which new offices will open in 2018 for Bank of England.
3) Accepted Alice reads a document outlining which new offices will open in 2018 for Air France.
4) Accepted Bob reads a document outlining which new offices will open in 2018 for American Airlines.
5) Denied Alice reads a document outlining which new offices will open in 2018 for Bank of England.
6) Accepted Bob reads a document outlining which new offices will open in 2018 for New York Times.
7) Accepted Alice reads a document outlining the yearly summary of earnings / losses for Air France.
8) Accepted Alice reads a document outlining the yearly summary of earnings / losses for Bank of Wales.
9) Accepted Bob reads a document outlining the yearly summary of earnings / losses for Bank of Wales.
10) Accepted Bob read a document outlining the yearly summary of earnings / losses for American Airlines.
11) Denied Bob reads a document outlining the yearly summary of earnings / losses for Air France.
12) Accepted Alice reads a document outlining which new offices will open in 2018 for Bank of Wales.

e) Reflect on your answer in (a), by considering the "new" accesses (7)—(11). (2p)

The model is about COI, but your answer in (d) is all about reading only. With (e), you also add writing and there could be a flow of information from Air France (Alice has access) to American Airlines (Bob has access) through the common Bank of Wales (Alice and Bob have access). The book speak about the *-property but also reflect that many times the user is doing an "analysis" and will not write directly to such documents.

5 Miscellanous Questions (10p)

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. What is meant by Security Target and Protection Profile?
Which is the difference? (2p)

book page 474—476, plus slides and other readings

b. There are three major methods for risk treatment. Please name, describe and exemplify these methods. (6p)

slides about risks

c. What is a salami attack? (2p)

off print #2