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, Wednesday 24 August 2016, 14:00—18:00

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

Teacher available during exam: Magnus Almgren, Ph.031-772 1702

Language: Answers and solutions must be given in English.

Grades: will be posted before Thursday 15 September 2016. The exam review date/place will then be posted on the homepage.

You are **not** allowed to use any means of aid.
However, according to general rules printed English language dictionaries are allowed.

Please write the answer to each question (question 1, question 2, etc) on a separate sheet of paper.

Grade: The grade is normally determined as follows:

30 p ≤ grade 3 < 38 p ≤ grade 4 < 46 p ≤ grade 5 (EDA263)

30 p ≤ pass < 46 p ≤ pass with distinction (DIT641)

1 UNIX Security

One of the simplest way of storing passwords on a system would be to use a list with the user names and the passwords in clear text, such as in the /etc/passwd file (with other info):

username	password	user identifier	(more fields)
olle	mydogiscalledFelix!	100	...
helen	s5%d#gqqj	101	...

Any system administrator concerned with security would not use such an implementation. Explain how passwords are actually stored in UNIX systems. For each feature that adds a layer of security, explain why it is there and how it increases the protection of the passwords. *Include an image* where the features you described are highlighted.

(10 p)

Lab 1, slides L2 slides on passwords, book p95--104
shadow file = only root can access
one way encryption (hash) = not in clear text in file (cannot reverse), can also be SLOW to stop attacker from trying many.
salt value = prevents duplicate passwords to look the same, makes offline attack more difficult, cannot determine if same person on different systems
figure to demonstrate points
extra: enforcing a length, or checking password against dictionary before used to avoid very simple passwords.

2 Risk Treatment

After having carried out a risk analysis the analyst team needs to take appropriate action.

a) There are three major methods to deal with the result of the risk analysis. Please name, describe and exemplify these methods.
b) Further, the book discusses two other methods for risk treatment that are more of a preventive type. Please name, describe and exemplify these two methods as well.

(10 p)

See slides L13, slide 21 or book 2nd - 528-529, 3rd - 526-527

3 Ethics

There are two theories of ethics called the teleological theory and deontology. These may either work on an individual level or on a universal level.

a) Explain how the teleological theory works, both used on the individual level or on a more universal level.
b) Explain how deontology works, both used on the individual level or on a more universal level.

Let's look at the vulnerability reporting process. You have discovered a severe flaw in a system that controls all hydro plants in Sweden. You realize that an attacker may use this flaw to stop the production of electricity.

c) Who would you tell / not tell about the flaw? How much detail would you tell to each party? Use arguments from the teleological theory to support your reasoning. That is, we are going to grade how you applied the theory to support your answer but not the answer itself. You will need to discuss disclosure to at least three parties to get full points. (6 p)

See offprint for theories and example cases

4 Security Metrication: Common Vulnerability Scoring System (CVSS)

Describe the main principles for the CVSS system. How is security metricated with CVSS. Which input data is used for the procedure. Which are the results delivered?

(4 p)

See slides L12

5 Malware

a) Give a short (i.e. less than ca. 5 lines) but exhaustive description to each of the following types of archetypal malware / attack vectors. For each instance, try to give an example and make a comparison between different types where appropriate.
Example answer: The properties for Malware X are the following:… In that sense, it is different from Malware Y described in (i). An example of malware X could do …

i. virus
ii. polymorphic virus
iii. macro virus
iv. Trojan Horse
v. logic bomb
vi. backdoor
vii. worm
viii. zero-day exploit
ix. keyloggers
x. rootkit
xi. spear-phishing
xii. drive-by-download

(12 p)

b) Ransomware attacks has lately increased. Describe how it works, and how you can protect yourself.

See slides L6, p11, p16, p21, p22, p26, Book: p202, p216

(2 p)

6 Miscellanous Questions

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.)

i. Explain the *side-channel attack*. Give an example.
ii. What is meant by Security Target and Protection Profile? Which is the difference?
iii. The Morris worm used three types of attacks. Explain two of them.
iv. There are two fundamentally different ways of causing a denial of service attack. Describe them and give an example for each type.
v. What is meant by computer forensics?
vi. Explain what two-factor authentication is.
vii. Should passwords be hashed? Why/why not?
viii. Briefly describe the difference between DAC and MAC related to authentication.

(16 p)

a) see L16 and slides
b) see L11 and slides
c) see L7, slide 5 (with details in the following)
d) See L11 and slide 9
e) see L15, slide 3
f) L2, slides + blackboard (see slide 4 mobile malware)
g) L2 discussion of passwords, book p96-99
h) book p130