CHALMERS UNIVERSITY OF TECHNOLOGY
Department of Computer Engineering

Tentamensskrivning i Tillämpad datasäkerhet EDA261 för D4 och LEU 321 för Di3, ChL
Tisdagen den 22 april 2003, kl 08.45 - 12.45
Examination in Applied Computer Security IMP 261 for the International Master’s Program in Dependable Computing Systems, Tuesday 22. April 2003, 08.45 - 12.45

Examiner: Professor Erland Jonsson, tel. 772 1698, email: erland.jonsson@ce.chalmers.se

Solutions: No solutions will be posted.

Language: The examination is written in English. Answers and solution may be given in English or Swedish.

Grades will at the latest be posted before Tuesday 6 May 2003, at 10.00 a.m. on the Department's notice board and the course's homepage.

Please contact the examiner if you want to review the coorection of the exam.

You are **not** allowed to use any means of aid.

Grade: The grade is normally determined as follows:

$24p \leq$ grade $3 < 36$ p $\leq$ grade $4 < 48$ p $\leq$ grade 5

1. Security mechanisms

There are many available security principles, methods and mechanism that work in different ways and with different focuses. Describe the following five "mechanisms" from a security point of view, e. g. how and to which extent they improve security:

- a digital signature
- an encryption mechanism
- an intrusion detection system
- a tiger team
- legislation against hackers and other attackers

In particualar should the relevant security aspect be mentioned. Further, must the relation of the "mechanism" with respect to the fundamental protection principles that have been mentioned in the course be addressed. (10p)

2. Passwords

a) What is a password from a security point of view? Explain.
b) The use of passwords present a number of vulnerabilities to the potential attacker, i.e. ways to get illegal access to the system. List and discuss at least four different methods to do this and discuss the reason why it is possible.
c) What is a one-way password? Explain and give examples!
d) In many cases is a one-time password more secure than an ordinary password. Explain how and why! Discuss the difference between "normal" passwords and one-time passwords for the intrusion methods you gave in b). (12p)

3. Intrusion detection

Intrusion detection systems (IDS) may be sub-divided into host-based or network-based systems. Another, orthogonal, way of sub-dividing IDS systems is into signature-based and anomaly-based systems. Describe and explain these four categories, pros and cons (fördelar och nackdelar) and performance issues. (8p)

4. Denial-of-service attacks

a) Describe a Denial-of-Service attack (DoS attack)! Clarify how it works, its security implications and the goal of the attacker.

Describe the in some detail the principles and functionality of the following DoS attacks:
b) SYN flooding
c) Ping-of-death
d) Mail bombing

e) A distributed DoS attack (DDoS attack) is a special type of DoS attack. What is specific about it? How does it work?
f) There are at least two different principles for how these attacks attain their goal on the victim system. List and explain these two principles. (10p)

5. Some security methods

Define and explain in some detail the concepts below. Discuss how they function and their relation to security:
a) covert channel
b) steganography
c) cryptography

Finally, discuss how they relate to each other, similarities and differences. (8p)

6. Key Escrow

Describe “key escrow”! Principles, functionality and objectives (syfte) of it. (5p)

7. Miscellaneous questions

Explain the following terms:

a) Demilitarized zone (DMZ)
b) query analysis
c) principle of least privilege
d) Virtual Private Network (VPN)
e) race condition
f) information flow model
g) reference monitor (7p)