CHALMERS UNIVERSITY OF TECHNOLOGY
Department of Computer Engineering

Tentamensskrivning i Tillämpad datasäkerhet EDA261 för D4 (även LEU 321 för ChL och INN 641 för GU) Lördagen den 13 december 2003, kl 08.45 - 12.45
Examination in Applied Computer Security EDA261 for the International Master's Program in Dependable Computing Systems Saturday 13 December 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: Answers and solutions may be given in English or Swedish.

Grades will at the latest be posted before January 9th, 2004 at 10.00 a.m. on the Department's notice board and on the course's homepage.

A review of the exam may take place January 12th, 2004 between 11.00 - 12.00 am.

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

Grade: The grade is normally determined as follows:

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

1. A fundamental system model of security

The course has suggested a fundamental model of computer security and dependability for a system. The model describes the security/dependability concepts and the system's interaction with its environment from various viewpoints. Draw a figure that describes the model, and give an explanation of it. (8p)

2. Covert channels

There are several types of covert channels. Please name these and explain how they work? Give examples. Include a general description of what is meant by a covert channel. The course has also covered some other application areas that are closely related to covert channels, or even could be said to represent variants of them. Name and describe those areas. (8p)

3. Intrusion detection

The function of an intrusion detection system (IDS) can be described by the false alarm rate. Define what is meant by this term. There are (at least) two other terms that describe the basic function of an IDS. Name and give a definition of these.
There is a fundamental reason why the false alarm rate is one of the biggest problem for IDS's, a reason that is generally applicable to many types of systems that have certain characteristics, and not only to IDS's. Describe this problem in some detail and explain why it is applicable to IDS's. Give a numeric example. (8p)

4. Databases

A problem with updating databases arises when the system goes down during an update.

a) Explain why this is a problem! Couldn't you just start from the beginning and redo the update? (1p)

b) There exists one specific method that ensures a correct update even if it is interrupted. Name and describe this method in detail. (4p)

5. Key Escrow Systems (Nyckeldepositionssystem)

a) What is meant by a key escrow system? (1p)
b) Why would you want such a system? What are the advantages? (1p)
c) State three important objections against a global infrastructure for key escrow. Explain and give examples! (3 p)

6. Miscellaneous questions

Give a short (i.e. less than ca 5 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 subject of the question would be applicable.)

a) What is meant by a capability?
b) What is a time stamp?
c) What is the goal and basic principle of the Chinese Wall security policy?
d) What is query analysis? What is the reason for applying it?
e) Why would you apply a call-back procedure?

f) Describe three methods to achieve unauthorized access to a password.
g) Why are modern “viruses”, such as Code Red and Sobig.F so successful?
h) Give three basic differences between a symmetric and an asymmetric crypto system.
i) What is a security plan?
j) What is meant by Security Target and Protection Profile? (10p)

7. Enterprise security

Congratulations! You have just been employed as security officer of a medium sized company, which means that you are the top responsible for the (computer) security of the company. The company is designing and delivering IT-based products. A smaller part of the production is top secret products to the Swedish military. Unfortunately, you do not know very much at all about the company in general, nor of its security status, but you have reason to suspect that security has been neglected. What are the first things you would do? How would approach your task?
NOTE! Give your answer in the form of a bulleted list. Your answer must not cover more than one page of normal-sized text! (8p)

8. Firewall configuration

The placement of rules in a firewall configuration script is significant. On the next page is a configuration script for a firewall, but we have removed some entries to make the script a bit more readable.

a) As telnet sends passwords in the clear and users unfortunately "reuse" passwords across systems, you want to make sure that no user on your computer leaks his or her password through telnet. You have decided to add a new rule to the firewall configuration script, which blocks all outgoing telnet connections from your computer. The rule you want to add is:

```
$IPTABLES -A OUTPUT -o eth0 -p tcp --dport 23 -j DROP
```

That is, all outgoing connections to port 23 (where the telnet daemon listens) are dropped.
In the configuration script below, we have marked six different possible places where you can insert the new rule. Please go through them all, and explain whether that place is a good or bad place for this kind of rule. We expect one sentence per placement, of the form:
Placement 1: This is a good/bad place because ...
Placement 2: This is a good/bad place because ...

b) Logging is very important, and you decide that you want to log all packets you drop with the rule above. Please explain whether you need to add more log rules than the three already present. If you need a new log rule, please include it in your answer. (8p)

```
#!/bin/bash -
IPTABLES=”/sbin/iptables”

### *** Placement 1 ***

# Default flushing and accepting packet of the NAT-module
$IPTABLES -t nat -F
$IPTABLES -t nat -P PREROUTING ACCEPT
$IPTABLES -t nat -P OUTPUT ACCEPT
$IPTABLES -t nat -P POSTROUTING ACCEPT

### *** Placement 2 ***

$IPTABLES -F INPUT
$IPTABLES -F OUTPUT
$IPTABLES -F FORWARD
$IPTABLES -P INPUT DROP
$IPTABLES -P OUTPUT DROP
$IPTABLES -P FORWARD DROP

# Kill malformed packets, i.e. tcp packets that are invalid
# Block XMAS packets
$IPTABLES -A INPUT -p tcp --tcp-flags ALL ALL -j DROP
$IPTABLES -A FORWARD -p tcp --tcp-flags ALL ALL -j DROP

### *** Placement 3 ***

$IPTABLES -A INPUT -i lo -j ACCEPT
$IPTABLES -A OUTPUT -o lo -j ACCEPT

$IPTABLES -A INPUT -i eth0 -s 10.0.0.0/8 -j DROP
$IPTABLES -A INPUT -i eth0 -s 172.16.0.0/12 -j DROP
$IPTABLES -A INPUT -i eth0 -s 169.254.0.0/16 -j DROP

### *** Placement 4 ***

$IPTABLES -A OUTPUT -o eth0 -j ACCEPT

# Allow SSH and HTTP
$IPTABLES -A INPUT -i eth0 -p tcp --dport 22 -j ACCEPT
$IPTABLES -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT

# Accept all related or established connections
$IPTABLES -A INPUT -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

### *** Placement 5 ***

# Log packets
$IPTABLES -A INPUT -j LOG
$IPTABLES -A OUTPUT -j LOG
$IPTABLES -A FORWARD -j LOG

### *** Placement 6 ***

echo “Done!”
```