KTH Datavetenskap
och kommunikation

DD2395 Computer Security
Exam 2010-12-14, 09.00 –12.00

This is a closed-book exam, no material (books, articles, laptops, phones, or any other electronic devices, etc.) permitted. Please answer in English if you can, only answer in Swedish if you must. Grading is according to the following preliminary point allocations. E 16–18p, D 19–21p, C 22–24p, B 25–27p, A 28–30p. Good luck!

1 Software security. [3 points]

1a What can we do to avoid buffer overflow attacks? Give 2 example strategies.

1b How could an attacker exploit the following program?

```
int login() {
char username[8];
char hashed_pw[8];
char password[8];
printf("login:"); gets(username);
lookup(username, hashed_pw); /* Put stored hash in hashed_pw */
printf("password:"); gets(password);
if (equal(hashed_pw, hash(password))) return OK;
else return INVALID_LOGIN;
}
```

2 Malware. [3 points]

2a Describe two different techniques that prevent viruses from being detected by an anti-virus software (even an up-to-date one).

2b What are backdoors and how do they differ from trojan horses?

3 Authentication. [4 points]

Usual authentication systems verify passwords with the help of their hashes stored in protected files.

3a What is the purpose of storing password hashes rather than the passwords themselves?

3b Why should we protect the access to the password hashes?

3c What is the purpose of salts?

3d Give an example each for authentication by something you know, something you have, something you are, something you do.

4 GPG E-Mail. [3 points]

Alice, who often uses her company's secure mail server, has just lost her private key but still has the corresponding public key. Answer the following questions both with yes/no and by giving a reason for each.

4a Is she still able to send encrypted mails? What about receiving?

4b Is she still able to sign the mails she sends? What about verifying the signatures of mails she receives?

4c What must she do to again be able to carry out all the operations mentioned above?

5 Web Attacks. [3 points]

5a How does cross-site scripting work?

5b What is the difference to cross-site request forgery?

5c How can we prevent SQL injection?

6 Intrusion Detection. [3 points]

An administrator installs an IDS that generates an alarm each time it detects an intrusion.

6a Mention a typical attack that can be detected by an IDS.

6b Mention a threat to which we expose ourselves by using such a system.

6c Name two ways of determining whether an action is classified as an intrusion.

7 Principles, Firewalls. [3 points]

For the following security design principles, explain what they mean and give an example of their application when setting up firewalls.

7a The principle of secure/fail-safe defaults.

7b The principle of complete mediation.

8 CIA. [3 points]
Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.

8a Eve installs firesheep and hijacks Alice's Facebook session. She reads Bob's messages to Alice and sends a response.

8b Julia hacks the website of www.visa.com and adds a message in support of wikileaks.

8c Claire installs a sniffer and captures her office mate's traffic.

8d Alex posts a message on 4chan, a popular online forum, asking people to visit the slashdot.org website at 2pm tomorrow.

8e Nick pretends to be a system administrator and calls Ellen from human resources at his company, to ask for her password. He then logs in as Ellen and increases his salary by 20 percent.

8f Ann mounts a man-in-the-middle attack by ARP spoofing and redirects all traffic at her student house through her own computer.

9 Multi-Level Security. [1 point]
What is the purpose of the no-write-down policy in the Bell La-Padula model?

10 Diffie-Hellman Key Exchange. [2 points]

10a Given Bob's public key Y_B, generated using the prime number q and α, a primitive root of q (same q and α as Alice used for her keys Y_A and X_A), how can Alice generate the secret key she shares with Bob?

10b What would Darth need to do to be able to read the messages between Alice and Bob?

11 Social Engineering. [2points]

11a What is meant by the term "social engineering"?

11b Describe one example of social engineering and what could be done to prevent it from succeeding.