KTH Datavetenskap
och kommunikation

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

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.

**Sample Solution:**

Any two of the following (plus insert explanations of what they mean):

Bounds checking

Don't allow execution of code on the stack

Canary/cookie

Appropriate library functions, programming languages

**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;
}
```

**Sample Solution:**

With a buffer overflow attack. The input length is not checked, one can insert an 8 char password twice (concatenated) and thereby overwrite the hashed password. This way the return will be OK.

Helpful: draw the stack

## 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).

**Sample Solution:**

Two of the following, always with an explanation of what they mean:

polymorphism

metamorphism

compression

encryption

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

**Sample Solution:**

Backdoors are left by developers (e.g. for debugging) or attackers to enable them to get unauthorized access to objects, bypassing authentication and access control.

Trojan horses disguise themselves as legitimate programs but contain malware, can be used to install backdoors.

## 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?

**Sample Solution:**

Clear text passwords could be used immediately by attackers that get unauthorized access to the file or even administrators that do have access; hashes need a deliberate effort and resources to find passwords that match them.

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

**Sample Solution:**

Given hash values to compare to, attackers can launch dictionary attacks (hashing all words in a dictionary), use rainbow tables (precomputed hases) or brute-force attacks offline. Once they find a match, they can log in.

**3c** What is the purpose of salts?

**Sample Solution:**

To (by increasing randomness by adding random strings/numbers to passwords when hashing) achieve the following: avoid dictionary attacks, make rainbow-table and brute-force attacks harder by needing an additional table for each salt value, and to result in different hashes even if users have chosen the same password.

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

**Sample Solution:**

know: password, pin code, answers to personal questions.

have: key, token, RFID card.

are: static biometrics: fingerprint, retina, iris.

do: dynamic biometrics: typing pattern, handwriting dynamics, gait.

## 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?

**Sample Solution:**

Yes, she can send encrypted mails, she needs only the public key of the receiver. The receiver cannot be sure that it was Alice who sent the message, though.

No, she cannot meaningfully receive mails since she cannot decrypt them without her private key.

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

**Sample Solution:**

No, she cannot sign her mails, as she needs her private key to do that.

Yes, she can verify others' signatures by using their public key, unless the signature is encrypted.

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

**Sample Solution:**

She needs to generate a new key pair, revoke her old key, get the new public key signed (preferably by a CA) and publish it.

## 5 Web Attacks. [3 points]

**5a** How does cross-site scripting work?

**Sample Solution:**

An attacker places malicious code on a web site (e.g. a forum) a user trusts. The code (script) is executed in the user's browser as if it came from the trusted web site (cross-site).

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

**Sample Solution:**

XSS exploits the trust of the user in a web site. The attack is executed in the user's browser. XSRF exploits the trust of a web site in its authenticated users. The attacker gets the victim to send a (forged) request on the attacker's behalf while the victim has an open session with the web site. This is done by having the user issue a request coming from the attacker's site (cross-site) that is executed at the web site the user is logged into.

**5c** How can we prevent SQL injection?

**Sample Solution:**

With an explanation of what you mean: input validation, prepared queries, escaping characters.

## 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.

**Sample Solution:**

Unauthorized access attempts (or any other of a long list of intrusions).

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

**Sample Solution:**

DoS the IDS itself by raising overwhelmingly many alarms.

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

**Sample Solution:**

anomaly detection: define normal user behavior, e.g. based on statistics, and see if the observed behavior deviates from it.

signature detection: see if an action matches the behavior of a known attack.

## 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.

**Sample Solution:**

The default, i.e., when no other specific rule exists, should be at the highest security level. Firewall example: use a white-list approach and by default deny all that are not specifically allowed.

**7b** The principle of complete mediation.

**Sample Solution:**

All requests for a resource must be checked. Firewall example: All traffic into the internal network and to the outside must go through the firewall.

## 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.

**Sample Solution:**

C by reading messages intended for Alice

I by sending messages to Bob

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

**Sample Solution:**

I by changing the website.

C if she reads anything on the server that is not public.

A if she disturbs the regular functioning.

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

**Sample Solution:**

C for unencrypted traffic, and even for encrypted traffic by looking at the packet headers (traffic analysis).

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

**Sample Solution:**

Intended A, might not succeed, by attempting to overwhelm the site with requests.

**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.

**Sample Solution:**

C for access to the salary data.

I for changing the salary.

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

**Sample Solution:**

C if she reads traffic.

I if she modifies it (and already by spoofing).

A if she drops packets or traffic is slowed due to her computer's performance limitations.

**9 Multi-Level Security. [1 point]**

What is the purpose of the no-write-down policy in the Bell La-Padula model?

**Sample Solution:**

Confidentiality: To avoid intentional or unintentional (malware-induced) leaks of information classified at a higher level down to a lower level by reducing the security level of the information.

**10 Diffie-Hellman Key Exchange. [2 points]**

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

**Sample Solution:**

$Y_B^{X_A}$,

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

**Sample Solution:**

He would need to mount a man-in-the-middle attack, generating a separate X and Y for Alice and Bob, and thus generate a separate secret key shared with Alice and another shared with Bob. He would need to know (by interception) $q$ and $\alpha$.

In theory, he could solve the discrete logarithm, but in practice he would not be able to do so.

**11 Social Engineering. [2points]**

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

**Sample Solution:**

Instead of using technical means, an attacker exploits human behavior to get unauthorized access or information to mount attacks.

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

**Sample Solution:**

For example the scenario in Question 8e. Prevention: user education, policies, rules to not give out passwords to anyone, etc.