KTH Datavetenskap
och kommunikation

DD2395 Computer Security
Exam 2012-01-10, 10.00 –13.00

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 16–19p, D 20–22p, C 23–25p, B 26–28p, A 29–31p. Good luck!

1 CIA. [3 points]

1a Explain the components of the CIA model: Confidentiality, Integrity, Availability.

Sample Solution:

- Confidentiality: Information (data) is not be made accesible (readable) to those without authorization. A loss of confidentiality would be unauthorized access to information.
- Integrity: Information (data) is not modifiable (changeable) without the right authorization. A system is safe from unauthorized manipulation which might alter its normal performance and functionality. A loss of integrity would be unauthorized modification (or deletion) of information.
- Availability: Services or resources can be accessed by authorized users or subjects in an unaltered way. A loss of availability would be the denial (or usage disruption) of service.

1b Which of these can message authentication codes provide? How does that work?

Sample Solution:

Message authentication provides integrity. One of the techniques are generating the message authentication by feeding some secure algorithm with the message (and using a secret key only known by the sender and the receiver) and appending this key (piece of data) to the message that is to be sent. Once the receiver gets the message it will feed the same algorithm with the message and the secret key, and compare the message authentication code obtained with the one attached to the message; if these match then the message has not been altered (but confidentiality is not guaranteed as the message does not undergo any transformation more than attaching the MAC).

2 Cryptography. [1 point]
There is an assumption underlying the following algorithms that - given large enough numbers for the parameters - it is difficult for an attacker to do the computation necessary to break them. What is the computation an attacker needs to do that makes it hard to break

2a RSA public-key encryption?

Sample Solution:

Factorization of large numbers.

2b Diffie-Hellman key exchange?

Sample Solution:

Computation of the discrete logarithm.

Note that writing down the mathematical formulas (and/or the steps required to achieve these computations) is not enough to answer this question. You must have shown that you understood what these computations are, what they mean basically.

3 Web attacks. [2 points]
Pick 2 items from the following list and explain briefly what they are and what an attacker can do:

- Broken Authentication and Session Management
- Insecure Direct Object References
- Cross-Site Request Forgery (CSRF)
- Security Misconfiguration
- Insecure Cryptographic Storage
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Unvalidated Redirects and Forwards

Sample Solution:
See the slides of OWASP lecture
Note that just listing examples from the slides is not enough, you need to explain and thus show understanding.

4 Denial-of-service. [3 points]

4a What is a denial-of-service attack?

Sample Solution:

Action aimed at disabling an information system (or a network) from providing its intended services, for instance, serving a webpage or authenticating users, by exhausting the resources allocated for these services (it is usually carried out by flooding the service of the system with multiple requests).

4b Explain reflection and amplification.

Sample Solution:

Reflection: An attack where the attacker sends a network packet to a known intermediary service using a spoofed source address which corresponds to the address of the target system. The response from the intermediary will be directed to the target system instead of the attacker as the source address of the network packet was manipulated.

Amplification: A variant of the reflection attack where besides spoofing the source address the amount of response packets is multiplied for each network packet sent. This can be achieved by directing the original network packet to the broadcast address of some network for instance, or using a DNS server as intermediary (by taking advantage, and exploiting, the functionality of DNS protocol)

Note that your explanation needs to make clear how they work.

5 Security principles. [1 point]

5a What is the principle of complete mediation?

Sample Solution:

Every access to every object must be checked for authority. This principle, when systematically applied, is the primary underpinning of the protection system. It forces a system-wide view of access control, which in addition to normal operation includes initialization, recovery, shutdown, and maintenance. It implies that a foolproof method of identifying the source of every request must be devised. It also requires that proposals to gain performance by remembering the result of an authority check be examined skeptically. If a change in authority occurs, such remembered results must be systematically updated.

Note that this definition is extracted from ’The Protection of Information in Computer Systems’ by Saltzer and Schroeder (1975), pp. 9. There is no need to answer this precisely, but the basics need to be there.

5b Why is it important?

Sample Solution:

When access is not checked, any security measures can be circumvented. All access needs to be authorized. This also means that even if a subjet has already accessed an object, the access rights need to be checked again the next time the same subject requests access to the object, as the rights can have changed in the meantime.

6 Access Control [2 points]

6a What is the main difference between discretionary and mandatory access control?

Sample Solution:

Mandatory Access Control is based on both the the security level of the object and security clearance the requestor (subject), while Discretionary Access Control is based on the identity of the requestor (and the access rules stated for the object). In MAC, an entity that has clearance to access a resource may not be able to allow another entity to access the same resource, while in DAC this is plausible and possible.

6b List and explain 2 advantages of role-based access control.

Sample Solution:

Management of permissions becomes easier as there is no need to go user by user when these change; for instance, the update of the permissions for a particular role will automatically apply to all users with that role.

Management of access rights becomes easier at an organizational level as roles can be administrated in groups; for instance, adding or deleting a new user does not require more than setting up its groups (roles).

The examples you choose need to reflect understanding of how role-based access control works.

7 Multi-Level Security [2 points]

KTH wants to adopt a multi-level mandatory access control system to make sure upcoming exams are kept confidential.

7a Which system would you choose for this purpose and why? Bell La Padula, Clark Wilson, or Chinese Wall?

Sample Solution:

Bell La Padula. This model focuses on confidentiality. The entities are divided into subjects and objects, that have some assigned security level. To achieve a better granularity, each security level can contain some set of categories. The model utilizes two mandatory access control rules (no read up, no write down) and one discretionary access control rule (granting access).

The Clark-Wilson model controls integrity of data and transactions, and not confidentiality. Therefore, it is not suitable.

Chinese Wall model tries to resolve conflict of interests. All objects are divided between conflict of interest classes, that are further divided into datasets. If you have access to one dataset, access to other datasets of the same class is forbidden. However, a subject can access objects from other classes, from which he does not have any information yet. A subject can write to a dataset if all objects that he has access to are only in this dataset. So, the main rule is that a subject can only access information that does not conflict with the information already possessed by the subject. Since access pattern is different for different subjects, the shape of the wall also differs between subjects. Chinese Wall cannot be used for university, because access control rules change with user behavior. It means that students might get access to information they are not supposed to.

7b What difficulties can you foresee if such a system were adopted?

Sample Solution:

Even if a teacher has two roles (teacher and student), manual administration (e.g. downgrading rights) will still be required in many situations. Exams have different confidentiality requirements over time, first only teachers should be able to read them, then students should read them as well and then teachers should be able to read the students' answers and then students should also be able to see the teachers' corrections. These changes cannot be done within the system but need intervention by an administrator.

8 Software security. [3 points]

8a What does an attacker need to do to exploit a stack overflow vulnerability to make a program crash? What if the attacker wants to run their own code first?

Sample Solution:

The attacker must first identify somehow (e.g. tracing, fuzzing tools) the buffer overflow vulnerability in a program.

The idea is to input more data to the buffer than it is supposed to handle. By overwriting the return address in the stack frame, one can get a segmentation fault or an illegal instruction error. This happens when function returns and tries to execute instructions at the location pointed by return address. There is a very high chance that the overwritten return address would not point to a valid address inside the process address space or the instruction would be valid if the attacker used some random input, and the program would crash.

To run arbitrary code attacker should put executable code in the buffer that is being overflowed and overwrite the return pointer to point to the buffer. The attacker has to guess the address of the buffer to succeed. The attacker can add NOP instructions at the beginning of the buffer, then add the executable code, and then overwritten return address. This greatly increases the chances of guessing the address, because even if the pointer does not point precisely to the beginning of the injected code but points instead to one of the NOP instructions, then NOP instructions will be executed and eventually the injected code will be executed after them.

8b For performance reasons, you'll have to use C for a program. As the programmer, what can you do to prevent buffer overflow attacks? Explain 2 techniques.

Sample Solution:

Safe libraries that check bounds and do other buffer management.

Random canaries: values (not known to the attacker) that are put in the buffer and if they are changed, it means there was a buffer overflow.

8c How can you avoid race conditions?

Sample Solution:

By using synchronization primitives like locks (e.g. mutex, semaphore) that give access to a resource to one thread at a time; by using simple atomic operations. For example, do not first test whether you can write to a file and then write to it in a separate instance. Just write. If you cannot, deal with that in the program.

9 Malware. [3 points]

9a Viruses and worms go through different phases over their life-time; list and explain at least 3 of them.

Sample Solution:

Dormant: idle waiting for some event

Propagation: searches for other systems, connects, copies

Triggering: being activated

Execution: the harmful action is performed

9b What can botnets be used for? List and explain two uses for an attacker.

Sample Solution:

Distributed Denial-of-service attacks - bots are used to generate enormous amount of traffic (flooding the target with messages)

Spamming - send massive amounts of spam

Click fraud (attack on pay-per-click online advertising by making multiple clicks from bots)

Parallel and distributed computing (computational power of the whole botnet used, for example, to break encryption or hashing)

10 Authentication. [3 points]

10a List and explain 3 ways of attacking password-based authentication.

Sample Solution:

The answer should contain 3 ways described in the course book pages 77-78. Minor variations of password guessing cannot be considered as separate ways.

10b What are appropriate countermeasures for these? **Sample Solution:**

also on the pages listed.

11 Firewalls. [1 point]

11a What is the purpose of a demilitarized zone (DMZ)?

Sample Solution:

A demilitarized zone (DMZ) is a network segment between the Internet and the organization's private network. Both internal and external users can access resources in the DMZ. Resources that need to be available for external users (e.g. web server) are put in the DMZ because then they are not directly exposed to the Internet, hence protected. At the same time, these resources are not put in the internal network, because a compromised server in the internal network would pose a great risk for the security of the whole system.

The DMZ is separated from the Internet and from the internal network by firewall(s). The location of firewall(s) defines the DMZ topology. For example, a low-cost solution would be a single firewall with 3 interfaces, so that the DMZ, the internal network and the Internet would be separated from each other.

11b What does one typically put into a DMZ?

Sample Solution:

Resources that need to be available for external users (e.g. Web server, Mail server, DNS server).

12 Intrusion Detection. [2 points]

12a What are advantages and disadvantages of signature-based detection versus anomaly detection?

Sample Solution:

Signature-based detection is based on a database of known attack signatures. Thus, new attacks that are not in the database will not be caught (false negatives).

Anomaly detection is based on behavioral patterns. This detection requires a learning period. Decisions on whether some action is malicious or not is based on statistical analysis and threshold settings. Anomaly detection can detect new, previously unknown attacks, but it is also prone to false-positives (legitimate action regarded as malicious).

12b Where would you place a honeypot? Explain why.

Sample Solution:

A honeypot is a decoy system (designed to look as an attractive target); it has no production value. Its purpose is to divert the attacker's attention from real resources, keep the attacker concentrated on it, and collecting information about malicious activity.

Honeypots can be located almost everywhere. They can be placed outside the external perimeter, in the DMZ, in the internal network. All this placements have their pros. and cons. For example, a honeypot located inside of the internal network can catch internal attacks, but if it gets compromised, it becomes a platform for attacking other internal systems.

13 Consulting. [2 points]

How would you respond to the following statements? Come up with an argument for why this is or is not a good idea.

13a I prefer to log in as administrator or root, this way I don't have to type in my password so often.

Sample Solution:

Bad idea. You can make mistakes, others can get root access if you leave your session unattended, get malware, and all these actions can result in more damage to the entire system than if you kept to your regular user account. Violates the principle of least privilege.

13b I just implemented my own version of AES and made some changes and optimizations. Now it runs much faster!

Sample Solution:

Bad idea. Your code was not reviewed by experts and the community at large, you probably made the implementation less secure. Do not implement your own crypto solutions unless they go through an extensive review process. Violates the principle of open design.

13c As a system administrator, I make the default settings very secure for the users. If need be, they can be changed later.

Sample Solution:

Good idea. Users often do not change their default settings, so it's better to start by erring on the more rather than less restrictive side. This way, users or malware can do less damage. This relates to both the principle of fail-safe or secure defaults and to the principle of least privilege.

13d When programming, I make sure to check user input against all the ways I can think of that it can go wrong. If I find a match, I raise an exception.

Sample Solution:

Bad idea. While it's good to check input, it is better to compare to the valid input (whitelist) as opposed to comparing to what can go wrong (blacklist), as you might not catch everything.

14 Social Engineering. [3points]

14a What is meant by the term "social engineering"?

Sample Solution:

Exploiting human behavior as opposed to technology to gain unauthorized access to information or other resources to attack a system. (Note: do not confuse with phishing or restrict only to passwords or to just gain information.)

14b List and describe 3 human tendencies of behavior that are commonly exploited by social engineers.

Sample Solution:

trust in people (and thus be more gullible and give out information to unauthorized people or perform unauthorized actions for them), the desire to help, desire to avoid confrontation (reluctance to say no to requests or to stop someone from doing something),

14c What countermeasures would you take to prevent such exploitations?

Sample Solution:

Develop clear security policies, for general rules as well as for correct behavior for specific scenarios and educate the users both about the policies and about social engineering tactics.