CHALMERS
EXAMINATION / TENTAMEN

Course code/ kurskod	Course name / kursnamn			
EDA263	Computer Security			
Anonymous code Anonym kod		Examination date Tentamensdatum	Number of pages Antal blad	Grade Betyg
EDA263-89		15/3 2014	9	5

Solved task Behandlade uppgifter. No / nr		Points per task Poäng på uppgiften.	Observe: Areas with bold contour are to be completed by the teacher. Anmärkning: Rutor inom bred kontur ifylles av lärare.
1	X	10	
2	X	8	
3	X	4+	
4	X	5	
5	X	5+	
6	X	8	
7	X	2+	
8	X	10	
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
Total examination points Summa poäng på tentamen		52	

a)

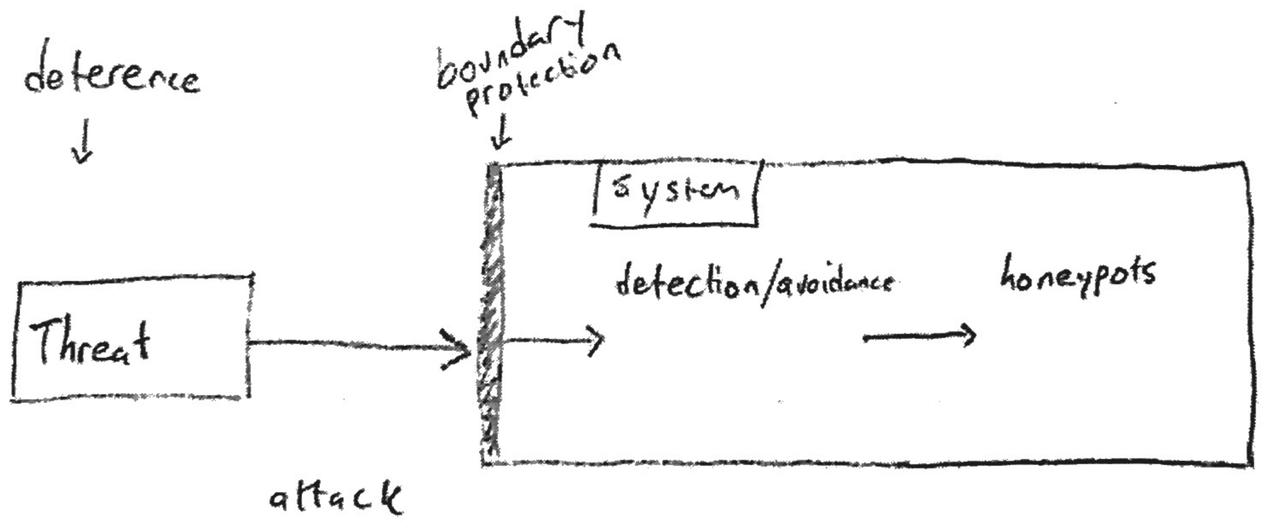
- Reliability: The probability of a system failure in some interval
- Safety: The probability of a catastrophic system failure in some interval
- Maintainability: Denotes how easy a system is to maintain and repair
- Confidentiality: The property of not revealing information to unauthorized users
- Integrity: The property of not allowing modifications by unauthorized users.
- Availability: The probability of the system being available (providing correct service)

1p

1p

1p

b)



Protection mechanisms include preventive actions deterring possible adversaries, such as legal protection etc. Another, and perhaps one of the most important, mechanism is boundary protection, this includes firewalls and passwords used to prevent security breaches and attackers getting in to the system (Cf. Castle wall). To mitigate damage in case an attacker still gets in we can use intrusion detection systems that tries to detect and warn administrators of intrusions, we can then either take action to stop the attack or lead the attackers to a honeypot. A honeypot is a decoy system used for research/forensics which gathers information about attacks and attackers. The information gained from honeypots can be used to further improve other protection mechanisms.

7p

10p

			2
	EDA263-89	X	2

a)

- TOE or Target of evaluation is the actual product being evaluated.

- PP is a document, often compiled by a user or user community, that defines a number of security requirements on a certain category of Security devices. PP is an acronym for Protection Policy.

+

- ST or Security target is an implementation-specific document that may be based on one or more PPs that specifies Security requirements for a TOE. These requirements are called SFRs (Security functional requirement) and SARs (Security assurance requirements). A TOE is evaluated against the SFRs in its ST.

+

- EAL means evaluation assurance level and denotes the depth and rigor of a CC evaluation.

+

b) In order to say Something about the Security of a System that has passed a CC evaluation we need to know more about the evaluation. First we need to look at the EAL to get an idea about how rigorously the evaluation has been performed. We also need to examine which Protection profiles were included in the ST in order to see if this is sufficient for the intended use (which of course also has to be known if we wish to say Something about the security). Does the implemented PPs correspond well to industry standards regarding the device/product at hand?

-

a) Some sort of public-key encryption algorithm.
0p

b) Exchange of (sensitive) keys used in symmetric encryption schemes, which cannot be done unless we have a secure channel
2p

c) This encryption algorithm is based on the idea that it is hard (takes a lot of computing time) to perform factorization on large numbers. (Pending the dreaded quantum computer)
2p

Rule set A describes a default allow policy whereas Rule set B describes a default deny policy. This can be seen by looking at the last rule, the catch-all case at the end.

The difference between the two is how they handle packets that are not covered by any other rule. Rule set B does not forward such packets and is more restrictive than A, this type of approach is similar to white-list mechanisms where all types of actions/packets/etc. that are allowed need to be specified in advance. Rule set A instead uses the default allow policy, this is more permissive and roughly similar to black-list approaches where known threats/vulnerabilities are handled with blocking/denying rules.

Advantages with rule set A include ease of use, convenience and flexibility. For example if a company sets up some sort of new service using a new port, the firewall would not need to be reconfigured (which it would have to be in a default deny setting). The main disadvantage of this approach is that vulnerabilities are not yet known or have not been considered may be exploited more easily. The permissive nature of this policy means that a lot of unused "doors" to the system/network are open.

Advantages with rule set B include improved security and control. No traffic that has not been cleared/allowed in advance will get through the firewall. The disadvantages with this approach is that we lose ease of use, flexibility and convenience. Setting up new services requires reconfiguration of the firewall and accessing outside services that has not been allowed in advance does aswell.

TOCTOU (time of check to time of use) flaws are caused by code/programs that check one or several properties of an object, in order to for example avoid opening files that a user should not have access to, and then using the object. The problem at hand is that the object or file can be changed between the check and the use, so that when it is used it no longer satisfies the checks performed.

In this example an attacker could attempt to swap a file that passes the checks with a symbolic link to something else right before the time of use.

As this is a rather short time span the attacker would need to do this at exactly the right time but several methods to do this exists (some aimed at making the scheduler behave in certain ways).

Attacker	program	
create regular file f run program		
	lstat-check on f (regular file.) IFREG-check on f (regular file)	} TOCTOU
Swap f with symlink		
	Open f (now a symlink)	

First off, passwords are not stored in plain text, instead passwords are hashed using some hash function. Hashing is supposed to be one-way so that getting a password from a hash is difficult. Password hashes are stored instead of plain text passwords and logins works as follows: user supplies password, which is hashed and then validated wrt the saved hash for the user in question. This means that if /etc/passwd (or actually /etc/shadow) is compromised, it would take time for the attacker to find the actual passwords of the users.

A second layer of security is added with salting. Salted hashes are used to make finding plaintext passwords even harder by introducing a random number added to each password before hashing. The result of this is that even if users have the same password their hashes will differ (as long as they have different salts). This also means that dictionaries of hashes become much harder to construct since every password has to be hashed together with every possible salt. In practice salting works like this: each time a user is created or a password is changed a salt is chosen, this salt is combined with the password which is then hashed the salt and the hash is then saved to be used for validation. Login works by letting the user supply their password, fetching the salt, hashing the supplied password combined with the salt and comparing this to the stored hash.

/etc/passwd

username	password	UID	(more fields)
olle	[placeholder]	100	...
helen	[placeholder]	101	...

/etc/shadow

Uid	salted hash	salt
100	[olles salted hash]	XXX (olles salt)
101	[helens salted hash]	YYY (helens salt)

5

EDA263-89

Points for question: 2 +

Consecutive page no: 7

Question no: 7

a) Two-factor authentication is authentication where two pieces of authentication information needs to be Validated for the user to be authenticated. One example of such a scheme could involve a user password and a one-time code of some sort which both are validated in the authentication process.

-1

b) If we consider a smartphone application for banking, an attack could be performed where an attacker creates a fake application that resembles the real one. When a user starts the login process she enters her username and password which are sent by the malware both to the legitimate bank server and to the attacker. This prompts the bank system to send out a one-time authentication code to the users phone via SMS. This is then either manually or automatically supplied to the malware which proceeds by sending the one-time code to the attacker (not to the legitimate bank server) and produces an error to the user saying something along the lines of "Service unavaliable, try again later". The attacker now has access to both pieces of authentication information and can use this to gain access and for example transfer money to their own account.

T

5

a) A Salami attack is an attack where seemingly inconsequential data is used and aggregated until a significant amount is achieved. One example of this is taking the fractions of cents produced when calculating interests for banks and putting it in your own account, the owners of the accounts would not notice, but it would soon (given enough accounts) add up to a significant amount of money.

b) Data remanence refers to data that is not completely removed from some storage media. Magnetic hard drives, for example, contain traces of old data until the space freed by the deletion has been reused (a number of times). One example relating to non-magnetic media is the possibility of freezing attacks against devices such as phones/computers where the entire file system is encrypted. This scheme requires the encryption key to be kept in RAM at all times. Information in RAM decays over time when a device is powered of, but slower in cold temperatures which could make reading the encryption key possible

c) A trojan horse is a program containing additional unwanted functionality. For example an attacker could place a keylogger within an instant messaging client and then distribute this modified version Any user installing and using the client also gets the Keylogger.

d) A Zombie or a bot is a computer infected by malware which makes it controlable by an attacker. This means that an attacker can use the computer and its resources when she wants to. Zombies are often used to send Spam or to perform DDOS attacks against other servers. Zombies can be dormant until the attacker chooses to use them.

e) Steganography is methods for hiding a message, but contrary to cryptography the point is not to hide the contents of the message but rather its existence. Steganography can be used to hide one message inside another, making it invisible to anyone but intended readers. However, if the hidden messages are in plain text and the extraction method exposed, anyone can read the messages.

f) The Morris worm used a password guessing/cracking attack, the debug facilities of Sendmail and a bug in finger. Password guessing is pretty straight-forward, the attacker constructed a program that would guess to find passwords. The bug in the finger daemon (fingerd) was related to the use of gets() which is a non-bounds checking function in C which can be used to perform buffer overflows.

2

g) The first method is using malformed packets etc to cause the system to fail, this is often called <u>poisoning</u> and one famous example is the ping-of-death attack.

The other method is <u>flooding</u>, where one or more computers (DOS vs DDOS) are used by the attacker(s) to send a large amount of traffic to the target, which overwhelms it and causes loss of availability.

2

h) A ticket in Kerberos is issued to a user by the ticket granting Service (TGS) and is a token/message used by the user to gain access to a service. One ticket is requested for each Service session. The term ticket is sometimes also used to describe the token given from the Kerberos authentication server (KAS) to a user to enable interaction with the TGS.

1