Final exam in

Computer Security EIT060

Department of Electrical and Information Technology
Lund University

March 18, 2016, 14-19

- You may answer in either Swedish or English.
- If any data is lacking, make (and state) reasonable assumptions.
- Use legible hand writing. If your answers cannot be read, you will receive zero points on that problem.
- Only pencil and eraser is allowed.
- Grading is done as follows.
  Grade 3 = 20–29 points,
  Grade 4 = 30–39 points,
  Grade 5 = 40–50 points.

Problem 1. Explain how an attacker could (try to) forge a digital signature.

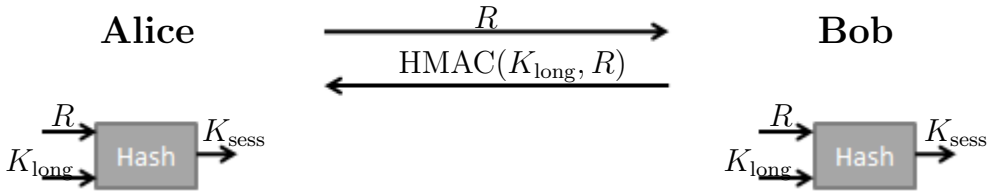
Answer
A forgery can be done either by obtaining the private key or by finding a collision in the hash function that is used in the signature. The private key can e.g., be stolen or an attempt to compute it from the public key can be done. (3 points)

Problem 2. Two communicating parties (A and B) are negotiating a session key. They both share a long term *symmetric* key, K_{long}. The picture shows how the session key, K_{sess}, is computed. The random value, R, is sent as part of the handshake protocol and thus known to both A and B at the time of computation.

a) What would be a suitable algorithm, to use inside the box in the figure, i.e., how should f such that $K_{\text{sess}} = f(K_{\text{long}}, R)$ be chosen?

b) Suggest a reasonable handshake protocol that provides *implicit key authentication* and *unilateral authentication*, using the long term symmetric key.

Answer
a) A hash algorithm is suitable. (Other answers, such as MAC or block cipher is acceptable if it is clearly motivated.)
b) Since we want implicit key authentication we wish to be certain that no one else besides a party knowing the long-term key can be able to compute the session key. Unilateral authentication can be obtained through a challenge-response protocol. Assume that Alice wishes to authenticate Bob. A simple protocol providing this would be



(1+2 points)

Problem 3. The TLS handshake protocol protects against replay attacks. Explain how this is achieved.

Answer
The Hello messages will include random values from both the client and the server and the finished messages will include an encrypted hash of the previous messages in the handshake, including the random values. If an attacker replays messages from e.g., the client side, the finished message will not be correct as it will include the wrong server generated random value. (3 points)

Problem 4. The IP header includes a 16-bit checksum. Basically, you take the header and divide it into 16-bit words and add these together. The checksum is the complement of this sum. However, the details are irrelevant to this problem.

a) Does this checksum provide integrity protection? Motivate your answer!

b) Assume that, instead of this checksum, a modern state-of-the-art hash function is used. How would this affect the integrity protection in the presence of a man-in-the-middle? Motivate your answer!

Answer
a) It provides integrity protection against unintentional modification, but not against an active attacker who can make changes to the header and recompute a valid checksum.
b) It does not change anything. A man-in-the-middle will still be able to make any changes and recompute the hash value. (1.5+1.5 points)

Problem 5. PGP uses the notions *validity* and *trust*.

a) When Alice signs Bob's public PGP key, what happens to the *trust* and *validity* of Bob's public key?

b) Further, assume that Bob has signed Charlie's public key. What is required in order for Alice to use Charlie's public key with very high confidence that the key is actually Charlie's?

Answer
a) In Alice's view, the validity of Bob's public key is *full*. The trust is not set implicitly (it is unknown), but has to be decided explicitly by Alice.
b) The confidence is decided by the validity of the key. If Alice decides to fully trust Bob, then the validity is full. If Alice decides to only marginally trust Bob, then there has to be either one other signature on Charlie's key by someone Alice fully trust or two other signatures by people who Alice has marginal trust in. If Alice does not trust Bob at all then there has to be either one other signature on Charlie's key by someone Alice fully trust or three other signatures by people who Alice has marginal trust in. (1+2 points)

Problem 6. Consider an executable file in Linux with the following permissions

```
-rwsrws--x 2 10 Alice Students prog
```

Assume that the user Bob successfully executes the program. List the different IDs that are associated with the running process and determine their values.

Answer
There are four IDs associated with the process and they take the following values: Real user ID: Bob
Effective user ID: Alice
Real group ID: Bob's primary group
Effective group ID: Students (3 points)

Problem 7. When authenticating to a computer or web service, a user often submits a password. How should, according to best practice, the password-related information be treated by the computer or web service?

Answer
At least the following properties should hold for a correctly stored password:

a) Passwords must be stored in hashed form.

b) Each user must have a unique salt associated with the password. This salt should be used as input to the hash function together with the password.

c) The hash function must be slow so that brute force or dictionary attacks only can test few passwords per second (typically in the order of a few hundred).

(3 points)

Problem 8. Compare how functionality and assurance are treated in Orange book and Common Critera evaluations.

Answer
In Orange book, functionality and assurance is tied together. Each evaluation level sets rules for both. In common criteria, the security target states the functionality of the product and the evaluation level states the assurance. Thus, functionality and assurance is separated in common criteria. (3 points)

Problem 9. Consider the Bell-LaPadula state below.

Current acces set, b
(Alice, file_b, w)
(Alice, file_a, r)
(Charlie, file_e, a)
(David, file_c, r)
(Erika, file_d, w)

Access Control Matrix, M

	file_a	file_b	file_c	file_d	file_e
Alice	r,w,a	r,w		e	a
Bob			a	r,e	
Charlie	r	r		r	r,e
David			r,w,a	r	r,w
Erika	a			r,w,e	

Functions, $f = (f_S, f_C, f_O)$

f_S:
Alice: (private {A,B}), Bob: (public, {A,B}), Charlie: (private, {A}), David: (private, {A,B}), Erika: (private, {A})

f_C:
Alice: (private, {∅}), Bob: (public, {A,B}), Charlie: (public, {B}), David: (public, {A,B}), Erika: (public, {∅})

f_O:
file_a: (private, {A}), file_b: (private, {∅}), file_c: (public, {A,B}), file_d: (public, {A,B}), file_e: (private, {A,B})

Assume that we have a lattice with two classifications, public and private, and two categories, A and B. These are used in the Bell-LaPadula model. Determine which security properties are broken and motivate why they are broken (if any).

Answer
ss-property is broken since Erika should not be allowed to write to file_d.
***-property** is broken since Alice is reading file_a and writing to file_b at the same time. This is not allowed since f_O(file_a) > f_O(file_b) which means that information from file_a can flow to file_b, i.e., downwards.
ds-property is broken since Charlie is not allowed to append to file_e according to the Access Control Matrix. (3 points)

Problem 10. In WEP, a challenge-response protocol based on a stream cipher (RC4) was used. What was the fundamental flaw in this protocol?

Answer
The flaw was that a stream cipher was used in order to compute the response as response = challenge $\oplus$ keystream. By xoring challenge and response the keystream could be used to either authenticate again (using the same IV as before) or to decrypt any traffic using the same IV. (3 points)

Problem 11. Several well-known antivirus products install a CA certificate on the user's computer. This is used to mount a man-in-the-middle attack on TLS connections

involving the computer.

a) Explain how the attack is performed and why it succeeds.

b) Why would an antivirus product mount an attack like this on the user?

Answer
a) The antivirus, acting as a MitM, will capture traffic before it leaves the computer and also capture returning traffic before it is delivered to the application. When installing the antivirus product, the user also installs a trusted CA certificate with the product's public key. This will allow the MitM to create legitimate certificates on the fly for any requested webpage. The MitM will then act as the webpage to the application and set up its own connection to the real webpage.
b) As a MitM, the antivirus will be able to read all incoming and outgoing traffic in unencrypted form. This will make it easier to detect malware or other types of attacks to the computer it protects. (3+2 points)

Problem 12. The buffer overflow attack is still one of the most common attacks. Both the attack and mitigation techniques have evolved since its first discovery.

a) What is the purpose of introducing NOP instructions in the program code in a buffer overflow attack?

b) What is a canary value and how does it protect against the attack?

c) How does ASLR make the attack more difficult?

Answer
a) When injecting code into a buffer, it is difficult to know the exact location of where it will end up. The return address should be chosen to be the start of the code and by starting the code with a number of NOP instruction, the attacker gives himself an error margin when guessing the location of the code.
b) A canary is a value inserted between local variable and the return address in the stack. The idea is that when overflowing a buffer in order to overwrite the return address, this will also overwrite the canary. Checking the integrity of the canary before returning from a function will detect an attack.
c) ASLR will randomize the location of the stack, heap and libraries in order to make it virtually impossible for an attacker to correctly guess the value of the return address to use in the attack. (2+2+1 points)

Problem 13. RSA is based on the problem of factoring large numbers. The public parameters of an insecure RSA scheme are:

- Modulus: $n = 221$
- Public exponent: $e = 7$

Recall that, in RSA, the private exponent d is chosen such that $e \cdot d \equiv 1 \mod \phi(n)$. Find d and decrypt the ciphertext $c = 2$.

The following table might be helpful:
$2^2 \equiv 4 \mod 221$
$2^4 \equiv 4^2 \equiv 16 \mod 221$
$2^8 \equiv 16^2 \equiv 35 \mod 221$
$2^{16} \equiv 35^2 \equiv 120 \mod 221$
$2^{32} \equiv 120^2 \equiv 35 \mod 221$

Answer
We know that $n = 221$ is the product of two primes. Testing a few primes gives us $221 = p \cdot q = 13 \cdot 17$. Thus, $\phi(n) = (p-1)(q-1) = 12 \cdot 16 = 192$. In RSA we have that $e \cdot d \equiv 1 \mod \phi(n) \Rightarrow e \cdot d = k \cdot \phi(n) + 1$, for some integer k. With $k = 2$ we find that $d = (192 \cdot 2 + 1)/7 = 55$.

The next step is to find $2^{55} \mod 221$. This is easy once we note that $2^{2x} \mod n \equiv (2^x \mod n)^2$, and that $55 = 1+2+4+16+32$. Using the table, we have $2^{55} \equiv 2 \cdot 4 \cdot 16 \cdot 120 \cdot 35 \equiv 128 \mod 221$. Note that the last two lines in the table implies that $120 \cdot 35 \equiv 1 \mod 221$ so the calculations becomes very simple. (5 points)

Problem 14. Explain shortly the following five terms:

a) HMAC

b) ECB mode for block ciphers

c) Encapsulating Security Payload (ESP)

d) Honeypot

e) Reference monitor

Answer
a) A MAC computed using a hash function.
b) A block cipher mode where each block is encrypted independently from other blocks.
c) IPsec protocol which offers both integrity and confidentiality.
d) A network connected computer which does not hold any valuable information, but exists in order to draw attention to attackers.
e) An abstract machinery with the purpose of making access control decisions. (5 points)
