Final exam in

Computer Security EIT060

Department of Electrical and Information Technology
Lund University

March 14, 2013, 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. The course has given (at least) three examples of situations where introducing publicly known randomness has resulted in more secure solutions. These are initialization vector (IV), salt, and nonce. For each of these, explain how this publically known value adds security.

Answer
An IV allows reuse of a key in a stream cipher and most block cipher modes of operation without revealing important information about the plaintext to an eavesdropper. A salt adds randomness to passwords before they are hashed in order to e.g., make two identical passwords hash to different values. A nonce is a random value used in protocols in order to authenticate peers and also to prevent replay attacks. (3 points)

Problem 2. A server often wants to authenticate a client. The SSL/TLS handshake protocol includes the possibility to authenticate the client, but this possibility is typically not used on the Internet when requesting SSL/TLS protected webpages. Why?

Answer
If client authentication is used, the client needs to have a certificate signed by a CA which is trusted by the server. It is not very practical to let all users have a certificate, or perhaps several certificates if they need different certificates for different webpages.

The signing procedures for these certificates would probably have to be rather insecure anyway so that anyone easily could get a certificate. In some situations, however, a client certificate could be reasonable as was seen in project 2. (3 points)

Problem 3. Give two differences between the LM and the NTLM hash that are important for security.

Answer
When computing the LM hash, the characters are first converted to upper case. Also, the hash is computed by independently hashing the first and last 7 characters of the password so each part can be cracked independently of the other. (3 points)

Problem 4. In the Bell-LaPadula security model, a secure state is a state that satisfies the ss-property, the *-property and the ds-property. Define these properties.

Answer
ss-property: If access operation includes read then subject security level must dominate classification of the object.
**-property:* If access operation includes append then subject security level must be dominated by the classification of the object.
ds-property: Any access operation must be allowed in the access control matrix. The matrix can be used to pass access rights on to other users. (3 points)

Problem 5.

a) Explain how a canary value can be used to detect a buffer overflow attack.

b) Give an example of how a buffer overflow attack can be prevented.

Answer
a) The canary value is a known value that is placed on the stack between the return address and the stack allocated variables. If a buffer overflow occurs that overwrites the return address the canary will also be overwritten and the overflow can be detected.
b) Prevention mechanisms include e.g., not using insecure functions such as strcpy(), making the stack non-executable and automatic source checking using software. (2+1 points)

Problem 6. IPsec can be used in either transport mode or tunnel mode and using either the AH or the ESP protocol.

a) A new IP header is constructed when tunnel mode is used. Explain the advantages of this (i.e., the advantages of tunnel mode compared to transport mode).

b) How does IPsec protect against replay attacks?

Answer
a) Tho original IP header can be fully protected. Also, it allows IPsec to be implemented in gateways so that individual computers do not have to implement the protocol.
b) The header (AH or ESP) includes a sequence number which the receiver can check.

(2+1 points)

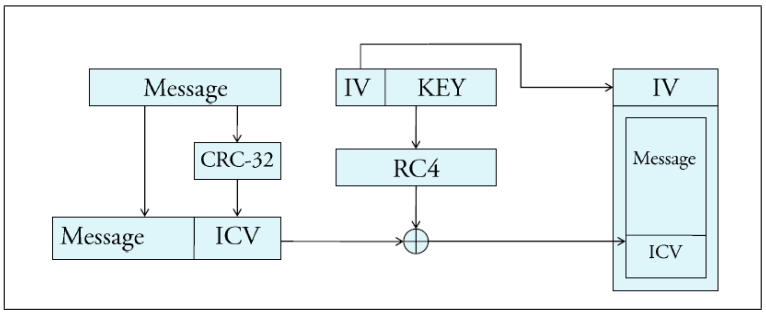
Problem 7. What are the differences between the two IDS techniques *anomaly detection* and *misuse detection*?

Answer
Anomaly detection analyses the system with respect to a baseline, i.e., something that is considered normal for the system. If the state or the behaviour is too far from the baseline this is regarded as an intrusion. This has the possibility of detecting new and previously unknown attack methods, but it will also miss those attacks that are too close to the normal behaviour. In misuse detection, the IDS compares system events to a database of events that are known to be attacks (signatures). This will reliably find well known attack methods but it will not detect new attacks that do not have their signature recorded in the database. (3 points)

Problem 8. How are the Orange book, ITSEC and Common Criteria related? How do they differ in their treatment of functionality and assurance?

Answer
Common criteria is partly based on experience and drawbacks that were present in the Orange Book and in ITSEC. While Orange book combined functionality and assurance and classified products based on both, ITSEC only classified products according to an assurance level, i.e., functionality and assurance was completely separated. Common Criteria instead uses protection profiles that defines basic fnctionality for a certain type of products. Then, the product can be evaluated against this protection profile. Thus there is separation between functionality and assurance, but they are not as independent as in ITSEC. (3 points)

Problem 9. In order to have integrity protection of the messages in WEP, CRC-32 is used. The linear function CRC-32 is used to compute an integrity check value (ICV) of the message. The ICV is appended to the message and the resulting bitstring is encrypted using RC4 (see figure). To verify that the message has not been changed during transmission, the recipient decrypts the bitstring, computes the ICV of the message using CRC-32 and compares it to the value in the decrypted bitstring.



Adding ICV to message in WEP.

Assume that you can intercept these encrypted bitstrings, change them, and forward them to the intended recipient. Explain how you could flip the first and the last bit of the message without the recipient being able to detect this when checking the integrity

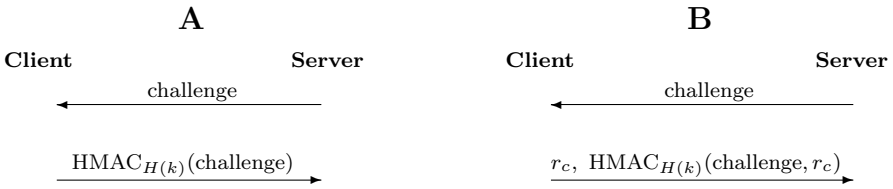
of the message.

Answer
Since the function is linear we have that CRC-32$(M + \Delta)$ = CRC-32$(M) \oplus$ CRC-32(Δ). The transmitted bitstring can be written as $M \| \text{CRC-32}(M) \oplus RC4(K)$. Our goal is to change M to $M \oplus \Delta$ where $\Delta = 100 \ldots 001$. Since we do not know the key K we do not know M or CRC-32(M). Instead we can compute CRC-32(Δ) and add these bitstrings to the received bitstring. Then the receiver will get

$$\begin{aligned} & M \| \text{CRC-32}(M) \oplus RC4(K) \oplus \Delta \| \text{CRC-32}(\Delta) \\ = \; & (M \oplus \Delta) \| \text{CRC-32}(M) \oplus \text{CRC-32}(\Delta) \oplus RC4(K) \\ = \; & (M \oplus \Delta) \| \text{CRC-32}(M \oplus \Delta) \oplus RC4(K) \end{aligned}$$

which will be accepted at the receiver side since the ICV is correct. (3 points)

Problem 10. Consider the two authentication protocols given below. HMAC$_{H(k)}(x)$ is an HMAC computed on the input x using key $H(k)$, where $H(k)$ is the hash computed on a password k.



a) You want to perform a TMTO attack to recover the password. Explain how a MITM attack can make a client use a challenge chosen by the attacker in protocol A.

b) A *known* (i.e., eavesdropped) challenge would be enough in a brute force or dictionary attack. Why is a known challenge not sufficient in a TMTO attack?

c) In protocol B, the client adds a random number r_c to the response. How will the security in the protocol change?

Answer
a) The MITM simply takes the nonce sent from the server and changes it to his own chosen nonce. Then the client will respond with a MAC that is based on the attacker's nonce.
b) The TMTO tables must be built *before* the actual attack starts, i.e., before the attacker learns the HMAC. When building the tables, a nonce must be used and this is the nonce that the attacker later has to pick as his chosen nonce.
c) The protection against TMTO attacks is significantly improved since now it is not enough that the MITM chooses the challenge sent from the server to the client. Each new HMAC will use a challenge that the attacker has no chance of influencing and it will thus not be possible to build tables without including r_c. (1+1+1 points)

Problem 11. Consider protocol A from Problem 10.

a) Explain how you would *build* the TMTO tables (or rainbow table, choose which you like best). Make sure you mention *startpoint*, *endpoint* and *reduction function*.

b) Assume that our online attack time should take time $T = 2^{24}$ and require memory $M = 2^{24}$. Approximately how complex can the recovered password be? Give the length of the largest passwords that can be broken assuming the passwords are alphanumerical.

c) How would a function like `PBKDF2()` improve the security of the protocol?

Answer
a) A random key k_0 is chosen as a startpoint. This key is hashed with H and an HMAC on a chosen value (the chosen challenge) is computed using the hashed random key as key. In other words, the function f to invert is given by $f : k- > HMAC_{H(k)}(\text{challenge})$. The result of this function is then transformed to a new key k_1 using a reduction function. This function can be chosen arbitrarily. Just truncating the HMAC is one simple alternative. The procedure is repeated for k_1, producing $k_2, k_3, \ldots, k_t$. The last value, k_t, in this chain is called endpoint. The startpoint and endpoint are saved and all other k_i are thrown away. Then a new chain is computed for another random password, again saving the start- and endpoints. In order to avoid merging chains due to the reduction function mapping the result to shorter strings, new tables using different reduction functions are built when the probability of merging chains is large (the details here are not required for full points).
b) With the given T and M we get $N = 2^{36}$. Since there are approximately 2^6 alphanumeric characters, the length of the passwords that can be broken is 6.
c) Since PBKDF2 is a function that makes a key from a password, this is very appropriate in our protocol. Its main feature is that it is much slower (with appropriately chosen parameters) than a hash function, providing key strengthening. This would increase the time for building the TMTO tables significantly and it would also make brute force and dictionary attacks much slower. (2+2+1 points)

Problem 12. Consider a hash function with n-bit output.

a) Explain what is meant by *preimage resistance, second preimage resistance*, and *collision resistance*.

b) How many different inputs are needed (approximately) before a collision is found.

c) How many different inputs are needed (approximately) before a second preimage is found?

Answer
a) Preimage resistance: Given y, it is difficult to find x such that $h(x) = y$
Second preimage resistance: Given x and $h(x)$, it is difficult to find x' such that $x' \neq x$ and $h(x') = h(x)$
Collision resistance: It is difficult to find x and x' such that $x' \neq x$ and $h(x') = h(x)$
b) For an n-bit hash function we expect that we need about $2^{n/2}$ different inputs in order to find a collision.
c) For an n-bit hash function we expect that we need about 2^n different inputs in order to find a second preimage. (3+1+1 points)

Problem 13. An example listing of directory content in Linux is given below, together with an excerpt from the file `/etc/group`.

Directory listing:

```
drwxrwsrwt   root   students  .
-rwsrwxrwx   alice  root      prog
```

/etc/group file:

```
students:x:1001:alice,bob,charlie
```

a) What will be the *ruid* of a process that executes prog?

b) What will be the *euid* of a process that executes prog?

c) Who can delete the file prog? Answer by giving an element in the powerset of {alice, bob, charlie, root}

d) Assume umask is 027, give the corresponding line in a directory listing when Alice creates a new non-executable file.

e) The file `/etc/passwd` often also has an 'x' in the corresponding position as can be seen in the `/etc/group` file above. What does this 'x' mean in the `/etc/passwd` file?

Answer
a) The same as the uid of the user starting the process
b) Uid of alice
c) {alice, root}
d) `-rw-r----- alice students filename`
e) The password hash is stored in a shadow file (1+1+1+1+1 points)

Problem 14. Explain shortly the following five terms:

a) Reference monitor

b) Clark-Wilson

c) CBC mode

d) Security descriptor

e) inode

Answer
a) The abstract machinery that is is charge of allowing or denying access to resources.
b) A securty model that focuses on integrity in non-military systems.
c) A block cipher mode of operation that does not preserve plaintext redundancy in the

ciphertext.
d) In Windows, data associated with securable object containing e.g., object owner and access control list.
e) In Unix/Linux, the data structure that holds information about a file, e.g., owner, group, access rights and time stamps. (1+1+1+1+1 points)
