Final exam in

Computer Security EIT060

Department of Electrical and Information Technology
Lund University

March, 10, 2011, 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.

Answer
Only symmetric cryptography is used in the UMTS key agreement and authentication protocol so there is no nonrepudiation provided at all. (3 points)

Problem 2.

Answer
The idea is to copy more data into a buffer than what has been allocated for that buffer, thereby overwriting the return address on the stack. This is possible when the programmer has used unsafe functions and if the buffer size of the destination is smaller than that of the source buffer. Overwriting the return address with an address that points to the attacker's code can force the program to run that code. (3 points)

Problem 3.

Answer
a) A trusted path (or secure attention sequence) can be provided by the operating system. It is constructed such that only the operating system can catch these sequences, no user

programs. An example is ctrl-alt-delete in Windows.
b) To detect such attacks the system can show the number of failed login attempt once a user has logged in correctly. (3 points)

Problem 4.

Answer

Confidentiality: The usage of the IV in the stream cipher is flawed. Also the IV is too short.
Integrity: The integrity algorithm used is linear. Since a stream cipher adds the keystream linearly to the message it is possible to modify the message and correctly compute a new integrity check value even though the message is encrypted.
Authentication: The challenge response scheme uses a stream cipher to encrypt the response. By eavesdropping one authentication, it is easy to obtain the keystream and then authenticate as that user at any time. (3 points)

Problem 5.

Answer

The real UID is the UID of the logged in user. It is used to identify the logged in user in case the effective UID is temporarily changed. The effective UID can always be changed to that of the real UID.
The effective UID is used for access control. Access rights for files are compared with the effective UID for the user. (3 points)

Problem 6.

Answer

In Windows, if a user has one set of access rights and the user is member of a group with another set of access rights, the user will be given the union of all access rights. In Linux, if the user is the owner of the file, the access rights of the owner are the ones that determine his access. Any group access rights will not be checked at all even if the user is a member of the group that is group owner of the file. (3 points)

Problem 7.

Answer

Both security models assign security levels to subjects and objects and access is granted based on these levels. The Bell-LaPadula security model focuses on confidentiality. For read access it is required that the security level of subject dominates the security level of the object. For append access it is required that the security level of the object dominates the security level of the subject (no read-up, no write-down). The Biba model focuses on integrity and for read and append (denoted modify in Biba) the opposite is true (no write-up, no read-down). (3 points)

Problem 8.

Answer

a) The payload data, padding, pad length and the next header field.
b) In transport mode, the original IP header is placed before the ESP header, i.e., before the data represented by the packet in the figure. In tunnel mode, the original IP header is part of the payload data in the figure.

(3 points)

Problem 9.

Answer
Packet filters do not examine data at application level. Instead the packet filter only looks at information in the IP and TCP header, i.e., IP addresses and port numbers. Rules based on these determine if a packet is allowed to pass the firewall or if it should be blocked. A stateful packet filter is similar, but keeps in memory all ongoing connections. If a connection is initiated from inside the firewall, traffic returning to the same port will be allowed. This memory is needed since the firewall cannot in general predict which port is used by client applications and without the memory all incoming traffic on ports that can be used by clients must be allowed. (3 points)

Problem 10.

Answer
In orange book, functionality and assurance were not separated. Being evaluated in one security class meant claiming both a certain functionality and a certain assurance. Products with low functionality could not be evaluated with high assurance and vice versa. In common criteria there is some separation between functionality and assurance. A product can be evaluated against one or more protection profiles which state the functionality of the product. The assurance level is then separated from this and is given by how much effort was put into the evaluation. (3 points)

Problem 11.

Answer
CA private key: Used to sign the client and server certificates that are used in the connection.
CA public key: Used to verify the signature in the client and server certificates so that these can be trusted.
Client private key: Used to sign previous messages in the handshake in order to prove that the client is in possession of the private key.
Client public key: Given in the client's certificate and used by the server to verify the signature above.
Server private key: Used by the server to decrypt the premaster secret.
Server public key: Given in the server's certificate and used by the client to encrypt the premaster secret. (5 points)

Problem 12.

Answer
a) It is a challenge sent to (S). This will allow the client (A) to authenticate (S) and to

verify that the key K_{ab} is fresh.
b) There is no difference. The data $eK_{bs}(K_{ab}, A)$ is sent in the next step anyway. Note that in the description of Kerberos, this packet is sent separately.
c) The last message authenticates (A) to (B).
d) The server (B) can not verify that the key K_{ab} is fresh. If this is an old session key that has been broken, an attacker can enter the protocol at step 3 and negotiate the broken key with (B). (5 points)

Problem 13.

Answer
Empirically secure: There are no known attacks on the algorithm. This is the strength of most (unbroken) stream ciphers and block ciphers, e.g., AES.
Provably secure: The problem of breaking the algorithm can be reduced to the problem of solving a hard problem, i.e., factoring or the discrete logarithm problem. An example is RSA.
Unconditionally secure: It is not possible to break at all, regardless of computation time. One example is the one time pad (or Vernam cipher). (5 points)

Problem 14.

Answer
a) If a test has n possible outcomes, the number of tests needed before there is a collision in the outcome is in the order of $\sqrt{n}$. This gives an upper bound on the problem of finding collisions in a hash function.
b) A symmetric primitive used to provide integrity of messages and data. Also called keyed hash function.
c) False rejection rate. The probability that an authorized person is not accepted in a biometric system.
d) Learning sensitive data by combining knowledge gained from nonsensitive data.
e) A security model focusing on avoiding conflicts of interest. (5 points)