Final exam in

Computer Security EITA25

Department of Electrical and Information Technology
Lund University

March 12, 2018, 8-13

- 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

a) Yes b) No c) No (1+1+1 points)

Problem 2.

Answer

It is a *public* initialization vector that is unique for each keystream generated under a given key. It is used to make sure that two different plaintexts, p_1 and p_2, are always encrypted using different keystreams. Adding two ciphertext bits, c_1 and c_2, encrypted with the same keystream bit, will leak information about the corresponding plaintext bits.

$$c_1^i \oplus c_2^i = k_1^i \oplus k_2^i \oplus p_1^i \oplus p_2^i = p_1^i \oplus p_2^i$$

(3 points)

Problem 3.

Answer

The powerset is the set of all subsets of a set. Using powersets we can define a partial ordering such that $a \leq b$ if $a \subseteq b$. By labelling subjects and objects using an element in the powerset, we can control access through the partial ordering. To achieve information

flow integrity, we only allow information to flow downwards in a hierarchy. Thus, subjects can only write information to objects lower in the hierarchy (or at the same level), and subjects can only read information from objects higher in the hierarchy (or at the same level). This can be useful in any setting where we wish that information should not be confidentiality protected but the accuracy of the information is important. It is e.g., used by letting users lower the integrity level of internet explorer such that it (or malware running with its privileges) can not make modifications to the rest of the computer. It can only write to a specific folder which has also a lower integrity level. However, the process can still read regular folders on the computer. (3 points)

Problem 4.

Answer

Assume that there is no randomness in the functions above. Then we can model the mapping from PMS to key k as a hash function with fixed input, $k = h(PMS)$. In a chosen-plaintext on the block cipher, we can model the mapping from key to ciphertext as $c = h'(k)$. Thus, the one way function we wish to invert is $c = h'(h(PMS)) = h''(PMS)$. When building the tables, we start with a PMS in our search space of size N and generate the corresponding ciphertext. Then we use a reduction function R_i to map the ciphertext to a new PMS in the search space and so on in order to build the chains. After t steps a new chain is built. This is repeated m times and when $mt^2 = N$, a new reduction function is chosen and a new table is built with this function.

If there is randomness, the approach is very similar, but instead of letting the tables cover only the PMS, it must cover both the PMS and the randomness since the randomness used in a particular handshake will not be known when the tables are built. Thus, the randomness significantly increases the complexity of the attack. (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

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.

(1+2 points)

Problem 7.

Answer

Empirically secure is a cryptographic algorithm that has not been broken despite repeated

attempts to break it. It can be said to have withstood the test of time. A provably secure cryptographic algorithm can be shown to be secure if also another, well-known and difficult, problem can not be solved, e.g., factoring the product of two large primes or solving the discrete log problem. An unconditionally secure cryptographic algorithm can be shown not to be breakable under any circumstances. (3 points)

Problem 8.

Answer

Since the function is linear we have that CRC-32$(M \oplus \Delta)$ = 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 9.

Answer

The user is not allowed write access to the file that stores the list of hashed passwords. Still the user must be allowed to make changes to this file when updating his password. At the same time we can not allow the user to just make any changes, we (the system) have to carefully control how the changes are made. The solution is to write a program that makes the appropriate changes and then let the user run this program. This is the concept of controlled invocation. In order to give the program write access to the file we use the setuid functionality which allows the program to run with the access rights of the program owner. If the program is owned by root the program will have root privileges and can thus write to the file. (3 points)

Problem 10.

Answer

The threshold is used to determine how accurately a biometric sample must match a template in order to accept a user. A high threshold will increase the probability that valid users are denied access (increase FRR) but it will lower the probability of falsely accepting the wrong user (decrease FAR). A low threshold will have the opposite effect. (3 points)

Problem 11.

Answer

a) A trusted path is a way of ensuring that users are communicating with the intended recipient. It defends e.g., against spoofing attacks, where someone creates a faked login

program in order to capture passwords.
b) The Orange Book was the first initiative to evaluate operating systems. The purpose was to help developers making secure systems and also to help users to acquire secure systems.
c) While the Orange Book combined functionality and assurance, Common Criteria attempts to partly separate this using protection profiles. Moreover, Common Criteria is valid internationally and comes with a (quite significant) fee, while Orange Book evaluations where only valid nationally and were conducted for free. (1+2+2 points)

Problem 12.

Answer
a) The CA only needs to know that the public key actually belongs to the website. For this, the private key is not needed, the party requesting the certificate only needs to show that it controls the domain, which can be achieved in several ways, e.g., showing that it can add things to the web server, send emails or add records to the DNS.
b) One simple variant would have been to sign a string using the private keys and submit the certificate used to verify the signature. If DigiCert can validate the signatures, then they can also be certain that Trustico have the private keys.
c) Since Trustico have the private keys they can, in the case of RSA, decrypt the premaster secret and learn the encryption keys. In the case of Ephemeral Diffie-Hellman a passive attack would not be possible since learning the encryption keys would require them to solve the discrete log problem. (1+2+2 points)

Problem 13.

Answer
a) The return address points to the place in memory where execution will continue upon finishing a subroutine. The goal in the attack is to overwrite this address.
e) NOP instructions are instructions that do not change the state of the processor. Their purpose in a buffer overflow attacks is to allow some errors when guessing the address to overwrite the return address with. As long as execution jumps somewhere in a sequence of NOPs, the attack will still succeed.
c) A canary is a piece of known data, placed before the return address on the stack. Its purpose is to detect if the return address has been overwritten.
d) ASLR is a mechanism to randomize the memory layout for a process. Its purpose is to make it difficult for an attacker to guess what memory address to use when overwriting the return address.
e) W $\oplus$ X is a mechanism for tagging memory such that it is either writeable or executable. Its purpose is to make it impossible for an attacker to have injected code on the stack executed.

(1+1+1+1+1 points)

Problem 14.

Answer
a) An access control mechanism, where access is based on the security level of subjects and objects.

b) A symmetric cryptographic function that ensures the integrity and authentication of data.
c) The property of not being able to deny having sent (or received) some information.
d) An authentication scheme that avoids sending any secrets in plaintext on a channel.
e) An old hash function that was used to store passwords in Windows systems, having limitation such as not supporting lower case characters and dividing passwords into independent chunks which could be broken separately. (1+1+1+1+1 points)
