Written exam in TSIT02 Computer security

08:00–12:00, 20th of April 2017

Jan-Åke Larsson
Institutionen för Systemteknik,
Linköpings Universitet

Permitted equipment: General dictionaries between English and another language without personal notes. (Thus not specific scientific dictionaries with or without formulæ.)

Solutions: Solutions will be posted in Lisam after the exam.

Grading: Grade 3 requires at least 20 points

Other information: Answers can be in English or Swedish.

1. The course starts by defining that computer security is about ensuring the CIA criteria for data. Explain in one short sentence for each (one for C, one for I and one for A) what word the letter stands for and what requirement for data that the word refers to. Hint: If you use the word “access” for more than one criterion, you probably have missed at least one point. (6p)

2. A company in the US sued their bank after having been targeted by a Trojan horse that enabled the creator of the Trojan to transfer several hundred thousand dollars of the company’s funds to his own account. The company filed the lawsuit because they thought the bank security was too weak. The court, however, noted that the security was state-of-the-art and also that the bank used two-factor authentication, because customers need to log on to the service with one password, and then give a different password for large transactions.

   (a) From a technical standpoint, what is wrong in the argumentation of the court? (1p)

   (b) Passwords are an example of a more general authentication mechanism, which? (1p)

   (c) List at least two different serious weaknesses with this mechanism, in addition to eavesdropping from a Trojan horse. (1p)

   (d) List two different ways to reduce these weaknesses. (1p)

   (e) What are the two other general mechanisms for authentication? (1p)

   (f) Give one example for each of these two mechanisms. (1p)

3. Default configurations are often weak, which has been shown by the recent Mirai botnet. Attackers can exploit insecure default configurations by, for instance, scanning the net for passwords such as “admin” or “default”. The first step of hardening a system is therefore to disable insecure accounts and passwords. Give two additional things that should be done when setting up a new system in order to harden the configuration. (2p)

4. One of the three properties of a threat is used in quantitative risk analysis to determine if it is worthwhile to protect an asset from the threat. What property *of the threat* do we need to know to do quantitative risk analysis? What is the formula for (simple) quantitative risk analysis, what do the different variables mean, and where do they enter in the chain "threat-vulnerability-damage"? (4p)

5. Which formal security model covered in the course handles only confidentiality? Describe the "simple" criterion, and the "star" criterion. (3p)

6. DES (Data Encryption Standard) is outdated because of the short key length, and has been superseded by another more modern standard algorithm of the same type.

   (a) What is the new algorithm called? (name and abbreviation, 1p)

   (b) What type of algorithm is it? (1p)

   (c) What least key length is recommended for this algorithm type? (1p)

7. RSA is a different type of algorithm, that for example can be used for digital signatures.

   (a) Why can it be used for digital signatures, and why cannot DES (or its successor) be used to create or verify digital signatures? (1p)

   (b) What key length is currently recommended for RSA encryption? (1p)

   (c) To create and verify signatures is computationally expensive if done on an entire message. For this reason, a message is shortened by using a hash function to shorten the message into a "hash". A hash function to be used in signing must fulfill a particular requirement, to be secure. What is this requirement, precisely? (1p)

8. What are the two basic types of IDSs (give short descriptions) and why do you typically need both types in a large internal network? (3 points)

9. Cookies are used to perform many things, including authentication in web pages. Often, an attacker wants to steal the contents of a cookie in order to steal sessions.

   (a) The attacker wants to steal the cookie by injecting code in the response from the server. What is this attack called? Give both the three-letter abbreviation and the full name. (2p)

   (b) Give two defenses against the attack described in a). One defense should be server-side, one defense should be client-side. (2p)

10. For Code-based access control, name three sources of evidence for access control decisions. (3p) What does the execution environment use to keep track of the current permission, as it changes across subroutine calls? (1p)

Solutions

1. The course starts by defining that computer security is about ensuring the CIA criteria for data. Explain in one short sentence for each (one for C, one for I and one for A) what word the letter stands for and what requirement for data that the word refers to. Hint: If you use the word "access" for more than one criterion, you probably have missed at least one point. (6p)

   - C: Confidentiality. Only authorized users can read these specific data. I: Integrity. Only authorised users can enter or alter these specific data. A: Availability. Authorized users can always access these data when they need to.

2. A company in the US sued their bank after having been targeted by a Trojan horse that enabled the creator of the Trojan to transfer several hundred thousand dollars of the company's funds to his own account. The company filed the lawsuit because they thought the bank security was too weak. The court, however, noted that the security was state-of-the-art and also that the bank used two-factor authentication, because customers need to log on to the service with one password, and then give a different password for large transactions.

   (a) From a technical standpoint, what is wrong in the argumentation of the court? (1p)

   (b) Passwords are an example of a more general authentication mechanism, which? (1p)

   (c) List at least two different serious weaknesses with this mechanism, in addition to eavesdropping from a Trojan horse. (1p)

   (d) List two different ways to reduce these weaknesses. (1p)

   (e) What are the two other general mechanisms for authentication? (1p)

   (f) Give one example for each of these two mechanisms. (1p)

   - This does not count as two-factor authentication, because it uses only one of the three main kinds of authentication
   - "What you know"
   - Passwords can be guessed if they are words or are related to the user, and can be found with exhaustive search if they are short.
   - Search in a word list, exhaustive search of short passwords
   - "What you are" and "What you have"
   - Fingerprint, iris, and physical key, pass card, credit card.

3. Default configurations are often weak, which has been shown by the recent Mirai botnet. Attackers can exploit insecure default configurations by, for instance, scanning the net for passwords such as "admin" or "default". The first step of hardening a system is therefore to disable insecure accounts and passwords. Give two additional things that should be done when setting up a new system in order to harden the configuration. (2p)

- Configuring all security mechanisms
- Turning off all unused services
- Logging and alerts
- Keeping software updated

4. One of the three properties of a threat is used in quantitative risk analysis to determine if it is worthwhile to protect an asset from the threat. What property *of the threat* do we need to know to do quantitative risk analysis? What is the formula for (simple) quantitative risk analysis, what do the different variables mean, and where do they enter in the chain "threat-vulnerability-damage"? (4p)

   - The probability or frequency of the threat
   - The formula is "install the countermeasure if $k < f_b s_b - f_a s_a$"
   - The parameters are the cost k of the countermeasure, which is determined from what the weakness is, f_b is the frequency or probability before the countermeasure, f_a is the frequency or probability after, s_b is the damage cost before countermeasure, och s_e is the damage cost after. The threat is still there after installing the countermeasure, but the frequency will change.

5. Which formal security model covered in the course handles only confidentiality? Describe the "simple" criterion, and the "star" criterion. (3p)

   - Bell-LaPadula
   - Simple security property: A subject may read object only if the security level of the subject is greater than or equal to the security level of the object
   - $*$-property ("star"-property): A subject may write to an object only if the security level of the subject is less than or equal to the security level of the object
   - The standard mnemonic for this is "No read up—No write down"

6. DES (Data Encryption Standard) is outdated because of the short key length, and has been superseded by another more modern standard algorithm of the same type.

   (a) What is the new algorithm called? (name and abbreviation, 1p)

   (b) What type of algorithm is it? (1p)

   (c) What least key length is recommended for this algorithm type? (1p)

   - DES was superseded by AES, the Advanced Encryption Standard.
   - DES and AES are symmetric (block)cryptos.
   - The recommended minimal key length for a symmetric key system is presently 128 bits.

7. RSA is a different type of algorithm, that for example can be used for digital signatures.

   (a) Why can it be used for digital signatures, and why cannot DES (or its successor) be used to create or verify digital signatures? (1p)

(b) What key length is currently recommended for RSA encryption? (1p)

(c) To create and verify signatures is computationally expensive if done on an entire message. For this reason, a message is shortened by using a hash function to shorten the message into a "hash". A hash function to be used in signing must fulfill a particular requirement, to be secure. What is this requirement, precisely? (1p)

- A digital signature should only be possible to created by only one subject. But DES is a symmetric algorithm where both sender and receiver(s) have identical keys. Therefore, if you use DES, if you can verify a tag for a message, you can also create it (=a MAC).
- The recommended minimal key length for RSA is presently 3kbit.
- A hash function needs to be "weakly collision resistant", that is, it must be difficult to find another message m' given the message m so that $h(m') = h(m)$.

8. What are the two basic types of IDSs (give short descriptions) and why do you typically need both types in a large internal network? (3 points)

- An HIDS looks at the activity at a host, trying to find signs of an attack and raising an alarm if there are such signs.
- An NIDS looks at the activity of the network, both local network and connection points to the net, trying to find signs of an attack and raising an alarm if there are such signs.
- You need to monitor activity both on hosts, and on the network

9. Cookies are used to perform many things, including authentication in web pages. Often, an attacker wants to steal the contents of a cookie in order to steal sessions.

(a) The attacker wants to steal the cookie by injecting code in the response from the server. What is this attack called? Give both the three-letter abbreviation and the full name. (2p)

(b) Give two defenses against the attack described in a). One defense should be server-side, one defense should be client-side. (2p)

- The attack is called XSS, Cross-Site Scripting
- Client-side defenses include disabling JavaScript or using NoScript. Server-side defenses include sanitizing inputs, improving authentication and improving access control, so that it becomes harder to steal user credentials through the same-origin policy

10. For Code-based access control, name three sources of evidence for access control decisions. (3p) What does the execution environment use to keep track of the current permission, as it changes across subroutine calls? (1p)

- Code origin, code signature, code identity, code proof
- An extended stack that contains permission information