Written exam in TSIT02 Computer security

14:00–18:00, 08th January 2018

Guilherme B. Xavier
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 on Lisam after the exam.

Grading: Grade 3 requires at least 20 points.

Other information: Answers must be written in English.

1. Decide for each of the security breaches below if its immediate damage is best classified as C, as I or as A. Please note that it is the direct, first effect on the victim's data for the described event that is to be classified, not any possible further damage due to the event. If you are in doubt, do not just write C, I or A, but also motivate your choice clearly. (0.5p per item, max 3p)
   (a) A DDoS attack hits your site.
   (b) A keylogger sends your key strokes to an outside address.
   (c) A worm sends spam from your site using your e-mail account.
   (d) A virus establishes itself in your program library.
   (e) A user logs in with correct user-ID and password on a phishing site instead of the e-bank site.
   (f) An activist defaces your official company webpage with unwanted text and links.
2. List the three major categories of methods for user authentication, and give an example of each. Which two are most common? (4p)
3. Give a short description of an access control list (ACL) and what it is intended to do. Why are ACLs necessary? Also explain one technique that can be used to keep ACLs short and efficient. (4p)

4. In the design of the operating software of an optical time domain reflectometer (OTDR), an equipment designed to perform fault measurements along optical fiber lines, there is considerable amount of development time to properly optimize the operational and calibration parameters to ensure the proper functioning of the OTDR. In order to ensure that the end users do not accidentally alter these parameters while using the equipment, how should the permissions be set for the user with respect to the system? What is this security model called? Which of the different C, I or A is it concerned with? (4p)

5. Why should inputs entered at a web form be sanitized? Give one example of an attack possible if inputs are not sanitized. (2p)

6. What is whitelisting and blacklisting. Which one should you use as a system administrator? (2p)

7. Why is cryptography only considered a specific tool and not a more general solution? Describe what is Kerckhoff's principle. What is the main difference between asymmetric and symmetric cryptographic systems? (4p)

8. One protocol for authentication in computer networks is Kerberos. Who are the participants in a Kerberos exchange? Who is authenticated in a standard Kerberos session, and how is this done? What does the whole Kerberos protocol end with, what is shared in the process? Who share this data item? (6p)

9. Why do you need asymmetric algorithms in order to create a digital signature? What is the name of the most widely used asymmetric algorithm used for digital signing? Why is the signature normally performed on a hash of the message and not on the full message? What is the most stringent security requirement for these signature hashes called, and what does that condition really mean? (6p)

10. Briefly describe the "inference problem" in database security. What is a direct attack? What is an indirect attack? Give an example of a direct attack. (4p)

11. What is the main difference between whaling and phishing? Mitigation of social engineering attacks has to be done through three main fronts: Policy, Awareness and Technology. State one action to be done in each front by the security administrator. (4p)

Solutions

1. CIA
   Decide for each of the security breaches below if its immediate damage is best classified as C, as I or as A. Please note that it is the direct, first effect on the victim's data for the described event that is to be classified, not any possible further damage due to the event. If you are in doubt, do not just write C, I or A, but also motivate your choice clearly. (0.5p per item, max 3p)

   (a) A DDoS attack hits your site.

   (b) A keylogger sends your key strokes to an outside address.

   (c) A worm sends spam from your site using your e-mail account.

   (d) A virus establishes itself in your program library.

   (e) A user logs in with correct user-ID and password on a phishing site instead of the e-bank site.

   (f) An activist defaces your official company webpage with unwanted text and links.

   - A DDoS attack is typically causing damage to Availability, A.
   - Information surreptitiously sent to an outside address is C, Confidentiality.
   - The e-mail is sent in your name, which is the wrong name, thus I, data integrity.
   - A virus writes itself into your library without permission, which is a breach of I, Integrity.
   - The user has revealed the correct user-ID and password to somebody else, C, Confidentiality.
   - Unauthorised changes to a webpage are I, Integrity.

2. List the three major categories of methods for user authentication, and give an example of each. Which two are most common? (4p)

   - What you know (PIN, password), what you have (key, credit card), and what you are (fingerprint, signature)
   - The first two

3. Give a short description of an access control list (ACL) and what it is intended to do. Why are ACLs necessary? Also explain one technique that can be used to keep ACLs short and efficient. (4p)

   - An ACL normally lists users' permissions to Read, Write and Execute the object.
   - ACLs are necessary to ensure the correct distribution of permissions among different users in the same network/environment.
   - Users can be divided into groups with the same permissions, thus diminishing the length of the lists and often the necessity to change many ACLs when a user changes working duties (just edit the group list, not all relevant ACLs).

4. In the design of the operating software of an optical time domain reflectometer (OTDR), an equipment designed to perform fault measurements along optical fiber lines, there is considerable amount of development time to properly optimize the operational and calibration parameters to ensure the proper functioning of the OTDR. In order to ensure that the end users do not accidentally alter these parameters while using the equipment, how should the permissions be set for the user with respect to the system? What is this security model called? Which of the different C, I or A is it concerned with? (4p)

    - The permissions should be set such that the user can only read the configuration parameters, but not alter them. Also the system should be set such that it cannot read the user files, to avoid contamination. Basically: "No write up - No read down".
    - This security model is called Biba.
    - Biba is only concerned with integrity.

5. Why should inputs entered at a web form be sanitized? Give one example of an attack possible if inputs are not sanitized. (2p)

    - If inputs are not verified, an attacker can get malicious code to run at the server by cleverly injecting commands at the input.
    - SQL injection

6. What is whitelisting and blacklisting. Which one should you use as a system administrator? (2p)

    - Whitelisting is having a list of people allowed to access the system. Blacklisting is the converse, that is, the list of people that cannot access the system.
    - It is safer in general to employ a whitelist strategy, as it is ensured that only authorized people can access the system, even if that causes some annoyances to the legitimate users.

7. Why is cryptography only considered a specific tool and not a more general solution? Describe what is Kerckhoff's principle. What is the main difference between asymmetric and symmetric cryptographic systems? (4p)

    - Cryptography does not take into account social aspects, and as such does not yield protection against social engineering attacks for instance. It also only ensures protection against specific scenarios, and security fails if an attacker is able to circumvent these conditions.
    - A cryptosystem should be secure even if everything about the system, except the key, is public knowledge
    - The main difference is in respect to the keys employed. In symmetric systems, the legitimate parties encrypt and decrypt with the same key, while asymmetric systems have different keys for encrypting/decrypting, and they are not shared among the parties.

8. One protocol for authentication in computer networks is Kerberos. Who are the participants in a Kerberos exchange? Who is authenticated in a standard Kerberos session, and how is this done? What does the whole Kerberos protocol end with, what is shared in the process? Who share this data item? (5p)

    - A client, a Kerberos (authentication) server, an access-granting (authorization) server, and a service server
    - The client is authenticated
    - The client requests a session key (for the access-granting server) from the Kerberos server. The server responds with a key, encrypted with the client's password. The client can decrypt this only if he knows the password.
    - The process results in a shared key with a limited lifetime (a "ticket")
    - This is shared between the client and the service server.

9. Why do you need asymmetric algorithms in order to create a digital signature? What is the name of the most widely used asymmetric algorithm used for digital signing? Why is the signature normally performed on a hash of the message and not on the full message? What is the most stringent security requirement for these signature hashes called, and what does that condition really mean? (6p)

    - A digital signature should only be possible to create for one person and should be checkable by everyone. Therefore, a symmetric-key system cannot be used, because in such a system, anyone who can check a MAC (not "signature" in symmetric systems) can also create the MAC. In an asymmetric-key systems you sign with your private key, and everyone can check the result with the corresponding public key.
    - RSA or DSA are often used for this.
    - Since RSA (and DSA) is slow when signing large messages, only the hash of the message is actually signed.
    - But then an attacker mustn't be able to exchange a signed message with another message with the same hash and thus the same signature. So these hashes must be "collision resistant", which means that it must be computationally hard to find pairs of messages having the same hash, even though these pairs exist.

10. Briefly describe the "inference problem" in database security. What is a direct attack? What is an indirect attack? Give an example of a direct attack. (4p)

    - The inference problem is that sensitive information can be derived from insensitive data
    - A direct attack is using a small sample so that information leaks directly
    - An indirect attack combining several aggregrates to infer information
    - An example is creating a database question that asks for the average grade (say) for a group, and selecting the group so narrowly that only one individual is in the group. Since there is only one person, the answer will be the grade of that person.

11. What is the main difference between whaling and phishing? Mitigation of social engineering attacks has to be done through three main fronts: Policy, Awareness and Technology. State one action to be done in each front by the security administrator. (4p)

    - Phishing is targeted randomly at many different people hoping that at least one will fall for the attack. Whaling on the other hand, is a custom-made attack directed at a specific target, typically a high-ranking employee at an organization.
    - Policy: State the rules through a company-wide policy: i.e. "Never click on links sent by external emails". Awareness: Teach common social engineering attacks to all employees. Technology: Authentication, digital signatures, etc...