Written exam in TSIT02 Computer security

14:00–18:00, 11th January 2019

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 **25** points, while grade 4 requires **33** and grade 5 **41** points respectively.

Other information: Answers must be written in English. All questions are designed to return short and direct answers. Overly long answers will not be considered.

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. (1p per item, max 12p)

   (a) Someone obtains your PIN by looking over your shoulder while you are making a purchase with your credit card.

   (b) Your computer is hit by ransomware, and with it, you receive an "offer" to remove it by paying up 150 USD worth of bitcoin.

   (c) All access to your website is routed to a copy of yours, owned by a malicious party, due to DNS cache poisoning.

   (d) A nurse intentionally falsifies patient data to harm the hospital.

   (e) An Internet service provider technical support line is overloaded due to widespread technical problems over the network.

   (f) An e-commerce website's database is attacked by hackers, who get hold of the plaintext list of customers with their credit card information.

   (g) Your password is guessed through an offline dictionary attack.

   (h) The power output of a power plant's turbines is dropped to zero with a carefully crafted worm that was injected in the plant's intranet.

(i) A worm sends the keys you press on your keyboard to an external server.

(j) Your backup data that is stored in the cloud can not be accessed due to problems in Internet connectivity.

(k) Cloud backup data from a company is accidentally modified by an employee with the proper security credentials.

(l) A hacker is able to get some personal data from a client by pretending to be his/her partner over the customer support line of the Internet Service Provider of the client.

2. a) Describe what two-factor authentication (2FA) is. b) A hacker sets up an attack where he/she randomly sends carefully crafted emails containing malicious links to previously well-researched targets. By clicking on the link the target is taken to a fake website that mimics his/her online bank. Simultaneously the hacker tries to log in to the bank using the target's credentials. This asks for the target's 2FA confirmation in their phone, which they then type in the fake website. This 2FA information is then sent to the hacker, who then enters it in the real bank's site, which then allows the hacker to access the target's bank account. What general class of attacks is being used here to trick the target into trying to log to the bank and giving his 2FA information? c) Can improvements in 2FA technology block this type of attack completely? d) What is the best protection against such attacks? (4p)

3. a) What is a botnet? b) Why can a botnet be assembled relatively easily? c) What can be done to minimize the risks new botnets are formed in the future? d) What is the most common type of attack performed by a botnet? (6p)

4. a) Why should only password hashes be stored and not the plaintext password itself? b) Should a slow or fast hash function be used? Why? c) What is salting? d) If x bits are used for the salt, how much larger should the dictionary pre-computed table be? e) Should the salt be random? f) What is the single best way to ensure users are protected against any password attack or leak in the near future? (7p)

5. a) What is the consequence of using short key lengths for encryption algorithms? b) How large is the key-space of a k-bit long key, but when only y (where $y < k$) bits per key are actually random? c) How should the first key exchange between two users take place? d) Why are third-party key servers important? (4p)

6. a) In an online forum why should the text provided by the different users be sanitized? b) What should a programmer be aware of when writing a program in low-level language (i.e. C) regarding user input? c) Why is database security more complex than standard file security? d) What is an inference attack? e) Why is it critical that a patch is installed as soon as it is made available? (6p)

7. a) Name the three possible actions on a file in access control in Unix. b) Which user by default has the highest possible access privileges in Unix and in Windows. c) Why should users be categorized in groups? d) Why is the possibility to quickly revoke privileges a necessity? e) In these cases why can TOCTTOU be an issue? (8p)

Solutions

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. (1p per item, max 12p)

   (a) Someone obtains your PIN by looking over your shoulder while you are making a purchase with your credit card.

   (b) Your computer is hit by ransomware, and with it, you receive an "offer" to remove it by paying up 150 USD worth of bitcoin.

   (c) All access to your website is routed to a copy of yours, owned by a malicious party, due to DNS cache poisoning.

   (d) A nurse intentionally falsifies patient data to harm the hospital.

   (e) An Internet service provider technical support line is overloaded due to widespread technical problems over the network.

   (f) An e-commerce website's database is attacked by hackers, who get hold of the plaintext list of customers with their credit card information.

   (g) Your password is guessed through an offline dictionary attack.

   (h) The power output of a power plant's turbines is dropped to zero with a carefully crafted worm that was planted in the plant's intranet.

   (i) All access to your website is routed to a copy owned by a malicious party, due to DNS cache poisoning.

   (j) Your backup data that is stored in the cloud can not be accessed due to problems in Internet connectivity.

   (k) Cloud backup data from a company is accidentally modified by an employee with the proper security credentials.

   (l) A hacker is able to get some data from a client by pretending to be his/her partner over the customer support line of the Internet Service Provider of the client.

   (a) Information is obtained from you, breach of confidentiality C

   (b) You cannot access your data unless you pay up, availability A

   (c) Your website cannot be externally accessed, availability A

   (d) Patient data is modified, integrity I

   (e) The technical support line is not accesible, availability A

   (f) Customer data is leaked out, breach of confidentiality C

   (g) Your password is discovered, breach of confidentiality C

   (h) The power plant can no longer produce output power, availability A

   (i) Information you type is transmitted to a third party, confidentiality C

   (j) You cannot access your data, availability A

(k) Your data is modified, integrity I

(l) Some of your personal data gets leaked, confidentiality C

2. a) Describe what two-factor authentication (2FA) is. b) A hacker sets up an attack where he/she randomly sends carefully crafted emails containing malicious links to previously well-researched targets. By clicking on the link the target is taken to a fake website that mimics his/her online bank. Simultaneously the hacker tries to log in to the bank using the target's credentials. This asks for the target's 2FA confirmation in their phone, which they then type in the fake website. This 2FA information is then sent to the hacker, who then enters it in the real bank's site, which then allows the hacker to access the target's bank account. What general class of attacks is being used here to trick the target into trying to log to the bank and giving his 2FA information? c) Can improvements in 2FA technology block this type of attack completely? d) What is the best protection against such attacks? (4p)

   a) 2FA is an authentication method that relies on two distinct pieces of evidence, i.e. password and fingerprint.

   b) Social Engineering

   c) Not really, since the target is tricked into providing his extra authentication factor to the hackers.

   d) Educating the users not to click on suspicious links.

3. a) What is a botnet? b) Why can a botnet be assembled relatively easily? c) What can be done to minimize the risks new botnets are formed in the future? d) What is the most common type of attack performed by a botnet? (6p)

   a) It is a network of hijacked devices, typically routers and webcams, that can be controlled to send traffic at a specified target.

   b) Due to devices being mostly unpatched, default passwords, etc...

   c) Build devices having better security features, implement automated patching, ship devices with extra features disabled by default etc...

   d) A (distributed) denial-of-service attack.

4. a) Why should only password hashes be stored and not the plaintext password itself? b) Should a slow or fast hash function be used? Why? c) What is salting? d) If x bits are used for the salt, how much larger should the dictionary table be? e) Should the salt be random? f) What is the single best way to ensure users are protected against any password attack or leak in the near future? (7p)

   a) To avoid direct access to the passwords if the password list is compromised.

   b) A slow function in order to make it harder to pre-generate hash tables

   c) It is the addition of an extra random string to the password before hashing.

   d) 2^x times larger

   e) Yes

   f) Use a long and truly random password.

5. a) What is the consequence of using short key lengths for encryption algorithms? b) How large is the key-space of a k-bit long key, but when only y (where $y < k$) bits per key are actually random? c) How should the first key exchange between two users take place? d) Why are third-party key servers important? (4p)

   a) It is more likely the key can be guessed and the encryption broken.

   b) 2^y possible keys

   c) Via a trusted courier (or a personal meeting)

   d) Key servers can authenticate different users without them having to meet beforehand.

6. a) In an online forum why should the text provided by the different users be sanitized? b) What should a programmer be aware of when writing a program in low-level language (i.e. C) regarding user input? c) Why is database security more complex than standard file security? d) What is an inference attack? e) Why is it critical that a patch is installed as soon as it is made available? (6p)

   a) To prevent malicious code from being run when other users view the forum.

   b) To check for inputs to avoid buffer overruns.

   c) Because the information is contained in the relations, and it is difficult to predict all possible relations in a complex database and how to control access to each of them.

   d) An inference attack is when information is extracted combining many indirect queries.

   e) Most attacks appear shortly after a patch is released (after the hackers have had the time to reverse engineer it).

7. a) Name the three possible actions on a file in access control in Unix. b) Which user by default has the highest possible access privileges in Unix and in Windows. c) Why should users be categorized in groups? d) Why is the possibility to quickly revoke privileges a necessity? e) In these cases why can TOCTTOU be an issue? (8p)

   a) read, write and execute

   b) Root in Unix and Admin in Windows

   c) To simplify access control

   d) If a user should no longer have access to the system, his privileges need to be quickly removed in order to physically blocking him from accessing the files and the system.

   e) After his privileges have been revoked, he can still access the system until his access rights are checked again.