Chapter 2

Emil Maric

October 5, 2015

1. dfdf

1a. Define each of these terms: confidentiality, integrity, availability.

- **Confidentiality:** Preventing unauthorized reading of information.
- **Integrity:** Preventing, or at least detecting unauthorized changes to data.
- **Availability:** Enabling access to data and resources.

1b. Give a concrete example where confidentiality is more important than integrity.
Browser history

1c. Give a concrete example where integrity is more important than confidentiality.
Bank account balance

1d. Give a concrete example where availability is the overriding concern.
Financial Services

2. From a bank' s perspective, which is usually more important, the integrity of its customer's data or the confidentiality of the data? From the perspective of the bank' s customers, which is more important?
From a bank's perspective, integrity is more important. From a customer's perspective, confidentiality is more important.

3. Instead of an online bank, suppose that Alice provides an online chess playing service known as Alice's Online Chess (AOC). Players, who pay a monthly fee, log into AO C where they are matched with another player of comparable ability.

3a. Where (and why) is confidentiality important for AO C and its customers?
Confidentiality is important to protect the financial information of the users.

3b. Why is integrity necessary?
Integrity is necessary so that Alice can ensure the financial information is correct, and that the user's chess ranking is also correct.

3c. Why is availability an important concern?
Availability is important so that Alice can make money from people visiting her site.

4. Instead of an online bank, suppose that Alice provides an online chess playing service known as Alice's Online Chess (AOC). Players, who pay a monthly fee, log into AOC where they are matched with another player of comparable ability.

4a. Where should cryptography be used in AOC?
Cryptography should be used in protecting the user's password and financial information.

4b. Where should access control used?
Access Control should be used for the login page to determine if the entered credentials are correct, and to distinguish between a regular user and site admin. Also to distinguish between a paying customer and non-paying.

4c. Where would security protocols be used?
Security protocols would be used at the login page to securely use the entered information to query the user database to verify

the credentials. They would also be used to setup a secure chess match between two players. Finally, they would also be used monthly to securely credit users' for their subscription.

4d. Is software security a concern for AOC? Why or why not?
Yes, because a flaw in the software security means that that someone could potentially exploit the system to gain access to user's financial information, which would compromise the confidentiality of AOC. Also, a security flaw could potentially change user's stats, which would compromise the integrity of the service. Also, a security flaw could potentially bring the site down, compromising the availability of the site.

5. Some authors distinguish between secrecy, privacy, and confidentiality. In this usage, secrecy is equivalent to our use of the term confidentiality, whereas privacy is secrecy applied to personal data, and confidentiality (in this misguided sense) refers to an obligation not to divulge certain information.

5a. Discuss a real-world situation where privacy is an important security issue.
Privacy is a real-world concern when accessing your finances online.

5b. Discuss a real-world situation where confidentiality (in this incorrect sense) is a critical security issue.
Using your financial information to register for services such as eBay, Amazon, etc.

6. RFID tags are extremely small devices capable of broadcasting a number over the air that can be read by a nearby sensor. RFID tags are used for tracking inventory, and they have many other potential uses. For example, RFID tags are used in passports and it has been suggested that they should be put into paper money to prevent counterfeiting. In the future, a person might be surrounded by a cloud of RFID numbers that would provide a great deal of information about the person.

6a. Discuss some privacy concerns related to the widespread use of RFID tags.
Using an RFID tag in a passport as an example, if someone was near enough to you with an RFID reader, they could read your passport information.

6b. Discuss security issues, other than privacy, that might arise due to the widespread use of RFID tags.
Unauthorized access using RFID tags.

7. Cryptography is sometimes said to be brittle, in the sense that it can be very strong, but when it breaks, it (generally) completely shatters. In contrast, some security features can "bend" without breaking completely-security may be lost as a result of the bending, but some useful level of security remains.

7a. Other than cryptography, give an example where security is brittle.
Login pages for services; if you have access to a user's account, there is usually no further security layers to prevent you from stealing all their information or compromising the integrity of the account.

7b. Provide an example where security is not brittle, that is, the security can bend without completely breaking.
Properly hashed passwords in a database using a unique salt. You have to bruteforce each password individually.

8. Read Diffie and Hellman's classic paper.
Skipped

9. The most famous World War II cipher machine was the German Enigma (see also Problem 10).
Skipped

10. The German Enigma is the most famous World War II cipher machine (see also Problem 9). The cipher was broken by the Allies and intelligence gained from Enigma messages proved invaluable. At first, the Allies were very careful when using the information gained from broken Enigma messagessometimes the Allies did not use information that could have given them an advantage. Later in the war, however, the Allies (in particular, the Americans) were much less careful, and they tended to use virtually all information obtained from broken

Enigma messages.

10a. The Allies were cautious about using information gained from broken Enigma messages for fear that the Germans would realize the cipher was broken. Discuss two different approaches that the Germans might have taken if they had realized that the Enigma was broken.
Use a different cipher and provide false information.

10b. At some point in the war, it should have become obvious to the Germans that the Enigma was broken, yet the Enigma was used until the end of the war. Why did the Nazis continue to use the Enigma?
They either didn't realize it was broken, or they underestimated the compromise. Also, they may have realized that the engima was fully cracked, and decided to use it to provide false information.

11. When you want to authenticate yourself to your computer, most likely you type in your username and password. The username is considered public knowledge, so it is the password that authenticates you. Your password is something you know.

11a. It is also possible to authenticate based on something you are, that is, a physical characteristic. Such a characteristic is known as a biometrie. Give an example of biometric-based authentication.
Finger-based authentication.

11b. It is also possible to authenticate based on something you have, that is, something in your possession. Give an example of authentication based on something you have.
Key card

11c. Two-factor authentication requires that two of the three authentication methods (something you know, something you have, something you are) be used. Give an example from everyday life where two-factor authentication is used. Which two of the three are used?
G-mail uses 2-factor authentication. It uses your password (something you know), as well as sending you a text or e-mail message with another 6 digit key (something you have).

12. CAPTCHAs are often used in an attempt to restrict access to humans (as opposed to automated processes).

12a. Give a real-world example where you were required to solve a CAPTCHA to gain access to some resource. What do you have to do to solve the CAPTCHA?
Creating an account on a website. You have to type in the letters/numbers that appear in the CAPTCHA image.

12b. Discuss various technical methods that might be used to break the CAPTCHA you described in part a.
A program that can read letters/numbers from an image and automatically create the account.

12c. Outline a non-technical method that might be used to attack the CAPTCHA from part a.
Brute force.

12d. How effective is the CAPTCHA in part a? How user-friendly is the CAPTCHA?
Pretty good.

12e. Why do you hate CAPTCHAs?
Sometimes the images suck.

13. Suppose that a particular security protocol is well designed and secure. However, there is a fairly common situation where insufficient information is available to complete the security protocol. In such cases, the protocol fails and, ideally, a transaction between the participants, say, Alice and Bob, should not be allowed to occur. However, in the real world, protocol designers must decide how to handle cases where protocols fail. As a practical matter, both security and convenience must be considered. Comment on the relative merits of each of the following solutions to protocol failure. Be sure to consider both the relative security and user-friendliness of each.

13a. When the protocol fails, a brief warning is given to Alice and Bob, but the transaction continues as if the protocol had succeeded, without any intervention required from either Alice or Bob.
This is neither user-friendly (because the user doesn't know that the transaction failed) nor secure.

13b. When the protocol fails, a warning is given to Alice and she decides (by clicking a checkbox) whether the

transaction should continue or not.
This is user-friendly for Alice, however not for Bob, but ideally the transcation should terminate if the protocol fails.

13c. When the protocol fails, a notification is given to Alice and Bob and the transaction terminates.
This is both user-friendly, as both parties know the transaction failed, and also secure, since the transaction terminates when the protocol fails.

13d. When the protocol fails, the transaction terminates with no explanation given to Alice or Bob.
This is secure, but not user-friendly, since neither Alice nor Bob know that the transaction was terminated.

14. Automatic teller machines (ATMs) are an interesting case study in security. Anderson [14] claims that when ATMs were first developed, most attention was paid to high-tech attacks. However, most real-world attacks on ATMs have been decidedly low tech.

14a. Examples of high-tech attacks on ATMs would be breaking the encryption or authentication protocol. If possible, find a real-world case where a high-tech attack on an ATM has actually occurred and provide the details.
No thanks

14b. Shoulder surfing is an example of a low-tech attack. In this scenario, Trudy stands behind Alice in line and watches the numbers Alice presses when entering her PIN. Then Trudy bonks Alice in the head and takes her ATM card. Give another example of a low-tech attack on an ATM that has actually occurred.
Stealing the ATM machine itself, and breaking it open in a secure and hidden location.

15. Large and complex software systems invariably have a large number of bugs.

15a. For honest users, such as Alice and Bob, buggy software is certainly annoying but why is it a security issue?
Other malicious users can exploit the flaws to compromise Alice and Bob's accounts.

15b. Why does Trudy love buggy software?
Trudy can use the bad software to exploit the system for personal gains.

15c. In general terms, how might Trudy use bugs in software to break the security of a system?
Explained above.

16. Malware is software that is intentionally malicious, in the sense that it is designed to do damage or break the security of a system. Malware comes in many familiar varieties, including viruses, worms, and Trojans.

16a. Has your computer ever been infected with malware? If so, what did the malware do and how did you get rid of the problem? If not, why have you been so lucky?
No never, my computer is the best.

16b. In the past, most malware was designed to annoy users. Today, it is often claimed that most malware is written for profit. How could malware possibly be profitable?
It can send data from your computer to the malicious user, specifically saved financial information.

17. In the movie Office Space, software developers attempt to modify company software so that for each financial transaction, any leftover fraction of a cent goes to the developers, instead of going to the company. The idea is that for any particular transaction, nobody will notice the missing fraction of a cent, but over time the developers will accumulate a large sum of money. This type of attack is sometimes known as a salami attack.

17a. Find a real-world example of a salami attack.
No thanks

17b. In the movie, the salami attack fails. Why?
I never watched the movie

18. Some commercial software is closed source, meaning that the source code is not available to users. On the other hand, some software is open source, meaning that the source code is available to users.

18a. Give an example of software that you use (or have used) that is closed source.
Windows OS

18b. Give an example of software that you use (or have used) that is open source.
Brew

18c. For open source software, what can Trudy do to search for security flaws in the software?
Look at the source code for bugs that are exploitable

18d. For closed source software, what can Trudy do to search for security flaws in the software?
Do a analysis and try to find potential bugs.

18e. For open source software, what can Alice do to make the software more secure?
File bugs for any errors she notices.

18f. For closed source software, what can Alice do to make the software more secure?
Same thing as above.

18g. Which is inherently more secure, open source software or closed source software? Why?
Closed source because the source code is not publicly available.

19. It's sometimes said that complexity is the enemy of security.

19a. Give an example of commercial software to which this statement applies, that is, find an example of software that is large and complex and has had significant security problems.
US health care website

19b. Find an example of a security protocol to which this statement applies.
Heartbleed bug (OpenSSL)

20. Suppose that this textbook was sold online (as a PDF) by your money grubbing author for, say, $5. Then the author would make more money off of each copy sold than he currently does and people who purchase the book would save a lot of money.

20a. What are the security issues related to the sale of an online book?
If it's sold online, one person could buy it and then distribute it online for free

20b. How could you make the selling of an online book more secure, from the copyright holder's perspective?
Use a pay system with a good reputation, such as PayPal. Also, make the book tied in with an account, so it can only be opened in an online app.

20c. How secure is your approach in part b? What are some possible attacks on your proposed system?
Someone could still make a PDF from the book on their own and distribute it that way. It would require a lot of work if there were many pages.