1 Problems

1. Among the fundamental challenges in information security are confidentiality, integrity and availability, or CIA.

   a. Define each of these terms, confidentiality, integrity, and availability.

   b. Give a specific example where confidentiality is more important than integrity.

   c. Give a specific example where integrity is more important than confidentiality.

   d. Give a specific example where availability is the overriding concern.

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 customer, which is more important?

3. Instead of an online bank, suppose that Alice's provides an online chess playing service—Alice's Online Chess (AOC). Players, who pay a monthly fee, log into AOC and they are matched with other players of comparable ability to play chess online.

   a. Where (and why) is confidentiality important for AOC and its customers?

   b. Why is integrity necessary?

   c. Why is availability an important concern?

4. Instead of an online bank, suppose that Alice's provides an online chess playing service—Alice's Online Chess (AOC). Players, who pay a monthly fee, log into AOC and they are matched with other players of comparable ability to play chess online.

   a. Where is cryptography used in AOC?

   b. Where is access control used?

   c. Where are security protocols used?

   d. Is software security a significant concern for AOC? Why or why not?

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 sense) refers to an obligation not to divulge certain information.

   a. Discuss a real-world situation where privacy is the most important security issue.

   b. Discuss a real-world situation where confidentiality (in this sense) is a critical security issue.

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, it has been suggested that RFID tags could be put into paper money, passports, clothing items, and so on. If this occurs, a person could be surrounded by a "cloud" of RFID number that would provide a great deal of information about the person.

   a. Discuss some privacy concerns related to the widespread use of RFID tags.

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

7. Cryptography is sometimes said to be "brittle", in the sense that when used correctly it is very strong, but when it breaks, it 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.

   a. Other than cryptography, give a real-world example where security is "brittle".

   b. Give a real-world example where security is not brittle, that is, the security can "bend" without breaking.

8. Read Diffie and Hellman's classic paper, New Directions in Cryptography [**?**].

   a. Briefly summarize the paper.

b. Diffie and Hellman give a system for distributing keys over an insecure channel (see Section 3 of the paper). How does this system work?

c. Diffie and Hellman also conjecture that a "one way compiler" might be used to construct a public key cryptosystem. Do you believe this is a plausible approach? Why or why not?

9. Without a doubt, the most famous World War II cipher machine is the German Enigma (see also Problem 10).

a. Draw a diagram illustrating the inner workings of the Enigma.

b. The Enigma was broken by the Allies and intelligence gained from Enigma intercepts was invaluable. Discuss a significant World War II event where broken Enigma messages played a role.

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 messages—sometimes the Allies did not use information that could have given them an advantage. Later in the war, however, the Allies (in particularly, the Americans) were less careful, and they tended to use virtually all information obtained from broken Enigma messages.

a. 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

b. 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 fail to realize that the Enigma was broken?

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. The password is "something you know".

a. It is also possible to authenticate based on "something you are", that is, a physical characteristic, or biometric. Give an example of biometric-based authentication.

b. 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.

c. "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?

12. Often it is desirable to limit access to some computing resource to humans, that is, we do not want automated processes to gain access. CAPTCHAs [**?**] are often used in an attempt to limit access to humans.

a. Give an example where you were required to complete a CAPTCHA to gain access to some resource. What did the CAPTCHA require you to do?

b. Outline a technical method that might be used to break the CAPTCHA in part a.

c. Outline a non-technical method that might be used to attack the CAPTCHA in part a.

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

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

i. When the protocol fails, a brief warning is given to Alice and Bob,

but the the transaction continues as if the protocol had succeeded, without any intervention required from either Alice or Bob.

    ii. When the protocol fails, a warning is given to Alice and she decides (by clicking a checkbox) whether the transaction should continue or not.

   iii. When the protocol fails, a notification is given to Alice and Bob and the transaction terminates.

   iv. When the protocol fails, the transaction terminates with no warning given to Alice or Bob.

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

    a. Examples of possible high-tech attack on an ATM would be breaking the encryption or the authentication protocol. If possible, find a real-world case where a high-tech attack on an ATM has actually occurred and provide the details.

    b. "Shoulder surfing" is an example of a low-tech attack—Trudy stands behind Alice in line and watches the numbers Alice presses when entering her PIN, then Trudy steals Alice's card. Give two different examples of low-tech attacks on ATMs that have actually occurred.

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

    a. For Alice and Bob, buggy software is certainly annoying but why is it a security issue?

    b. Why does Trudy love buggy software?

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

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

a. 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?

b. 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?

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

a. Find a real-world example of a successful salami attack.

b. In the movie, the salami attack fails. Why?

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.

a. Give examples of software that you use (or have used) that are closed source.

b. Give examples of software that you use (or have used) that are open source.

c. If some particular software is open source, what could Trudy do to find security flaws in the software?

d. If some particular software is closed source, what could Trudy do to find security flaws in the software?

e. If some particular software is open source, what could Alice and Bob do to make the software more secure?

f. If some particular software is closed source, what could Alice and Bob do to make the software more secure?

g. Which is inherently more secure, open source or closed source software? Why?

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

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

    b. Find an example of a security protocol to which this statement applies.

20. Suppose that this textbook was sold online (as a PDF) by the author for, say, $5. The author would make more money off of each copy sold than he currently does[1] and people who purchase the book would save money.

    a. What are the relevant security issues related to the sale of an online book?

    b. How could you make the selling of an online book more secure, from the copyright holder's perspective?

    c. How secure is your approach in part b? What are some possible attacks on your proposed system?

21. The PowerPoint slides at [**?**] describe a network security class project where students successfully hacked the Boston subway system.

    a. Summarize each of the various attacks. What was the crucial vulnerability that enabled each attack to succeed?

    b. The students planned to give a public presentation at the self-proclaimed "hacker's convention", Defcon 16 [**?**], where they would have presented the PowerPoint slides at [**?**]. At the request of the Boston transit authority, a judge issued a temporary restraining order (since lifted) which prevented the students from talking about their work. Do you think this was justified, based on the material in the slides?

    c. What are "war dialing", "war driving", etc.? What is "war carting"?

    d. Comment on the production quality of the "melodramatic video about the warcart" (a link to the video can be found at [**?**]).

---

[1]Believe it or not...