# Chapter 1

Emil Maric

September 20, 2015

**1.**
**1a.**

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

**1b.** Browser history
**1c.** Bank account balance
**1d.** Financial Services

**2.** From a bank's perspective, integrity is more important. From a customer's perspective, confidentiality is more important.

**3.**
**3a.** Confidentiality is important to protect the financial information of the users.
**3b.** Integrity is necessary so that Alice can ensure the financial information is correct, and that the user's chess ranking is also correct.
**3c.** Availability is important so that Alice can make money from people visiting her site.

**4.**
**4a.** Cryptography should be used in protecting the user's password and financial informaiton.
**4b.** 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.** 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.** 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.**
**5a.** Privacy is a real-world concern when accessing your finances online.
**5b.** Using your financial information to register for services such as eBay, Amazon, etc.

**6.**
**6a.** 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.** Unauthorized access using RFID tags.

**7.**
**7a.** 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.** Properly hashed passwords in a database using a unique salt. You have to bruteforce each password individually.

**8.** Skipped

**9.** Skipped

**10.**
**10a.** Use a different cipher and provide false information.
**10b.** 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.**
**11a.** Finger-based authentication.
**11b.** Key card
**11c.** 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.**
**12a.** Creating an account on a website. You have to type in the letters/numbers that appear in the CAPTCHA image.
**12b.** A program that can read letters/numbers from an image and automatically create the account.
**12c.** Brute force.
**12d.** Pretty good.
**12e.** Sometimes the images suck.

**13.**
**13a.** This is neither user-friendly (because the user doesn't know that the transaction failed) nor secure.
**13b.** This is user-friendly for Alice, however not for Bob, but ideally the transcation should terminate if the protocol fails.
**13c.** This is both user-friendly, as both parties know the transaction failed, and also secure, since the transaction terminates when the protocol fails.
**13d.** This is secure, but not user-friendly, since neither Alice nor Bob know that the transaction was terminated.

**14.**
**14a.** No thanks
**14b.** Stealing the ATM machine itself, and breaking it open in a secure and hidden location.

**15.**
**15a.** Other malicious users can exploit the flaws to compromise Alice and Bob's accounts.
**15b.** Trudy can use the bad software to exploit the system for personal gains.
**15c.** Explained above.

**16.**
**16a.** No never, my computer is the best.
**16b.** It can send data from your computer to the malicious user, specifically saved financial information.

**17.**
**17a.** No thanks
**17b.** I never watched the movie

**18.**
**18a.** Windows OS
**18b.** Brew
**18c.** Look at the source code for bugs that are exploitable
**18d.** Do a analysis and try to find potential bugs.
**18e.** File bugs for any errors she notices.
**18f.** Same thing as above.
**18g.** Closed source because the source code is not publicly available.

**19.**
**19a.** US health care website
**19b.** Heartbleed bug (OpenSSL)

**20.**
**20a.** If it's sold online, one person could buy it and then distribute it online for free
**20b.** 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.** 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.