Assignment 1

1. **Among the fundamental challenges in information security are confidentiality, integrity, and availability, or CIA.**
   1. Define each of these terms: confidentiality, integrity, availability.

Confidentiality is to keep information private from others and only allow the authorized people to be able to see that information.

Integrity is to be able to prevent or detect unauthorized people to change information that they are not supposed to change.

Availability is to allow people to access their data fast and easy whenever they need it.

* 1. Give a concrete example where confidentiality is more important than integrity

An example would be an email service provider; I think email providers would have to focus mostly on confidentiality, because keeping things private is the most important thing about using email, while integrity is still important, but keeping customer’s data secure is even more important.

* 1. Give a concrete example where integrity is more important than confidentiality.

An example would be banks, Keeping data integrity in a bank is very important, because if not, people could things like changing balances of the bank accounts and this could be a major chaos for the bank, while confidentiality will just means that they will displease some of their customers.

* 1. Give a concrete example where availability is the overriding concern.

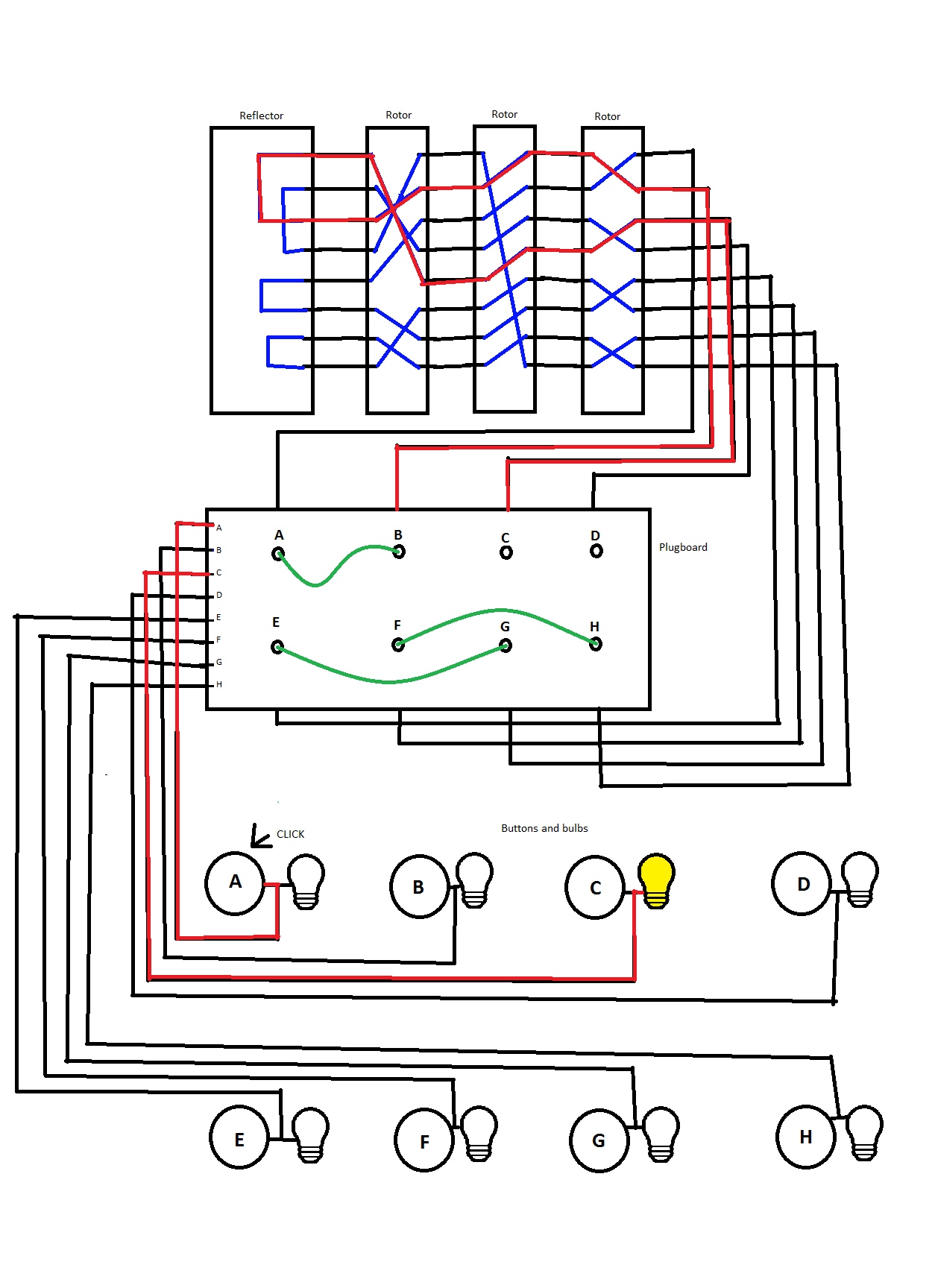
An example would be financial companies, because the stock market fluctuates really fast, it is very important to have good availability, because if not, customers will leave because of slow system and they would not be able to make stock trades fast enough.

1. **The most famous World War II cipher machine was the German Enigma**
   1. Draw a diagram illustrating the inner workings of the enigma

Sources:

<http://enigma.louisedade.co.uk/howitworks.html>

<http://en.wikipedia.org/wiki/Enigma_machine>



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

I think the Enigmas messages played a major role in the Second Battle of El Alamein, in this battle the Allies won because they had the advantage of decrypted enigma messages, and they were able to know where the Axis are, their supply position, force disposition and intentions. This advantage gave the Allies the upper hand because they knew what the Axis’ strategy and how to counter them.

1. **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.**
   1. It is also possible to authenticate based on something you are, that is, a physical characteristic. Such a characteristic is known as a biometric. Give an example of biometric-based authentication.

Examples of biometric-based authentications are eye scans, finger print scans, voice recognition, facial recognition, etc.

* 1. 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.

Examples of authentication based on physical items are USB authenticators, smart cards, RSA SecurID, etc.

* 1. 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?

Example from everyday life that uses two-factor authentication is Banks and Video games from Blizzard. Some banks provide the option to allow customers to get something similar to the RSA SecurID that generates a new sequence of number every 30 seconds or so. Another example is the video game company Blizzard, after numerous hacks, the company required users to have an physical or mobile authenticator in order to perform money related transactions on their account.

1. **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.**
   1. 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 solution is simple and it considers favors the user-friendliness side more than the security side, it does warn the user of protocol failure but it can be easily ignored by the user, without giving fair warning of what can happen if the transaction continues.

* 1. 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 solution in the balance between security and user-friendliness, when the protocol fails, this solution requires forces users to decide whether to continue the transaction or not, making it impossible to ignore and being able to warn the users.

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

This solution mainly focuses on security, and does not consider user-friendliness; it does not allow people to continue even though they understand the consequences of the protocol failure, which is very user-unfriendly.

* 1. When the protocol fails, the transaction terminates with no explanation given to Alice or Bob.

This solution focuses on security but it is also very user-unfriendly. This solution can be very secure, but users will not understand what is happening and will mostly frustrate any user that experience protocol failure.

1. **Large and complex software systems invariably have a large number of bug.**
   1. For honest users, such as Alice and Bob, buggy software is certainly annoying but why is it a security issue?

Buggy software could be a security issue for Alice and Bob, because it could allow intruders to take advantage of the bug and be able to break through confidentiality securities and also to be able to impersonate Alice and Bob and use their data.

* 1. Why does Trudy love buggy software?

Trudy loves buggy software, because Trudy is an intruder and to be able to hack into the server or other people’s credential, it is easier if the software is buggy and to be able to take advantage of those bugs.

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

The way to break the security depends on the types of bug, if a bug allows Trudy to see non-encrypted information, then the bug itself allows Trudy to break the security, another example would be “Heartbleed” with the bug, intruders could extract the private encryption key from the server and then use it to decrypt data between the user and the server.

1. **In the movie Office Space [223], 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.**
   1. Find a real-world example of a salami attack.

In 2008 Michael Largent wrote a program to open accounts like Google checkout, E\*Trade, Charles Schwab and many other companies, his method is to make as many account as he could and then verify those accounts by using his back account, by doing this, companies will deposit amounts from 1 cent to 2 dollars into Michael’s account. Michael’s program was able to create over 58 thousand accounts and earned him from $40,000 to $50,000, but he was arrested.

Source: <http://www.academia.edu/2525315/Salami_Attacks-_Collect_the_round_off_technique>

* 1. In the movie, the salami attack fails. Why?

The salami attack fails because the programmer had a bug and he wrote the wrong decimals ending up taking too much money from the company and they are in trouble of getting caught.

**Keystroke sniffer** – In this article, the author Bryan Cockfield introduces the Keystroke sniffer “KeySweeper” that is made by Samy Kamkar. Kamkar explains the hardware that is needed to build the KeySweeper that is camouflaged as a USB wall charger, the device works by receiving 2.4Ghz packets from a Microsoft keyboard, decrypt the packet to know the key and sends that information using mobile network either through a text message or the internet. Apart from being camouflaged as a wall charger, this device also includes a lithium battery that can keep the device powered on to keep sniffing keystrokes even if it is disconnected from the wall.

**EBay asks 145 million users to change passwords after cyber-attack** – On May 21st of 2014; eBay has admitted to being hacked three months ago some customer data has been compromised, therefore they are asking their customers to change their passwords. The hackers of this event are still unknown and the compromised data includes email addresses, encrypted passwords, birthdates, mailing address, etc. EBay only admits that a large number of accounts have been compromised, but refuses to tell how many. One of the main issues is that the compromised data does not only affect eBay, but also accounts from other popular services that uses the same login credentials. The hackers performed this hack by gaining login credentials from eBay employees, which allowed them to get into the company’s network.

**Regin** – Regin is a virus/malware that have been going through computers around the world for around six years. This virus can be compared to the “Stuxnet”, but the difference is that Stuxnet was created with the purpose of spying on the Iranian nuclear program, while Regin’s purpose is still unknown and their creators still remain a mystery. Regin is not a normal virus like others that try to steal credit card information or any other information; Regin uses different types of encryption, modular structure making it very difficult to know what the virus is doing. The clues we have is that the virus is mostly found in Russia and Saudi Arabia, and it is used to gain intelligence by spying on Private and individual small businesses, telecoms backbone, hospitality, airlines, etc.