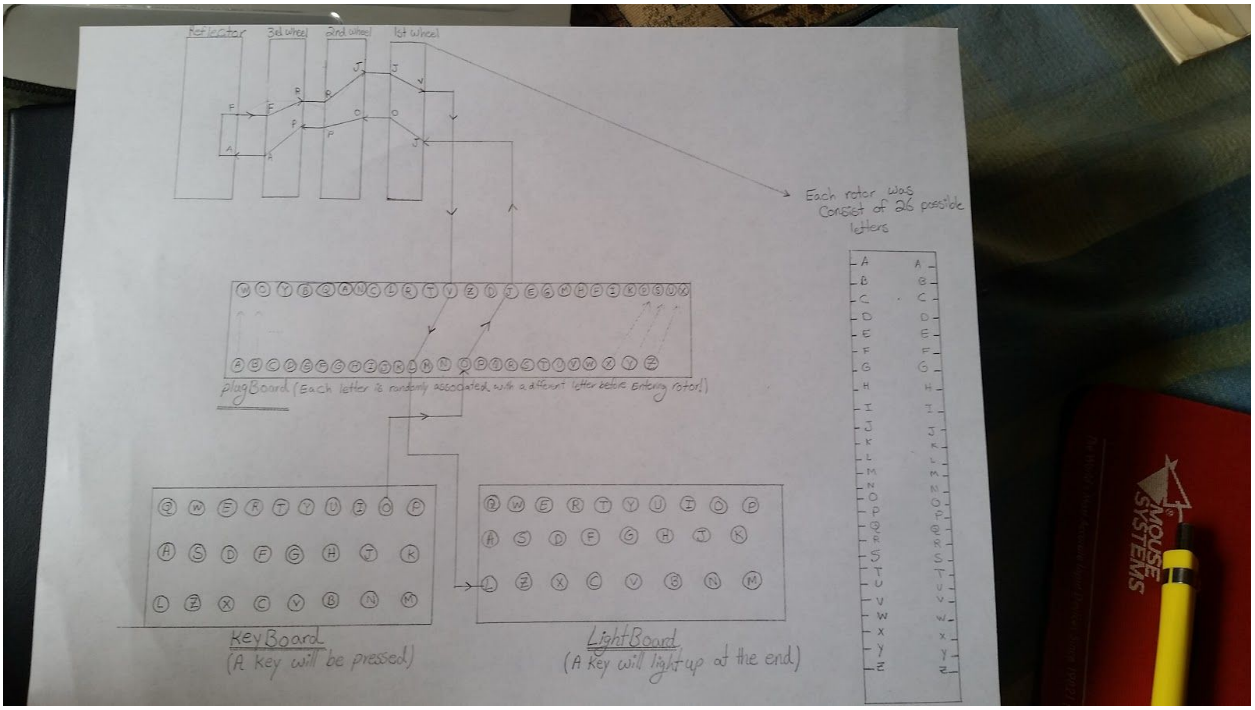
Amir Radman
CS 166
MW 18:00 - 19:15

Homework # 1

9)


Reflector
3rd wheel
2nd wheel
1st wheel
F
F
R
R
J
J
V
A
A
P
P
O
O
J
Each rotor was Consist of 26 possible letters
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
W O Y B Q A N C L R T V Z D J E G M H F I K P S U X
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
plugBoard (Each letter is randomly associated with a different letter before Entering rotor!)
Q W E R T Y U I O P
A S D F G H J K
L Z X C V B N M
KeyBoard
(A key will be pressed)
Q W E R T Y U I O P
A S D F G H J K
L Z X C V B N M
LightBoard
(A Key will light-up at the end)

Process : After pressing a letter, that specific letter is associated with one specific other letter (e.g A → T, V → G), then the associated letter is entered into the Rotor system. Each rotor is consist of 26 number, each being a letter. Each time, the letter enters the rotor, it exits the previous rotor and enters the next one as a different number, following a completely randomized pattern. At the end it hits the reflector, changes to a different letter and again follows the same procedure going back. At the end of the process, the path's projection will light up a different letter in the lightBoard than the one pressed in the main keyBoard.

b) From around 1940 onwards, a team at Bletchley Park(including Alan Turing) cracked the Enigma messages to determine the movement of the German U-Boats and where they were heading and their plan of attack. Using this knowledge, the British were then able to direct their ships away from the danger. It is speculated that breaking the Enigma code allowed the British to shorten WWII by approximately 3-4 years.

Source :
http://www.iwm.org.uk/history/how-alan-turing-cracked-the-enigma-code

11)

a. An example of biometric-based authentication would be using fingerprint. Often times when an individual is requesting to obtain an official document such as green card, drivers license, etc, a fingerprint will be used to uniquely associate that as credentials to that individual.
b. An example of authentication based on something you posses would be obtaining boarding ticket at the airport using barcode sent to your email. Another example would be swiping credit card in the bank for a transaction as a way of authenticating yourself.
c. An example of two-factor authentication would be paying by credit card. When you pay with credit card, first you swipe the card which is authenticating using something I have and then I have to sign it. Signature although is not directly authenticating based on what I am, it is a form of biometric authentication.

13)

a.

Looking at this situation from the convenience point of view is relatively convenient for both Bob and Alice, considering no additional steps needs to be taken to ensure their task is completed without any interruption or delay. However; looking at the security aspect of it, it is insecure since Bob and Alice will not be able to intervene the transaction until the end. In a case of fraud for instance, if Alice and Bob are not able to stop the transaction when the warning is displayed, their information could be exposed to the hacker. (Most Convenient - Least Secure)

b.

In this case, it is slightly inconvenient for Alice to go through the transaction by having to go through the transaction. However; in this situation, Alice is given an option to terminate the transaction and understands there is a possible risk continuing. Although this solution causes inconvenience, it is a good tradeoff for the security measures it provides.(Less Convenient - More Secure)

c.

In my opinion, this situation is extremely inconvenient for both Alice and Bob because it prevents them from completing their transaction. However; if stops the possible exposure of their information to unauthorized individuals caused by protocol failure.(Least Convenient - Most Secure)

15)

a.

Existing bugs in software systems are security issues because it could problems in situations where security is a top priority for the user. For instance, in a situation where a buggy system is supposed to get the password in * format, but instead it would display it in plaintext. That could expose her password to a hacker.

b.
Trudy loves buggy systems because it provide him with more opportunities/loopholes In the code/system so he could take advantage of them and gain access to Alice's and Bob's private information.

c.
A bug in a software could provide Trudy with an opportunity to gain access to the software's database. As a result, he can gain unauthorized access to their system and use their information or take complete control over their system.

Articles Summary

Keystroke Sniffer

http://hackaday.com/2015/01/14/keystroke-sniffer-hides-as-a-wall-wart-is-scary/

This article introduced a device(USB Wall wart-style) that connects to an outlet and it discovers Microsoft wireless keyboard keystrokes and it sends them live through SMS. This device is primarily consist of RF chips, a lithium battery, a USB charging circuit. This device has the capability of detecting the Microsoft keyboard keystrokes and sends them through SMS. In addition, not only the device works when connected to the wall, it also works with the lithium battery when disconnected from the outlet

EBay asks 145 million users to change passwords after cyber attack

http://www.reuters.com/article/2014/05/21/us-ebay-password-idUSBREA4K0B420140521

This article reports an attack on a hacking case against eBay. The company's database containing their online users' sensitive information, such as e-mail addresses, encrypted passwords, and mailing addresses were compromised by an unknown hacker on May 2015. The company urges its users to change their online passwords immediately and, though no evidence of fraud or attempts on hacking into PayPal, to stay aware for possible frauds in the future. This attack on eBay is particularly risky for online users. If the hacker manages to unscramble encrypted passwords they stole from eBay, they could easily use automated software to search other popular sites, such as Facebook and online banking sites, to see where else the password is used. For this reason, eBay stresses on its users to change their passwords and stay alert. This attack also caused eBay's share to momentarily drop in the market.

Regin
http://money.cnn.com/2014/11/23/technology/security/regin-malware-symantec/index.html

“Regin” is a new type of malware detected as a serious threat by Symantec, the company that created Norton Antivirus. This sophisticated malware is installed on company computers around the world and searches through a person’s traveling history/records, such as its airline information and hotel room numbers. It also hacks into a person’s telecommunication devices to see who s/he is talking to. It is a very complex malware that is well-concealed with layers of encryption and various methods to communicate with the hacker. This malware seems to be installed in computers around the world, particularly in countries such as Iran, Russia, and Saudi Arabia.

================================THE END=================================