Valerie Angulo

Practical Computer Security

Spring 2018

1. Equifax Breach 2017:

The threat was that attackers could access data by exploiting an unpatched flaw in the web application building tool Apache Struts, the vulnerabilities were the flaw in Apache Struts (technical failure) along with taking too long to fix this flaw (human error) and the attack was that hackers were able to use this vulnerability to take control of the website and gain access to peoples personal data from May 13 to July 30.

The major consequence of the attack is that hackers had access to the personal data (name, birth dates, address, social security number, and some drivers licenses) of 145.5 million people, leaving them at risk for identity theft and credit fraud. Consequently, the Equifax CEO, chief information officer and chief security officer have all retired after the attack and those impacted had to freeze their credit.

This act is a violation of confidentiality, since personal data was accessed by unauthorized parties. From this incident, we've learned that if a technical failure is detected, it should be fixed as soon as possible. The attack occurred between May and June, 2 months after the flaw had been disclosed. Communication security could mitigate an attack like this because all of the data would be encrypted.

Uber Data Breach:

The threat was that intruders accessed Ubers web account and instead of disclosing the attack, Uber paid off the attackers to delete the data and keep quiet about the breach. The vulnerability was that user data was stored unencrypted and that the username and password for Ubers web account containing important personal data was on Ubers GitHub account. Two attackers accessed the stored data on Ubers Amazon Web Services account by obtaining login credentials found on Ubers GitHub account. The data (name, email address, phone number, and names and numbers of drivers licenses of 600,000 drivers in the US) of 57 million users and drivers was compromised. Two employees responsible for not notifying those affected by the breach left the company. This attack is a violation of confidentiality, because attackers accessed data that they were unauthorized to access. Data should be encrypted and username/passwords should not be left easily found or written down in plain text, and definitely shouldn't be uploaded to public sites. Security controls that could’ve helped the company to prevent such an attack would be communication security such as encryption and administrative controls to manage usernames and passwords more effectively.

NHS Cyber Attack:

The threat was that the NSA knew about the EternalBlue exploit (which gives access to all computers using Microsoft Windows) and didn’t tell Microsoft about it because they wanted to take advantage of it for their own work, and that attackers could access/find out about the exploit in Windows and utilize it for malicious purposes. The vulnerabilities were Window’s Server Message Block protocol being able to be exploited and that older versions of the system weren’t patched to prevent this exploitation, and that Microsoft didn’t know about the vulnerability. The attack was a ransomware cryptoworm called Wanna Decryptor that was spread through phishing emails with attachments that affected those with older versions of Windows by encrypting the users files and demanding payment in bitcoin to decrypt the files.

The attack impacted the NHS, hospitals, FedEx, phone companies and other high profile companies around the world. There were over 200,000 victims and more than 300,000 computers in 150 countries were infected. This attack was a violation of confidentiality, integrity and availability. Users files and data were accessed by parties other than the user, the data was modified through encryption and users were prevented from accessing their data. Prevention is the best form of defense against attacks, preventative security controls is the biggest security control in mitigating an attack. Always keep your software updated, and make sure you have good anti-virus software as well. You should also be cautious when opening file attachments from unknown senders and be more aware of where your emails are coming from and make sure you only download from official sources. Everyone is vulnerable to cyber attacks, even government organizations, so it is best to be as preventative as possible.

2. One real-world attack that exploited the vulnerability associated to the principle of psychological acceptability is a recent cyber attack on parliamentary user accounts to gain access to user’s e-mails. The users that were targeted were Lords, aides, staff and other members of Parliament. This attack was carried out by brute force to guess user’s passwords to their e-mail accounts and took advantage of user’s tendencies to have predictable passwords, such as the same password with minor variations. The attack was caught early on and stopped. However, login details of more than 9,000 people were collected from sites like LinkedIn, MySpace etc. but it is unknown how many e-mail accounts were compromised.

Website: http://www.independent.co.uk/news/uk/home-news/parliament-cyber-attack-mp-email-accounts-houses-commons-politicians-security-police-a7806456.html

I believe psychological acceptability can be applied in the design/operation of a system. Psychological acceptability is a principle of human action, a system can be put into place to safeguard data but people will always find a way around the system if it is too cumbersome. Therefore, a system shouldn't be too much of a hassle to use, otherwise it will not be operated securely. Systems should be made with a balance between being secure and having the security measures be an acceptable level of effort for its users.

3. I believe human fallibility is the leading cause for continuing security breaches, especially for preventable ones. People either don't know how to implement security measures properly or don't want to because it is too time consuming. I agree with Ross Anderson when he says that "instead of worrying about what might possibly go wrong, we need to make a systematic study of what is likely to [go wrong]". By worrying about possibilities, the security systems become very complex, and there aren't enough qualified people to manage these systems effectively. If what is likely to go wrong is focused upon, there would be clearer and more effective corrective methods. However, Anderson believes that to make security systems more effective, programmers jobs should become more involved rather than easier. I believe the system should make the security programmers job easier because I believe that human error and poor implementation of security products is what is most harmful. By making the systems easier to operate, we don't have to be as dependent on the skill level of the people who set up the system. I think it would take too much time and there wouldn't be enough qualified people for all the security measures that need to be implemented, therefore making systems clearer and easier to operate, thus lessening human fallibility, would probably be more efficient in increasing security measures.