# Assignment 2

## Cybersecurity

Cybersecurity is the act of securing digital data and computer systems. Cybersecurity is usually guided by three main factors - confidentially (secrecy), integrity and availability.

Confidentiality (secrecy) relates to the storage of sensitive information, such as personal information, payment details or any other sensitive data. Measures are taken to ensure information is stored securely and only viewable by authorized users or individuals. Malicious threats involve man-in-the-middle attacks, social engineering or access by unauthorized third parties.

Integrity involves ensuring only authorized people have rights to access, move, delete or modify data. Measures must be taken to ensure the users or individuals accessing the data are authorized and have the necessary rights to make such changes or view such information. Current technologies include the encryption of data during transit, use of user access controls and technologies such as checksums so end-users can check the integrity of the data received. Malicious threats involve the exploitation of invalid user permissions, avoiding of integrity checks (direct access) or use of another user’s information.

The last factor is Availability - being able to access the data you are authorized to access. In a general sense, availability is ensured through redundancy methods such as RAID arrays, failovers, etc. In a cyber security sense, threats such as distributed denial of service (DDoS) attacks must be considered.

So in a sentence cybersecurity is protecting sensitive digital information from cyberthreats and these cyberthreats can take many forms such as, malware, ransomware, phishing and exploit kits to stop these kinds of threats governments and enterprises use multiple security prevention techniques such as anti-virus programs on end devices, secure firewalls on network devices, high security programs and cybersecurity training for employee’s

At this moment in time our greatest technology against cyberthreats is to train the end user on how to identify the most common cyberthreats which are phishing e-mail with links to download malware or lead to an infected website, leaving your computer unlocked and unattended and having a complex password.

As for computer technologies, we have anti-virus packages, spam-filters, software and hardware firewalls, encryption, etc. The one thing that lets all these technologies down is that they are all controlled by human security engineers which can’t be updated as soon as a vulnerability is find in the security solution.

There is a new advancement being developed for cybersecurity which is deep learning. This will eliminate the need for human interaction when a vulnerability is found in a system, a security engineer will not have to patch the vulnerability as the deep learning advancement will allow the software to patch the system on its own. This is could Context-Aware Behavioural Analytics.

This is achieved by using deep learning methods of processing information in the computer. Deep learning takes the concept of the human brain and transfers it to the computer process using a technic called “neural networks” where a programmer will feed information in to the program with different outcomes E.G am I hungry if the answer is yes then how much money do I have determines the place you eat at. If the computer processes the question 1000 time with multiple outcomes it can learn what the correct answer or most beneficial answer is.

The deep learning technology has only been available since the advancement in computing power an example of this is the intel 2nd gen CPU being optimized for in the kernel for “intel MKL-DNN” intel Math Kernel Library for deep neural networks. Deep learning takes a lot of computer processing time as it needs to calculate all the different scenarios and previously this was not available.

Other technology that will benefit from deep learning is bio security as deep learning doesn’t need to know the features of a person’s face but will save it into a database and make up the structure of the end users face that can determine the best feature of the end users face individually. This gives great advantage for bio security as each end users features will be defined differently. This has not been possible until now as bio technologies are getting with more advanced cameras and sensors

Deep learning will like to have huge as it will allow computer systems to protect themselves against cyberthreats without having to wait for the cybersecurity engineers to develop a patch for the vulnerability.

The changes this will have will be very impactful as it will remove the need for “zero day patches” and remove the need for a systems administrator to monitor that their security systems have to be always up-to-date. Deep Learn could even fix a flaw in a routers firewall as it would locate where the entry of the attack started a correct it.

A personal experience that I had was in 2016 when A client’s files were crypto lockered. The attacker had kept the files encrypted and demanded payment for it to be decrypted. With deep learning, this sort of action could have been detected before it happened. It could have saved the client a lot of time in trying to restore their files from a backup and losing a whole days work at the same time.

This will affect lots of I.T professional because it will remove the need for security engineers to spend time fixing vulnerabilities and lead to downsizing software security departments due tp the less need of the engineers that will have to maintain the deep learning algorithm.

This could affect me personally by knowing that when I am using my computer, I am always going to be secured. This and including using cloud storage or browsing the internet as many people before me, may have already encountered this vulnerability on the service and had the anti-virus software/firewall patched to stop you using the service or running the infected code.

Overall, deep learning is very beneficial to everyone. Given the cases that are raised in cybersecurity, people nowadays require more protection and with this sort of technology it will be helpful in reducing frauds and any cyber crime that is around there.

References :

<https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security>

<https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html>

<https://umbrella.cisco.com/blog/2013/10/08/top-ten-important-cyber-security-tips-users/>

<https://www.youtube.com/watch?v=bPVaOlJ6ln0>

<https://www.ecpi.edu/blog/new-cybersecurity-technologies-what-is-shaking-up-the-field>

<https://resources.infosecinstitute.com/artificial-intelligence-impact-cyber-security/>

<https://software.intel.com/en-us/articles/intel-processors-for-deep-learning-training>

<https://towardsdatascience.com/decoding-deep-learning-a-big-lie-or-the-next-big-thing-b924298f26d4?gi=51389740879>