Jack Bell Report On Cyber Security

Written on 30/06/2022 – 14/07/22

Student number = S3966999

What does it do? (600 words) What is the state of the art of this new technology? What can be done now? What is likely to be
able to be done soon (say in the next 3 years)? What technological or other developments make this possible?

Cyber security covers all aspects of IT, including devices such as:

PC, Laptop, Smartphone.

Network Infrastructure.

Servers/Cloud Computing.

Physical storage of digital information on CDs, USB, and Internal drives.

Cyber security must cover all 7 layers of the OSI framework (Check Point, 2022), while also ensuring and educating the users of such systems to have due diligence regarding passwords and access keys, (Login details) for if they become compromised then the whole system will be put at risk.

Cyber security is an industry that employs approximately 1 million people worldwide and ~30000 in Australia. (Cisco-Portal.Com Team, 2021)

Recent cyber security attacks are generally a mixture of social engineering and abuse of known exploits in systems. such as email phishing attacks from black hat hackers. These attacks will often display threatening messages to the users saying if you don’t install this malware, you would be locked out of your computer (Sujata, 2021).

On offensive cyber security:

The state of the art in cyber security is Machine learning (Kirandeep Kaur, 2021). This could be used to bypass and dismantle cyber-security systems faster than most prevention methods and detection tools can keep up with.

On defensive cyber security:

A method of security is to defend a system by comparing predictive logic against behavioral signals from an external source that suggests a threat. Machine learning algorithms are being employed to discover harmful network traffic. They are called Intrusion Detection systems (IDS) (Check Point, 2022).

Currently, in cyber security, the best way to secure information stored on a digital device is to ensure that network infostructure is correctly configured, and physically secured, users are educated on the potential risks and permissions/passwords are correctly assigned (Bradly M, 2021).

When configuring devices use a strong password and change the default settings. It is also essential to avoid outdated and insecure protocols such as telnet and WPA within sensitive environments.

Physical security is ensuring that network devices and infrastructure are behind locked doors and that only authorized users are granted access with passwords via wireless or cable.

Another major exposure point for IT environments is the users themselves. As the consequences of security breaches have increased in frequency and consequence, the industry has put in place many measures to mitigate the risks. As back-end security has improved, malicious actors have moved their attention to the most vulnerable component in any system, the users. All administrative controls have one major flaw, the need for human access. In a 2016 study, 93% of data breaches were attributed to human error (Evans. M et al pg .3 table. 1 [https://onlinelibrary.wiley.com/doi/epdf/10.1002/sec.1657]). It is therefore essential that users are educated on attacks they may encounter, and given the training and tools to identify and avoid threats.

The WIFI password is not common knowledge in the office/workplace and only the network administrator/authorized personnel know the WIFI password so that someone cannot ask anyone for the password and gain admin access to the whole network.

In the Australian defence force, they use a cloud-based wide area network (WAN) network that is secured to exchange secret information (Microsoft News Center,2020)

Going forward in cyber security, nations are now performing cyber-attacks against other nations, in acts of aggression or war which can also be called a new military strategy (Donghui, 2016).

Cyber-attacks are becoming commonplace, such as what happened in Ukraine by Russia in 2022 before war broke out a cyber-attack was performed to cripple Ukraine's economy and military (James Pearson,2022).

In peacetime, the government of North Korea frequently performs cyber attacks against South Korea as a new military strategy (Donghui, 2016).

Based on these developments Cyber security attacks will soon be able to perform fast, easy effective attacks against computer systems on small mobile devices like in the game series "Watchdogs" (Jill Scharr, 2014).

In the game, a city-wide operating system "ctOS" operates many electronic devices such as ATM, Traffic lights, and security cameras, and stores the residents personal information such as bank cards, address, age, and occupation, creating a large network containing sensitive personal information, the protagonist(Aiden) an individual who breached/hacked the ctOS system this allows him to alter the networks devices, traffic lights, for example, to change while in a high-speed chase with authorities and being able to walk up to any ATM in the city and withdraw money at a victim/NPC expense (Jill Scharr, 2014).

These developments could cause completely automated cyber-attacks without the stationary computer by putting in some basic input of what you want into a tool or set of tools that enables fast and easy cyber-attacks for people with minimal computer knowledge. This would be possible through machine learning and clever application with a streamlined approach (Jill Scharr, 2014).

An example of the above is an extremely small brute-forcing device to attack a WIFI password and crack within seconds by imputing the network SSID, you could achieve this by quantum computers having extreme computing power than binary computers thus cracking hashed passwords in seconds (Kirk McElhearn, 2020).

In the near future, quantum computers and their applications regarding their computational power will make many current protocols obsolete, and methods of encryption a large part of cyber security to also become obsolete, foundations of network working such as the OSI layers will most likely need to be completely reworked (NIST, 2016).

Manufacturing technologies could improve causing more transistors in a smaller space possible, this could cause vast increases in computational capability, even if quantum computers do not become the future, then this development could emulate the same effect (Lawrence Berkeley, 2014).

Soon with AI technology there will be a potential for AI technology to replace radio operators with Artificially intelligent Radio operators. These would be vastly superior to the human type in a way that self-driving cars are safer than human drivers due to computers never losing focus (Techopedia, 2022). The application of this in cyber security is that computers can be hacked, unlike humans.

What is the likely impact? (300 words) What is the potential impact of this development? What is likely to change?

people will be most affected and how? Will this create, replace or make redundant any current jobs or technologies?

The potential impact of easy-to-use small mobile devices for cyber-attacks, this development would cause the need to create new ways of building systems and applications to be able to deal with these devices carrying out cyber-attacks. This in turn would cause a significant need for security experts and designers to create more secure protocols, encryption algorithms to ensure that cyber security can be maintained, also being able to function correctly with a new age of hackers and security risks(Norwich University, 2021).

In the next 3 years the use of the cloud and its many current and potential applications and potential security risks to cyber security, experts will have to figure out and come up with methods to allow for cyber security to be maintained (Zainab Al Mehdar, 2018). Cloud-based applications such as Drobox and google drive, cloud-based networks and many other similar applications and networks are used by lots of companies today store sensitive information in these as the future of the cloud becomes more embedded in day-to-day life and business.

Cheap long-range high-gain antennas could also become a thing as manufacturing techniques improve along with new innovative software, essentially shrinking the distance that a cyber-attack could occur on a network, this has both civilian and military applications (Jenny List, 2020).

This application regarding antennas could potentially change an entire military core of signals in the ADF could go from the command post to command post creating a network, to an extremely developed command post with extremely powerful signal equipment in Canberra, combine that with AI radio operators you have changed an entire core in the military. These deployments regarding signals would be very far off into the future though >50 years at least (Jill Scharr, 2014).

The above developments will change the job of cyber security, network administrators, data entry workers, and office workers, all jobs were people who work with a network worth securing from cyber-attacks because sensitive information is stored on the network, and transmitted to and from around the world.

How will this affect you? (300 words) In your daily life, how will this affect you? What will be different for you? How might this affect members of your family or your friends

In my daily life cyber security matters to me because I use a computer for many functions in my current jobs (computer Technicon, personal trainer, UNI student) such as sending invoices and storage of information that is sensitive, being able to save UNI work for later and build off previous saves. This would enable me to fix something after being submitted because I have a copy of this report, for example, if I had a security breach say all my files got deleted then I would have serious work output issues, for example, having to do this whole report again and lose all or a lot of retained information, that is not externally backed up.

Cyber security as an industry also affects my job prospects because I am looking to gain employment in cyber security via UNI studies and my cert 4 in cyber security if something big happened in cyber security such as a ground-breaking invention, then I would have to be familiar with this new technology such as quantum computers making WPA2 networks obsolete (NIST, 2016).

Cyber security affects family members as well because that’s where they would store memories in the form of digital photos these photos could be on a cloud or a local device. Family members also store personal information such as a photo of a birth cert and driver’s license which could in the wrong hands be used for identity theft (Sujata, 2021).

Cyber security also affects a company’s reputation, the April 2021 Facebook Breach where users’ birthdates, phone numbers, and passwords were leaked to hackers, exposing personal information and causing people to distrust Facebook changing some people’s behaviors about what they share when using Facebook (Kate O'Flaherty, 2021).

In conclusion, as technologies advance it will become easier and cheaper for the people/organizations who are performing powerful cyber-attacks. It will also become more and more commonplace, previous methods of securing networks such as passwords could become obsolete, though passwords are an easy and very useful tool for programmers and network administers they do not completely secure a system form potential hackers. These issues are duplicated with encryption.

References

Cisco-Portal.Com Team, 2021, How Many Cybersecurity Jobs Are There? - CISO Portal, Retrieved 05/07/2022.

Kirandeep Kaur, 2021, Role of Machine Learning in Cyber Security Retrieved 14/07/2022.

Sujata, 2021, Social Engineering Attacks, Retrieved 09/07/2022.

Check Point, 2022, What is an Intrusion Detection System (IDS), Retrieved 09/07/2022.

Bradly M, 2021, Why You Should Change Wi-Fi Network Default Passwords, Retrieved 08/07/2022.

Mark Walker, 2017, Cable's Role in Cybersecurity, Retrieved 09/07/2022.

Microsoft News, 2020 Department of Defence selects Microsoft, Retrieved 09/07/2022.

Donghui Park, 2016, North Korea Cyber Attacks: A New Asymmetrical Military Strategy, Retrieved 09/07/2022.

Jill Scharr, 2014, Could 'Watch Dogs' City Hacking Really Happen?, Retrieved 09/07/2022.

Kirk McElhearn, 2020 How Quantum Computing Will Affect Computer Security and Passwords , Retrieved 09/07/2022.

Nist, 2018, Quantum Communications and Networks | NIST Retrieved 09/07/2022.

Lawrence Berkeley, 2014, Extending Moore's Law: Shrinking transistor size for smaller, more efficient computers, Retrieved 09/07/2022.

Techopedia Staff, 2022,Are autonomous vehicles safer than cars operated by humans?, Retrieved 09/07/2022.

Norwich University, 2021, The Importance of Implementing Security Protocol, Practices and Awareness | Norwich University Online, Retrieved 10/07/2022.

Zainab Al Mehdar, 2018, Cybersecurity and Cloud Computing: Risks and Benefits | Rewind, Retrieved 10/07/2022.

Jenny List, 2020, A Simple Yagi Antenna For Your Wi-Fi Router | , Retrieved 10/07/2022.

Kate O'Flaherty, 2021, Facebook Data Breach: Here’s What To Do Now ,Retrieved 10/07/2022.