Cyber Security

Subject Seminar

On

“Challenges in Cyber Security”

Submitted by

Anagha P

Roll no: 10

S2, MCA

ITEC Palayad

Introduction

Today cyber security is the main component of the country's overall national security and economic security strategies. In India, there are so many challenges related to cyber security. With the increase of the cyber-attacks, every organization needs a security analyst who makes sure that their system is secured. These security analysts face many challenges related to cyber security such as securing confidential data of government organizations, securing the private organization servers, etc.

Contents

1. Third Parties Can Unlawfully Misuse the Potential of 5G Network

5G network is something that is making the youth more curious. This is because it will let the current generation use their beloved gadgets more efficiently. But here arises a problem – the generation will be the victim of either the emotional or physical attacks. Such attacks will be from the side of cyber assaulters who will unlawfully enter the 5G wireless networks comprising complex architectures via various endpoints and misuse the data collected or stored by the smart plus speedy gadgets. Primarily, those attackers would be the third parties who have choked the necks of telecommunications departments with their revolutionary marketing steps. Till **2027**, the **5G** infrastructure market **may reach 47.775 Million** US Dollars with the rising demand for M2M connections. Thus, this is essential to identify the identities of third-party assaulters who are in a constant journey of taking unauthorized access to the users' data and then, violating the privacy and trust towards the reliable and customer-centric organizations they are engaged with.

2. An Increasing Rate of Mobile Malware

Mobile malware is harmful software that can intentionally target the operating systems of mobiles and then, disturb their performances. The prime reason for its occurrence – non-secure usage of URLs over Wi-Fi or other internet networks. As per the 2021 Mobile Security Report, threats related to mobile malware are faced by **97%** of organizations from different vendors claiming to offer next-level security to the existing cellular networks. And we can’t ignore such vendors because they will be inheriting Trojan activities, cyber-risks, and some vulnerabilities associated with them. Moreover, such an increasing rate of malware attacks over the existing mobile phones has become the pandemic theme of the COVID-19 times. Various packages naming *tousanticovid.apk*, *covid.apk*, *covidMappia_v1.0.3.apk*, *covidMapv8.1.7.apk*, *and coviddetect.apk* are hidden in various applications of banking. And when those applications are dropped on malicious websites and the associated hyperlinks, they have started coating the mobile users with spam and other cybersecurity attacks. Undoubtedly, the number will increase in the coming times because the masses are moving towards the remote working era and here, cybercriminals will be running their malware attack campaigns as this is and will be their assured resorts.

3. Artificial Intelligence: AI is Somewhere Controlling Cybersecurity Systems

Nowadays, healthcare industries and supply chain departments are adopting tools that support **Artificial Intelligence**. Also, those tools have some glimpses of Machine Learning and NLP with which they are helpful in controlling the datasets primarily involved with patients' info or orders in which retailers/distributors are interested. As per the McKinsey report, more than **25 percent** of healthcare organizations are investing in AI tools in this COVID-age. Even the banking sector has an impact of more than **30 percent** of the analytics derived via AI/ML tools.

The main loophole in using those Artificial Intelligent tools is that passwords and biometric logins are modified frequently by the patients, distributors, and other participants of the supply chain. With that, hackers can feasibly pick the pain points thereby controlling the monitoring of details like address, bank details, etc. Since AI tools perform at minimal human input in real-times, healthcare and supply chain industries are sensing attacks of malware, ransomware strongly destroying their incentivize growth. No doubt, cybercriminals will be involved with data violence so that they can continuously gain access to that sensitive data for targeting more patients or supply chain participants.

4. The Growing Popularity of IoT Devices

The usage of **Internet-of-Things devices** is trending nowadays because of their robust reaction-time and the lesser cost they invite in processing the merits of the cloud technology. Furthermore, the solutions those devices push through their communication channels are incredible and considered by organizations comprising a varying number of workforces. However, with such growing popularity, cybercrimes are increasing continuously. This is because cybercriminals can expose the profitable assets whose data is accessed from some industrial cloud network. In 2021, the IoT market has reached the potential of 418 billion US dollars, and we may expect it to grow to around **1.567 trillion USD by 2025**.

5. Ransomware Attacks are Targeting the Critical Business Aspects

Ransomware attacks are directly or indirectly becoming unpredictable predictions for small or medium businesses. With no hesitations, those attacks are also impacting the larger organizations having proper knowledge of data violence and other compliance standards. As per the Check Point Research, the percentage of ransomware attacks has gone **up to 102 in 2021** across the globe and our country has got impacted the most by **213 attacks weekly**. You may think about what happens in those attacks! In them, cybercriminals send malware or other viruses to your phones or the cellular networks you use currently. This infects the devices like mobiles, laptops you are connected with and then, all your personal info is accessed by such assaulters. Now, no one can stop those online criminals from asking you ransom (amount asked for releasing the captive) and they will be harassing you for that! Over 1000 organizations are impacted weekly due to those ransomware attacks and the number will go up if organizations aren’t skillful enough in strengthening their cybersecurity models or preventing their business aspects from being targeted by those online criminals.

6. No Control Over Phishing and Spear-Phishing Attacks

Spear-phishing attacks will easily be understood once we understand what phishing attacks are basically? So, phishing is somewhere related to social media and the cybercriminals prefer those phishing attacks because this helps them gather your card details (credit/debit), current location, or other sensitive info. Such attackers use deceptive emails or websites and show them in such a manner they look legitimate. Spear-phishing, on the other hand, is a sub-part of phishing and is its more sophisticated version. Here, online fraudulent send malicious emails, and they are sent to well-researched victims (such victims are analyzed well by the cyberattackers on the grounds of mental and emotional strengths). According to the 2021 investigation report of Verizon, 29,207 real-time security incidents were analyzed and 5,285 were confirmed data breaches. Out of these, **36 percent of breaches involve phishing** which is increased by 11 percent from the previous year. And if we talk about spear-phishing attacks, the number is actually not mentioned, but there is a discussion about credential stuffing. Approximately **95 percent of organizations suffered such stuffing** which is a spear-phishing attack

7. Growth of Hacktivism

Hacktivism is a combination of words Hack N Activism. In general, this is done with the purpose of breaking into someone's computer and steal that information that supports political or social agendas in the wrong way. The target of hacktivists is primarily to gain their visibility on the websites of government organizations and deface their security protocols by promoting their politically influenced cause. According to the 2021 IBM X-Force report, there was **25 percent of data thefts and leak attacks** (in 2020) in which hacktivists have demonstrated their interest in seeking data of multi-national corporations and the government bodies connected with them. No matter what the intention of the hacktivists was, but such criminal attacks are a slap to government organizations taking care of the assets of their customers. With this, a sort of motivation for challenging governments or forcing them to go against their morals is unknowingly promoted. There are many **anonymous hacktivist groups** working (**since 2008**) against disturbing the internal business processes of government or multinational organizations in the name of public welfare. They mix with the C-Level executives and continue embarrassing the government through the ideology of taking revenge with their online campaigns supporting regular flow DDoS attacks. This is a newer version of breaking into cybersecurity systems of the government so that the protests of hacktivists may spread throughout the world and launch a shuttle of defacement of the reputation immorally.

8. Dronejacking is a New Wave Disturbing Cyber Experts

Dronejacking is a way through which cybercriminals are using a toy-like drone and easily taking control over personal information. According to the report of Intel, Drones have targeted deliveries, camera crews, and some hobbyists for knocking out the enforced security law standards. Though drones are a major tool for farmers, photographers, shippers, and some law enforcement agencies, yet they seem to be a new wave of cyber threats. With dronejacking, cybercriminals with their malicious intent can potentially offer financial destruction to the companies like Amazon and UPS who are known for supplying essentials to their customers. Via dronejack, hackers can easily determine how many packages will be delivered to how many customers? All this may be done for fun sometimes, but the aftereffects are really threatening as this is a direct attack on the security compliance of the organizations focusing on consumer’s success and their overall popularity in a positive way. Apart from all this, variable risks are there like loss of expensive drones, destruction of private property (commercial airplanes) with which the hackers can easily detect the response time and capabilities of the hardware controller driving those drones. If the commercial operators and cybersecurity teams of bigger organizations won’t stay themselves tuned about the latest security software and vigilant protection solutions, they will continue to bear the losses of drone attacks and become the easy targets of such criminals anonymously.

9. Preventive measures of social engineering

Social engineering is concerned with a type of cyber attacks where hackers focus on tricks and non-tech strategies rather than using core tech approaches or tools to trap the users. There are some preventive measures associated, and they are setting the spam filters from low to high, instant denial or deletion of help requests, researching the sources of unsolicited emails, and many more. However, hackers are sophisticated nowadays and understand the frequency with which we are adopting such measures. They can feasibly take the legitimate access to our personal info and then, exploit us really well on the grounds of personality weaknesses. As per the report of Google, most of the **SEAs or Social Engineering attacks** are phishing via official emails or malicious websites which almost look authentic.

10. Office People Having Access to Data of their Organizations

Internal politics is something that everyone is aware of and this happens in every organization. Whether you talk about a tech-giant or a well-reputed automation agency, employees are assigned with some privileges and this makes the finances vulnerable to huge losses. All this gives rise to **insider threats**. They have grown up by 47 percent in the past 2 years and successfully inviting cybercriminals to nourish their fraudulent activities well.

More than **34 percent** of businesses are affected every year by such threats and this is giving the way to accidental breaches for breaking the trust and reputation of customers. Those **insider threats** are underestimated by the businesses a lot as they think it is important for them to deal with the complex market trends rather than giving such threats a look! All this disturbs the current status of a company as their employees have signed some deals with hackers for providing them the important information about the company. Later, those cyber criminals infect the security systems of organizations well which are managing the business complexities well in this second layer. If the organizations keep on underestimating them and keep on delaying in limiting the privileges, then it would be difficult for them to put a halt to the destructive and careless behavior of their employees somewhere challenging the pre-established secure protocols of cyber security.