Short notes

a) Evolution of malware

Just six years after the introduction of the personal computer the first computer virus was introduced to the world. In 1982 Elk Cloner the malware which was targeted apple OS, and the malware was attached to a game. It infected the Apple's boot sector and spread by cloning itself to new disks introducing to the system. When the virus is triggered it displays that how it cloned itself throughout the infected machine. A year after the first personal malware was found "in the wild," the term "computer virus" was coined to refer to a malicious program written to destroy data or to corrupt systems. As time moved on, the computer virus branched off into many different categories, each meant to define how it acted. In the 90's internet came into public use hence, malwares were facilitate to attack more entities. And also malwares in these period started to learn evading methods. Therefore, antivirus software industry also grew drastically. In the early 2000's 'I love you' worm and "Love Letter" was considered as the most damaging worm. It infected millions of computers worldwide after about 15 minutes of its release. So, this can be identified as the first aggressive social engineering criminal of cyber-crimes. In this era the laws against the cyber-crimes were also came into the picture and there were some arrestments of criminals such as Jan de Wit who authored the worm known as Anna Kournikova. In the mid 2000's more than a million known malwares were circulating around the internet. As well as the email spamming digital picture frames and hard drives from china which malware pre-installed on them were great threats in this period of time. In November 2008 the Conficker worm quickly infected more than 15 million machines worldwide. Researchers stated that this was not only an experiment to test new spreading capabilities but also a state-sponsored experiment. But in early times this was only a fiction. This became reality with the case Stuxnet in 2010 which was based on bug of windows system and this worm attacked Iranian Nuclear facility. Ransomware made their first appearance in September 2013 which locked user's file systems which only could be unlocked with a unique key. For the key the attackers asked for ransom. That's why called ransomware. Malware will be transformed into many types in near future. Because it a characteristic of malware. So being prevent of those threats is better than trying to destroy them.

b) Web threats

As the internet become more public in early 90's almost everyone could access internet with their own devices. As a result of that and the efficient data transferring methods used for almost every information based activities caused to create a huge information exchange via internet. This fact mostly caused for the increment of security threats of the web. Denial of Service (DoS) attacks have grown more and more sophisticated as the internet becomes larger. The primary objective of a DoS attack is to overwhelm the capacity of the web hosting web server. Hackers will continually flood your web traffic to finally shut down your host simply due to overloading. This is devastating for businesses and subscribers who need constant updates. Another type of web attack is SQL injections. SQL Injections are malicious programs, which were designed to infiltrate a database with the purpose of obtaining sensitive information. SQL Injections looks for faulty code or poor designed forms that might give the hacker a way to access your database's scripting. Once the hacker gains access, a hacker can "inject" their own code into the database, allowing them to manipulate and steal the sensitive stored data. There is another type called XSS (Cross-site scripting). XSS is one of the most threat full attacks on the web. XSS is a malicious code injected to the client-side of a website. One could get infected by simply visiting a website or using a web application. Just like SQL Injections, hackers look into a website for any kind of input vulnerability so they can inject their own code. XSS downloads your user's cookie information allowing the hacker to impersonate you and access your online accounts with ease. XSS lets the hacker record your keyboard's events so your IDs, passwords, and even bank account information could be collected by the hacker. Phishing would be considered the minimum threat of all web attacks. Usually phishing comes in the form of emails sent by seemingly credible entities such as banks, relatives, shops, etc. In reality, they are fake emails crafted by a hacker. The emails will bait the users to click a link or fill a form. The hacker will receive the information and gain access to your personal accounts, leaving you exposed for identity theft, online scams or much worse.

c) Mobile Threats

The main threat comes with mobile devices is when user losses the device. Phishing, spyware, malware is also play a huge role. Hackers continue to use the same techniques because they work. Tweak an application a little, adjust a phishing email and you keep getting results. Another aspect is Cryptocurrencies. Cryptocurrencies are not, in and of themselves, a security threat. And your end users may not be participating in the cryptocurrency speculation boom. As the hype around Bitcoin and other cryptocurrencies reaches fever pitch, we're going to see more and more thieves going after Bitcoin wallets and Bitcoin exchanges, in addition to any other financial data they find. Wallets are often stored on mobile devices, and as these wallets skyrocket in value, thieves are looking for any way to grab them, which means new types of spyware and malware, and new opportunities for data leakage. The risks of wireless networks, both Wi-Fi and carrier, continue to grow, and there's no end in sight. Carrier attacks have been better hidden, but as the costs of tools such as software-defined radios come down, can expect more threats here as well. Knowing what the problem will be is impossible, but it's a near certainty that there will be some major wireless security problem or a long series of smaller ones or both. By now, getting malware on a device is nothing new. But with the broadening of the Android manufacturer base, a shortage of security talent and tightening release timelines everywhere, we can expect more malware in factory-fresh devices.

d) IoT Exposed

IoT seems to be conquered the world in IT and business at the moment. Simply put, IoT is defined as everyday objects with computing devices embedded in them that have an information to send and receive data over the internet. But the main problem is IoT's insecure web interface. The web interfaces built into IoT devices that allows a user to interact with the device, but at the same time could allow an attacker to gain unauthorized access to the device. And also insufficient authentication is a major issue with IoT. Ineffective mechanisms being in place to authenticate to the IoT user interface and/or poor authorization mechanisms whereby a user can gain higher levels of access then allowed. Insecure network services are also a threat for IoT devices. Vulnerabilities in the network services that are used to access the IoT device that might allow an intruder to gain unauthorized access to the device or associated data. Another issue is lack of transport encryption. This could easily lead to an intruder sniffing the data and either capturing this data for later use or compromising the device itself. Privacy concerns are generated by the collection of personal data in addition to the lack of proper protection of that data. Privacy concerns are easy to discover by simply reviewing the data that is being collected as the user sets up and activates the device.

Automated tools can also look for specific patterns of data that may indicate collection of personal data or other sensitive data. Insecure cloud interface used to interact with the IoT device. Typically this would imply poor authentication controls or data traveling in an unencrypted format allowing an attacker access to the device or the underlying data. Insecure mobile interface also leads to the issues stated above. Insufficient security configurability is present when users of the device have limited or no ability to alter its security controls. Insufficient security configurability is apparent when the web interface of the device has no options for creating granular user permissions or for example, forcing the use of strong passwords. The risk with this is that the IoT device could be easier to attack allowing unauthorized access to the device or the data. The lack of ability for a device to be updated presents a security weakness on its own. Devices should have the ability to be updated when vulnerabilities are discovered and software/firmware updates can be insecure when the updated files themselves and the network connection they are delivered on are not protected. Software/Firmware can also be insecure if they contain hardcoded sensitive data such as credentials. The inability of software/firmware being updated means that the devices remain vulnerable indefinitely to the security issue that the update is meant to address. Further, if the devices have hardcoded sensitive credentials, if these credentials get exposed, then they remain so for an indefinite period of time. Physical security weaknesses are present when an attacker can disassemble a device to easily access the storage medium and any data stored on that medium. Weaknesses are also present when USB ports or other external ports can be used to access the device using features intended for configuration or maintenance. This could lead to easy unauthorized access to the device or the data.

e) Ransomware, coinmining and underground economy

Aspiring cyber criminals often start with “low risk, low yield” attacks, to ease in the trade. Ransomware has had this role for a few years. Many were impacted, as ransomware’s destructive side effect started tipping the criminal business model. The risk for criminals has increased. There’s a good chance ransomware will lose its place as “cybercrime 101”. Although crypto ransomware existed in 1989, modern ransomware started in 2013 as a side project of the GameOver ZeuS fraud group. Called cryptolocker, it got huge attention from the industry and press. These ransomware got simple proceudure.

1. Infect PC
2. Store bot identifier in C2; create unique, strong, private key
3. Encrypt important files on victim device
4. Accept BTC payments
5. Immediately return private key to victim after payment

Unfortunately, in 2017 the high profile ransomware attacks, specifically Wannacry and Notpetya, forgot the importance of rule 5. Payments lagged after reports that no one got their files back. Researchers found that Wannacry didn’t even have the necessary code to facilitate the process. The criminals couldn’t return your files even if they wanted to. Notpetya had a manual, broken process for returning files. An e-mail address was quickly taken down, leaving the criminals unable to return a key. Almost no-one got their files back. Untrustworthy bunch. Ransomware is becoming deprecated. Today, the majority of malware we spot in the wild is still ransomware, but that might change. Crypto currency mining has been around for some time in the DIY space, and criminals are taking notice. The premise is to use victims computing power to do the billions of calculations needed to find new electronic currency, a process called mining. It might seem crypto currency mining is essentially stealing electricity. From a victim perspective, this kind of attack is way more friendly, since it doesn’t destroy or steal data.

f) vulnerabilities and Patching

Vulnerability management is a pro-active approach to managing network security. The purpose of the Vulnerability Assessment policy is to establish controls and processes to help identify vulnerabilities within the firm's technology infrastructure and information system components which could be exploited by attackers to gain unauthorized access, disrupt business operations and steal or leak sensitive data. It include the following steps.

- ✓ **Checking for vulnerabilities** : This process should include regular network scanning, firewall logging, penetration testing
- ✓ **Identifying vulnerabilities** : This involves analyzing network scans and pen test results, firewall logs or vulnerability scan results to find anomalies that suggest a malware attack
- ✓ **Verifying vulnerabilities** : This process includes ascertaining whether the identified vulnerabilities could actually be exploited on servers, applications, networks or other systems
- ✓ **Mitigating vulnerabilities** : This is the process of figuring out how to prevent vulnerabilities from being exploited before a patch is available, or in the event that there is no patch.
- ✓ **Patching vulnerabilities** : This is the process of getting patches usually from the vendors of the affected software or hardware and applying them to all the affected areas in a timely way.