**CS808 – Computer Security Fundamentals**

**Coursework Assignment**

**Deployment of security infrastructure:**

Business get a deployment of application from which all have the security from any devices or online workplace which are not complicated to use. Example of mobile devices for security deployment.[[1]](#endnote-1) Any mobile devices to connect with any network which are protected with the firebox are safe to use, i.e. wireless AP Device which can directly connect with the firebox which means “when the mobile security enforcement are enable for the Trusted-2 interface” then the security of mobile drops the traffic received on the same interface from the mobile device which are not manageable[[2]](#endnote-2).Drone another scenario where the security deployment is very important as per the recent report because these days drones are very commonly used and it can be dangerous if used in an unauthorised manner but mostly drones are also very useful[[3]](#endnote-3) as Pilot of drone Berry crack explained the importance of Drone security deployment to secure the future as an example ,i.e. “Drone can carry blood to the hospital preferably not compromising the busy traffic[[4]](#endnote-4).

**Biometrics is built on several unproven assumptions:**

The Technology of Biometrics give the authority to the government to deal with the crimes more effectively which make safest world and public have more security. There are varieties of finger printing types which links to significant check of database background, which are done in collaboration with agents of state, police and the business to have the fingerprint of a person to access detail background check[[5]](#endnote-5).Also, sometimes people feel, biometric technology creates huge threat to the privacy and security because the application can be easily differentiated to examine and a person’s profile[[6]](#endnote-6). Biometrics cannot be false or fake because the fingerprints and an eye scanner are unique for each person. Though biometrics have the safe security system still it has some dispute to solve like the most problem to focus about biometrics are the less accuracy while capturing the data, map the identity which can be sometimes a failure as well as the privacy which is the major thing to think about because when the server is saving biometric information’s can be hacked which can result a risk to a person. Sometimes there could be a fake rejection or acceptance in biometric devices when device can’t read the proper information due to any device error which can lead to accept an unauthorised person and an authorized person could be rejected which could cause serious damage to the individual or a country. The main disadvantage of biometric is very expensive to run the system and storing as well as the maintenance of the system[[7]](#endnote-7).As an Example, This year the Suprema’s BioStar 2 program found that the BioStar 2 customer users are being accessed by the third-party in an unauthorised manner by the researcher but because of the ethical reasons they never tried to download any fingerprints information instead they collected the file samples and converted the suprema’s software to the fingerprints of visible type. So according to Mr Peter who revealed to the BBC news that they have evidence of biometric data has been leaked[[8]](#endnote-8).Aadhaar card India’s most required biometric-based identity database issued by the government in 2016, where estimated around 1.2billion people hold aadhaar card where people give their fingerprints and retina scan. But again, there are privacy issues whether it is safe or unsafe for the public as biometrics store very personnel information of each individual, and later it was clear that there are safeguards to the sensitive information so there is no privacy risk associated with aadhaar card[[9]](#endnote-9).

**Technology solutions can fix deeply embedded political problems:**

Not valid to put technology in trouble which are not technical instead find other solutions to recognize. So, the International of privacy and the partners found that the government are very interested in developing a data security project[[10]](#endnote-10). From past ten years technology has achieved lot to reshape many ways for the society like politics. Gadgets like computer, mobile phone, tablet etc has made the politician more convenient to communicate with parties and people using the new technology. New technology has made the politician more efficient to work and there are lots of benefits in future for the politician using new technology like Chatbots helps business to communicate with the consumers in less time which has the power of mimic the conversation. There are many political parties implement many chatbots to connect with the audience, register for voting and many more[[11]](#endnote-11).I think Technology have both positive and negative way of impact on political society. These days people get all the updates of upcoming events as well as people can participate in the political issues through mobile phones, computer and social media with the help of internet connection which is the positive side of the Technology in politics. But there is also negative impact of Technology are people can get manipulated with false rumours and domestic politics[[12]](#endnote-12). An example of politics uses Technology as During 2009 while Iranians were protesting “Green Movement” they used social media like Facebook and YouTube videos to spread their message worldwide. After two years, Arab springs started protesting the movement True power, they too used the social media for support and to convey their message in Tunisia and Egypt[[13]](#endnote-13).Auditing for fraud requires entire populations to be tracked using their personal data: Fraud happens using a person’s private information’s with his knowledge by someone else. Incorrect document is used for crime like breaking the security system or to use the government agencies i.e. immigration[[14]](#endnote-14).Demanding for biometric information like Iris and facial scan are risky.

As an example, A conflict among the United Nations World Food Program and Houthi rebels run the capital region has threatened many people’s life in Yemen. So, they demanded Houthi officials to let them use of biometric technology such as iris scans or digital fingerprints to track the crime during food distribution. Other than the good intentions , the thought of using technology as biometrics are made of many unproven assumptions like technology solutions can settle all political problems but to find the fraud needs whole population to monitor accessing their private files which can arise a chaotic situation as the ethics of concern are not applicable for the starving humans. Biometric and digital Technology can significantly damage lives of humans who are not in place. Tons of migrants and refugees in Europe who had conflict in East Africa was told that how little inconsistency in recognising database creates administrative chaos. If there is a mistake with spelling in someone’s name as an example can be a huge risk of separating parents from their child or children also sometimes can cause rejection in the asylum application. Not necessarily always the database will work proper based on some government officials carry the biometric to differentiate against the people who are lost due to which refugees avoid camps which need fingerprint for swapping food and shelter. So, tracking and collecting data are important to deliver safe and security for the right people and in the correct place for the humanity[[15]](#endnote-15).In the modern world non-stop connectivity, cyber security is very important for every organizations. Cyber security is always a headline topic everywhere of the security of information being breaking, these days cyber security is always on the news headlines. As in the recent times there are cyber crisis which means attacks on the cyber security and breaking the data because of the vast connectivity and dependency on the computer system[[16]](#endnote-16).

**Experimental technologies will work as planned in a chaotic conflict setting:**

The Experiment in the chaos technology system get confidence with their performance before deployment. According to Netflix team, adding instruction to the code where fault injection occur to specific instructions will be working in a chaotic conflict setting and push the system clock out of synchronize with one another. In 2018 the chaos technology arises from Netflix where the streaming of subscription started changing from their own data into public cloud.so, the Chaos Monkey, which is an automated testing tool, continuously stopped executing virtual machine production of instances which was made in the year 2010. Then later in 2012 released as the open source software to get success in the continuous testing process rather than the failure. Chaos Technology is useful in finding if there are failure of any source of software in the system, which can fail without having the whole system inoperable to the customer. Chaos Technology are applied in many other development processes such as “Canary analysis” where the deployment of any brand-new programme can measure with their performance widely[[17]](#endnote-17).Chaos Kong another tool was built to inject small level of production failure to overcome so that it will increase the safety towards the experimentation, where they run experiments in their production without affecting the customers. To do this, they should keep few requests at risk to protect their overall availability, where the risk will be minimum. Example1: At Netflix, there are hundreds of deployments takes place every day in the production, which reduces the confidence with the experiment report. So, to have safe experiments, an automated analysis has been replaced known as Canary analysis to keep the result up to date. Example2: People want to know how API deal with the failure in the Rating system, where people can rate movies using the Like, Thumbs Up and Thumbs Down symbol. To set this experiment, technologist deploy new API clusters which measure the proportion of the people want to read. Therefore, the request of routing will be overridden to limit and experiment people to direct the traffic to new cluster rather than production cluster. So, the experiment of traffic will send to the cluster to request among the API and ratings will be affected[[18]](#endnote-18).

**The ethics of consent don’t apply for people who are starving:**

I think computer ethics is not applicable to the people with poverty because some people who are starving may not have any devices like computer or mobile phone to connect with the modern world or people may have device but may not have any internet connection to communicate. Starving poor people don’t really need biometric card or anything related reason behind poor people can’t carry any card with them or they don’t travel and don’t use any network. Example: If any accident happens like fire they cannot afford to apply for a new biometric card and will lose all the evidence of their identity. Also, poor people can buy licencing cost of software, so they go for pirated version of software. Unknowingly start-ups use copyrighted data for targeting customers to reduce the operational cost. Devices having pirated copies of embedded software are also on the rise. Starving people only worry about the costs. As such computer ethics goes for a toss. When common people are dealing with it as they are following an unethical computing practices in order to feed themselves and their dependents.

**References:**

1. <https://www.akamai.com/uk/en/resources/application-deployment.jsp?gclid=Cj0KCQjwoqDtBRD-ARIsAL4pviCjhXgVzJMawA3xoZjgzjEANxTSsSDeQisn29MvkldSMkLO6eAk47MaAnd5EALw_wcB&ef_id=Cj0KCQjwoqDtBRD-ARIsAL4pviCjhXgVzJMawA3xoZjgzjEANxTSsSDeQisn29MvkldSMkLO6eAk47MaAnd5> [↑](#endnote-ref-1)
2. <https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/mobile_security/mosec_examples.html> [↑](#endnote-ref-2)
3. <https://www.ifsecglobal.com/security-drones/> [↑](#endnote-ref-3)
4. <https://www.ifsecglobal.com/drones/using-drones-to-secure-the-future-ifsec-2019-panel-debate/> [↑](#endnote-ref-4)
5. <https://www.gemalto.com/govt/biometrics> [↑](#endnote-ref-5)
6. <https://privacyinternational.org/learning-topics/biometrics> [↑](#endnote-ref-6)
7. <https://www.securitycommunity.tcs.com/infosecsoapbox/articles/2017/01/05/15-important-pros-and-cons-biometric-authentication> [↑](#endnote-ref-7)
8. <https://www.bbc.co.uk/news/technology-49418931> [↑](#endnote-ref-8)
9. <https://www.bbc.co.uk/news/world-asia-india-45650649> [↑](#endnote-ref-9)
10. <https://privacyinternational.org/learning-topics/biometrics> [↑](#endnote-ref-10)
11. <https://www.business2community.com/social-media/5-ways-technology-shaping-politics-2017-01838986> [↑](#endnote-ref-11)
12. <https://www.pewresearch.org/internet/2019/05/13/publics-think-technology-impacts-the-political-environment-in-both-positive-and-negative-ways/> [↑](#endnote-ref-12)
13. <https://www.vox.com/policy-and-politics/2019/1/22/18177076/social-media-facebook-far-right-authoritarian-populism> [↑](#endnote-ref-13)
14. <https://en.wikipedia.org/wiki/Identity_theft> [↑](#endnote-ref-14)
15. <https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html> [↑](#endnote-ref-15)
16. <https://assets.kpmg/content/dam/kpmg/ch/pdf/key-risks-internal-audit-2018.pdf> [↑](#endnote-ref-16)
17. <https://www.techrepublic.com/article/chaos-engineering-a-cheat-sheet/> [↑](#endnote-ref-17)
18. <https://www.techrepublic.com/article/chaos-engineering-a-cheat-sheet/>

    **TLS:” Sok: Lessons Learned From SSL/TLS Attacks”**

    **Abstract:**

    The secure socket layer protocol (SSL) introduced in 1994 now known as the Transport layer security (TLS) evolved from the standard of securing the transport layer (SSL/TLS) are used for the confidential data, integrity, and authenticity while transporting information. The main feature is the protocol is the flexibility through different cipher suites to configure the mode of the operation and security of data.

    **Introduction:**

    During 1994, Netscape entitled HTTP traffic by the Secure Sockets Layer protocol known as Transport Layer Protocol. SSL means secure socket layer protocol fix all the security issues from many decades. Now the advanced version of secure socket layer protocol is name as transport layer security. [1] Basically SSL protocol creates a secure connection and trust between the server and the client. To have a secure connection for any business where the customers can trust and have confident feelings, they provide the padlock with various colours.

    The SSL/TLS layer has two design blocks

    Handshake protocol known as authenticated key exchange protocol for compromising with the cryptographic privacy and algorithm.

    Record protocol is to Encrypt the layer between the application and TCP Layer.

    **Attacks on the Handshake protocol:**

    Wagner and Schneier mentioned about the cipher suite rollback attack, which are to limit the cipher suite list by the client to weaken one or NULL ciphers. In a connection third person can attack in middle to change the Client Hello message and replace the cipher-suite list. Then the server will have no option either will have to reject the connection or has to accept the weaker cipher-suite. This problem was fixed by releasing the SSL 3.0 with authentication of the message in the Handshake protocol. The client sends and receive all the messages by the hash value of all the handshake protocol.[1] To prove the establishment of the secure connection SSL provide key pair of certificates i.e., private key and public key , using both the keys the connection become encrypted where client and server can have trusted communication between each other. we have to use three keys for SSL protocol to ensure the connection on both the sides are secure i.e. private key, public key and session key. The ChangeCiperSpec Message Drop was feasible in SSL 2.0 only. During Handshake phase the cryptographic primitives are determined and to activate the message both parties has to send a ChangeCiperSpec Message. This message is to inform that the communication will be secured by the previously agreed parameters.[2] Client and Server will be sent message to each other to start the negotiation which they decided. The client will verify the certificate and the key exchange then send the ChangeCiperSpec message to server. when server receives the message from client server sends back the ChangeCiperSpec message.

    SSL 3.0 supports the use of temporary key material during the handshake phase signed with a long-term key. Each party implicitly decides based on the context, which key material is expected and decode accordingly. This creates the surface for a type confusion attack. So, this attack is to highlight the need for context-free message structure and misinterpretation of a received message should be avoided. Server and client should share two different keys with each other where the man in the middle will not be able to break the algorithm to attack. An attack where a client Hello message Premaster Secret of the clientKeyExchange message. So, the Backward compatibility has a serious threat.[3] client or server the victim might be fooled with the man in the middle who attack breaking the old weaker version of cryptography where attackers will delete the bytes in the last part of the message so to prevent the attack users must update with the new version of cryptography.

    In 1998, an attack on RSA based Cipher suits was presented by Daniel Bleichenbacher’s where he used the strict structure of the PKCS#1 v1.5 format to prove that it is possible to decrypt the PreMasterSecret in a reasonable timespan. The random value generated by the client and sent within the ClientKeyExchange is known as PreMasterSecret. Here the attacker will decrypt the message by thinking the server as a decryption oracle. In the internet one should provide with less information because here attackers can attack the system and crack your information later using that information can decrypt the premaster secret.

    The attack takeout the private key from the server whom they are targeting by tracking the time gap between sending the ClientKeyExchange message with an alert message received as an invalid format of PreMasterSecret.[4] In timing attack the attacker attacks on the security system by finding the time of system process for various inputs. Cryptographer Paul Kocher who uncover the private decryption keys without interfering RSA. Smartphones and web servers are also the victim of timing attacks due to the network conditions where the time gap can be hidden.[5] The best way to prevent from timing attack are to have a constant processing time. Time based attack is an interesting concept to discuss because here the attacks takes place due to the time variations.[6]If the system process with continuous change of time then the system time will be interrelated with the calculation time where the attacker will be able to calculate and find out the time needed for system process. So, to prevent attacker to attack the system the better way to make the same number of times to process the system.

    **Note:** In the cipher suite protocol a third person can attack in middle which will weaken the server so server might get confuse and accept the wrong message. lesson learnt here is to have a secure connection we should use certified software where the connection will be encrypted from both the sides using the keys where the server and client will trust each other to communicate. During the handshake phase SSL 3.0 use temporary key where the attacker can create a confusion between the server and the client to break the algorithm so that the server and the client will have miscommunication where the third party will enter and change the code or message. so, to prevent this kind of attack server and client should use two different keys where the man in the middle will not be able to break the algorithm. The backward compatibility has a big threat where the attacker can change the client message or delete some information from the message so the client and server might impact badly by receiving the wrong message so to prevent this attack user should always update the device with new version of software. If providing with lot of information on the internet the attacker can attack the system to decrypt the message and better to provide less information in the internet so that there will be less chance for the attacker to decrypt any private data.

    **Questions:**

    1. How can we encrypt the connection between the client and server?
    2. what happens during handshake phase?
    3. Explain the man in the middle interpretation and how can we prevent the attack?
    4. Discuss the way how can the user prevent themselves from the backward compatibility where the attacker might interfere?
    5. what may happen if the attacker changes the hello message?
    6. why should the user update with the new version of cryptography?
    7. What attackers can do to decrypt the message between the client and server?

    **Attacks on the Record and Application Data Protocols:**

    [1a] Phishing attacks are targeting to steal the Mac/apple logins. Where the attacker locks the apple account to restore, we have to confirm the login id. And also, the attacker sends an expensive money to purchase including a cancel link. In this case the fake email and the fake website will look very genuine. Attackers cannot install virus in MacOS so they hijack browser to show the ads from hackers which can change the browsers homepage as well as the default search engines. The most common way of getting malware onto a Mac is through the fake flash player update so its better to ignore those fake flash players or do not allow flash player on the Mac anytime.

    **Attacks on the PKI:**

    [2a] In the world of Technology, where to gain trust on the service for any business require a certificate which is known as PKI. For example, if we are browsing any website like bank, for security purpose the client will request the certificate to trust the site is genuine. Which guarantee the authenticity and the secure communication between the user and the service which protect from the attacker to break or change the transaction. But though the certificate looks trustworthy if in case the attacker get access on Certificate authority there the possibility to issue a false certificate then can have fake website for users to believe. So, the issue is when the web browser certificates are being stored by the server though SSL restrict the access to information by attackers, still a threat being stolen the certificates by attackers as there are no built-in technique which could allow limited access to the data by attackers. Sometimes if there are lot of information on the device while in busy traffic attacker can easily access the information. To prevent the application from attacks company should use anti-Dos and anti DDoS protection. [3a] In the recent past in 2015 research was done where it suggests to use blockchain for decentralized PKI which is better way to proceed towards the current PKI. Decentralized PKI restricts any third party where the data will not compromise the integrity and the security of the device. The main benefit of blockchain for decentralized PKI is that it has the power to secure the information study and protect the attacks from MITM as well as limit interference of any third party to resolve any issues.But the main reason why any user doesn’t want to use blockchain is because user have to download the whole copy of the information so the main issue is the size of the data to download without losing the privacy.

    **Note:** In the modern world technology play keen role where people perform most of their task online using network connection so there are chances that the third party can attack all the personnel information like credit card detail etc through spoofing so to protect these kinds of MITM attack user should use PKI technology which provide digital certificates.

    **Questions:**

    1. Provide a scenario how MITM can attack and how to prevent that attack?
    2. What are the advantage and disadvantage of using PKI?
    3. What does PKI mean?

    **Various Attacks:**

    [4a] Cryptography are the common area in the cyber security world to think of. But there are issues with algorithms, implementation of cryptographic protocols, authentication algorithm and various things. Therefore, the security engineers have knowledge of using these algorithms as an encryption key. Basically, any encryption algorithm will be random as pseudo random number generators. [5a] If using pseudo-random number generator (PRNG) make the cryptography stronger while the using non-cryptographic PRNG can allow some kind of attacks. Which means weak algorithms contain less power to process the system. Where some features can use to crack the cryptography. Usually PRNG are to authenticate and give some kind of authorization like session ID or allow to generate a key of cryptography where an attacker can calculate ID or the key to access the information.

    **Note:** Pseudo random generators are used for stronger cryptography to limit the attacker break the system of data whereas the non-pseudo random numbers are weak due to the slow process of the system where the attacker can identify the ID to break the system data.

    **Question:**

    1. What is PRNG?
    2. What is the benefit of using random number?
    3. In which situation an attacker can break the pool of random number generator?

    **Reference:**

    1.<https://www.digicert.com/ssl/>

    2.<https://www.slashroot.in/changecipherspec-protocol-ssl>

    3.<https://courses.cs.washington.edu/courses/cse484/12sp/lectures/Lecture19-Sp-2012.pdf>

    4.<https://searchsecurity.techtarget.com/definition/timing-attack>

    5.<https://security.stackexchange.com/questions/30782/is-it-reasonable-to-prevent-timing-attacks-by-using-fixed-processing-time>

    6.<http://www.fit.vutbr.cz/~cvrcek/cards/timingattack/timingat.htm.en>

    1a. <https://9to5mac.com/2019/09/12/phishing-attacks-targeting-mac/>

    2a. <https://www.securityweek.com/examining-threats-facing-public-key-infrastructure-pki-and-secure-socket-layer-ssl>

    3a. <https://diode.io/blockchain/MITM-attacks-and-why-it's-time-to-start-thinking-about-decentralized-PKI-19210/>

    4a. <https://www.cryptomathic.com/news-events/blog/generating-cryptographic-keys-with-random-number-generators-prng>

    5a. <https://cwe.mitre.org/data/definitions/338.html>

    **Case 1: A DoS attack on a website:**

    [7] DoS the distributed Denial of service is the cyber attack which target the connectivity which rises a

    Denial service for users of the targeted resource. A Dos attack look for multiple malware infected systems to attack a single computer. If the network slows down or if we receive lot of spam emails which mean there are an occurrence of dos attack. It is helpful to select DDOS mitigation service where the engineers and network administrators will monitor the traffic regularly.

    [8] If you are supposed to do online shopping and you visited an online website to shop. Your computer sends an information to the website as “hello” which means your computer is saying hi want to come please allow me inside. After the server receives your message it tells you OK if you are real. Your computer says yes, I am real and that way the communication starts between you and the server. In case of Dos attack a computer continuously sends thousands of messages to the server which can’t recognise the message are fake so they response back with usual message then wait for reply the reply. When the server receives no reply, the server slows down the connection and then the computer performs the repeat attacks sending next new fake requests.

    The following are the ways we can prevent DoS attack:

    We should use anti DDoS service to protect ourselves from the attack, also we can identify between the law in the network traffic and a DDoS attack.

    If we find our computer is on attack, we should inform our internet service provider immediately to identify if my traffic can be rerouted. Also, it’s good to back up our ISP.

    To prevent the website or the network from crashing we can use black hole routing which will send the unwanted traffic into the NULL route.

    To prevent the computer from false traffic we should configure the firewall and routers in our computer

    [9] Dos attack take place mostly through a botnet, where lot of device will send request to the server at the same time. DoS attacks (don’t steal data or don’t break any privacy rule.

    **Case 2: A keylogger that captures and sends sensitive data to the attacker:**

    [10] Many hackers hack the computer through internet using keyloggers. Spyware is one kind of

    malware which record all the computer activities. A keylogger captures every key stroke one does in

    the keyboard a computer. Using keylogger a hacker can find your username and password for many

    sites without knowing what’s on the screen. For example, if you open Gmail then enter your username

    and password. Everything you entered will be sent to the hacker database through the internet. Another name of keyloggers keystroke loggers. Key loggers will not make the computer slow and we can’t know when the hackers are on operation. Keyloggers have built into the operating systems, this kind of malware is known as the toolkit virus. There is another type of keylogger known as the hypervisor malware which operate in a lower level. Some keyloggers infect the webpages so whenever someone visit that webpage hackers will steal their information. To steal information the keyloggers will change the memory process to access the webpage.

    So, there are different scenarios for keyloggers to run their program in many different locations on the computer.

    To detect a keylogger we have to right click on the windows and open the task manager there we can we find the list under the background process and also, we can find keyloggers in the startup tab. Its better to disable pressing the button anything you find in the startup tab which you don’t have any idea of installing. To remove keyloggers from the computer install antikeylogger software like Malwarebytes Anti-Rootkit, McAfee Rootkit Remover and Norton Power Eraser.

    [11] There are three types of keyloggers are as follows:

    User mode keyloggers

    Kernel mode keyloggers

    Hardware based keyloggers

    [12] For all the online user’s keylogging is a big threat of cybercrime because keyloggers can steal all the private data without your knowledge like username and password of person’s online banking and many more. Key stroke can be done through hardware keylogger and software keylogger. A hardware keylogger will create a connection between the computer and the keyboard. Software keylogger are the computer programme which has to be installed on the target device. So, to avoid keyloggers one should follow few things:

    Use anti-virus software with the anti keylogger so that u the anti-virus software can detect the keystroke logging software and will be able to remove the keystroke logging software from the device.

    As there are chance that keyloggers will attach them to the free version of software available on the internet like free screensavers so it is better not to install such type of software in the device.

    Should use a secure browser like Firefox, google chrome etc.

    [13] Best practice to change the password regularly so that even the hacker stole the password and not use it then it will not be useful for the hacker. Changing the password regularly means you are protecting your accounts from the keyloggers.

    **Case 3: A phishing login page:**

    [14]A phishing is an attack in the social network where the private information like login detail or debit card detail will be stolen through an email, message or text message. where the victim will be fooled to click on a malicious link which can result in installing a malware or freeze the computer as there might be a ransomware attack or disclosing the private data which make the criminal to do an unauthorized shopping, stealing the money. Email phishing is one of the phishing attack technique where an attacker sends lots of scam messages.

    And sometimes the attacker will force the users for an immediate action by sending mail about the account expires or won some lottery because of which sometimes some user believes and take an action.

    If there are grammar or spelling mistakes in a message that means the message is send by an attacker.

    [15] Phishing attackers will send you a fraud email to reveal all your detail information then using that information they may empty your bank account or change your username and password to get access to your account. [16]phishing attacks are very dangerous and the high threat is to detect the phishing attack which is really difficult where attackers are well experienced and they know all the trick to attack any computer in such a way that the user consider the process safe and genuine to access the webpage or any information send by the attacker and taking wrong action they become the victim. So, it is very essential to monitor the integrity of the webpage, files and directories.[17] To protect yourself from phishing attack should be very careful about any email you receive if it looks like phishing attack you should delete the email. Avoid clicking on any unknown links or any listed link in the email message. should not disclose any personal data on any pop-up screen. Try to install a phishing filter on your email as well as on the web browser to avoid receiving any phishing messages.

    **Case 4: A government backdoor installed in an email program and a VoIP app:**

    [18] The National Security Agency reveals the way government are spying on us which is indeed not acceptable. Using private WIFI the government demands for backdoor access to the well-known websites which create a large data base of all the emails we send and later the data brokers hijack all our information and sell it. The government worked on a project as PRISM in 2007 which track all the communication between the US citizens with the foreign nationals. Where NSA was monitoring everything like email, video, photos, VoIP (internet phone calls), video conference and social network information’s where the users are from largest online companies like Google, Apple, Facebook and YouTube.

    **(i)Describe which of the security properties are compromised, with an explanation:**

    [19] The most valuable asset for any company are the intellectual property which can be harmed and compromised. Today the intellectual property is stored electronically and are of many types like the knowledge of a company work process or operating process. So, its very important to protect the company’s intellectual property because an information that compromises may result a bad impact to your organization as the asset might be with one of your biggest competitors.

    Some intellectual property is to have the legal enforcement ownership grant and only source of authority in exchange for the disclosure of public to have protected intellectual property. Trade secrets are another intellectual property where owner should be the only dependent to maintain the secret and protect incase the property is compromised. External and internal source can attack to compromise this kind of intellectual property. To protect the property against compromise, organization should restrict the disclosure of key employees and limit the access to the core members. Cyber-attacks and computer hacks can be the source of threat where the intellectual property could be compromised. So, the owner should keep high security protocol for all their systems, like using firewalls, security monitors, an action to detect and prevent the system from hacking. Trade secret is another risk of compromising the security of the property so to prevent partner should have limited manufacturer contract where the key components are gathered from different suppliers so there will be less disclosure of related intellectual property to an organizations.[20] In the year 2014 the Telecommunication giant revealed that , an insider accessed customer information in an unauthorized manner and leaked the private customer data where the customer privacy rule was breached and was able to get access to the customers private information like social security number, driving licence number etc which could be a security threat to the customer .[21] security compromise may arise when without intention any private data are disclosed or someone access any data without having authorisation which is known as the breach of data. If the data are disclosed in an unauthorised way then there might be bad impact on the company profit and reputation. Also, the risk of protecting private data of the company.

    **(ii) Describe one countermeasure that might be employed to prevent the compromise:**

    [20] To prevent the data compromise, company should have control on the IP property which includes the location of the property, terms and conditions of the license and their renewal times. Certain policies and procedures should follow by the company and should implement internal security system where the managers only get access to some specific data and there should be a log incase of the data loss they can retrieve the data back again as well as incase of any unauthorized access the system administrator will get the notification.

    Companies can have non-disclosure agreements with external partners and encrypted information and software to prevent the compromise of the data.[22] Non -disclosure agreement will protect the company private data from others to have an unauthorised access , it is important to save companies business strategy, private information of the customers, trade secrets and many other information.[23]In an organization there are few areas where the company needs to share private information with another company. The way to share such things safely is to make other company follow and respect the confidential data which cannot be used without the permission of the owner of the provided organization by using the non-disclosure agreement where the company sign the agreement and is bound to follow the rules.

    **References:**

    7.<https://phoenixnap.com/blog/prevent-ddos-attacks>

    8.<https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html>

    9.<https://www.globalsign.com/en/blog/denial-of-service-in-the-iot/>

    10.<https://www.comparitech.com/blog/vpn-privacy/what-is-keylogger/>

    11. <https://www.lastline.com/labsblog/detecting-keyloggers-on-dynamic-analysis-systems/>

    12.<https://www.lastline.com/labsblog/detecting-keyloggers-on-dynamic-analysis-systems/>

    13. <https://vpnoverview.com/internet-safety/malware/keyloggers/>

    14. <https://www.imperva.com/learn/application-security/phishing-attack-scam/>

    15. <https://safety.yahoo.com/Security/PHISHING-SITE.html>

    16. <https://blog.sucuri.net/2016/08/modern-web-phishing-works.html>

    17. <https://www.cisecurity.org/daily-tip/protect-yourself-from-phishing-scams/>

    18. <https://blog.privatewifi.com/ask-the-expert-can-a-vpn-protect-you-from-government-surveillance/>

    19. <https://digitalguardian.com/blog/how-to-secure-intellectual-property>

    20. <https://www.eweek.com/security/two-at-t-data-breaches-draw-attention-to-insider-access-issues>

    21. <https://bizfluent.com/about-6567858-definition-security-compromise.html>

    22. <https://www.legalnature.co.uk/vlp/na-4732/non-disclosure-agreement?utm_source=Google&utm_medium=ppc&utm_term=non%20disclosure%20agreement&utm_campaign=Non-Disclosure%20Agreement_Search_LN&fid=24589977&revamp=true>

    23. <https://www.forbes.com/sites/allbusiness/2016/03/10/the-key-elements-of-non-disclosure-agreements/#3bfadc8f627d>

    **The WEP (Wired Equivalent Privacy) security protocol was designed to secure packets on wireless networks. It uses 24bits of Initialisation Vector (IV) to generate the keystream. Describe a fundamental vulnerability due to this design decision in the protocol. Propose an attack that exploits this design vulnerability.**

    [24] Sometime the users who uses the WEP security protocol, they don’t change their keys for long period of time while using the wireless network which means sharing the same key for a long time is one of the security vulnerabilities where the attackers can break all the algorithm to crack private information. Because the access point administrator is not responsible of changing keys as the WEP don’t have any kind of key management facilities. For an example , loosing a laptop could be dangerous because the key could be compromised so it’s a good idea to keep changing the key.24bits of IV is too short and texts are very clear which are generated by the RC4 algorithm which might be repeating on a busy network where the hackers can crack the data to decrypt the ciphertext.[25] For every IV the small space was allocated where an attacker can make a table to break the key and if the key is identified then the attacker can decrypt all the data which was used by the IV. If the attacker was success in building the table for every key then it will be easy to break every packet sent through the wireless link which is known as the Dictionary Building Attack where the initialisation vector of WEP is a 24bit access target which can break IV in 5hours time only.

    **A face-recognition system installed at a busy airport is said to work with 99.99999% accuracy in recognising legitimate travellers. That is a one in a million chance of mistakenly recognising one person for another. How many people need to pass through an airport before the recognition system mistakenly detects one person as another. Describe and justify your argument in detail.**

    One person at a time has to pass through an airport before the recognition system mistakes generally the face recognition is appropriate in reading every individual face. [26] biometric or face-recognition is a technology which are becoming famous almost every airport uses these technologies in the modern world. These days facial recognition technique is more advanced than ever before but at the same time have issues with the privacy and protection of the information’s. while entering in a country the E-passport gates compare the picture in the passport against the face in the camera available there also scan the other information provided in the passport which takes around 6 to 10 seconds to complete the process. This process does work because in the database they have all the information about the person including the photo got through documents like Visa or some other source. The photo is recorded as a template than a real photo by making a map of the photo using various points on a face. So, during the face scan at the airport it makes another similar template and cross check the picture with the database and if the photo match 90% with the database the rest of the process happens fast in few seconds. I think it’s a good thing to have face recognition because face is the only sensitive data which cannot be changed and the increase rate of biometric data means the person can be identified at any time for anything it is a good technique to find criminals and prevent the country from any dangerous act to happen.

    **References:**

    24. <https://www.dummies.com/programming/networking/understanding-wep-weaknesses/>

    25.<https://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS7/Wireless%20Networking%20Security.htm>

    26. <https://www.businesstraveller.com/features/airport-facial-recognition-what-you-need-to-know/> [↑](#endnote-ref-18)