An investigation into cyber security in terms of costs, impacts and occurrence of current ICT issues in front of private sectors and electronic governments

MSc. Karwan M. Kareem

Abstract- Information and communication services have too much vulnerability that produces a new type of crime, illegal behaviour and bad activities such as stealing, attack and broke data onto the internet and communication tools. The growing of information and communication technology elements such as hand held devices, network and computer has caused increasing the risk of cyber-attack. Therefore, cyber security becomes a big issue, for today to protect information, catch the attackers and decrease the risk of cyber-attack, especially in front of private sectors and electronic governments.

Index Terms— Intruder, cyber-attacker, cyber-crime, free ware, pop-up programs, exploitations**,** Safe Cache, compromised system and disclosure

1. INTRODUCTION

In recent years, information and communication technology services have grown very quickly. Huge amount of data and information has processed, transformed and analyzed by ICT tools such as the hand held devices, Internet and computer. Consequently, ICT has affected different aspects of real life for instance the economy, society and industry that have influenced the infrastructure of our life, and changed our life to softer. However, information and communication services have too much vulnerability that produces a new type of crime, illegal behaviour and bad activities like stealing, attack and broke data via communication tools.

The growing of information and communication technology devices such as hand held devices has caused increasing the risk of cyber-attack. Therefore, cyber security becomes a big issue for today to protect data, catch the attackers and decrease the risk of cyber-attack. Cyber security has become a major issue especially in front of private sectors and electronic governments for many years. Cyber-attack cause of produce some private sectors, group and cyber security organization in different area around the world. The European Network and information Security Agency, the US Department of Homeland Security, the Council of Group, the Asia-Pacific Economic Cooperation and the council of European Cyber-crime Convention are most common cyber security organizations that try to protect data and information, decrease the risk of cyber-attacks and detect the cyber attacker. (ProCon Ltd, 2006).

2. Costs and Impacts of Cyber security

2.1 Increasing the number of cyber security users:

Nowadays, security sectors try to produce different kind of cyber security tools, devices and software's like anti-viruses, firewall and access control. These tools and software's used everywhere trough different level of sectors such as public, business and industry sectors, and also cyber security programs are used by numerous Internet users to keep their data and information. ProCon Ltd writes that according to a survey which was implemented by the Federal Bureau of Investigation (FBI) and Computer Security Institute (CSI). The implementation of this survey shows that approximately, most of the companies used cyber security tools and software's to protect their data, decrease the risk of cyber-attacks.

Moreover, the cyber security cause of raising the number of employees in private, business and industry sectors around the world. This study explores that cyber security cause of raising the number of internet and network users. Cyber security programs and devices cannot be perfect tool to detect all kinds of the risk of cyber-attacks, because day by day new technique of cyber-attacks are invented by cyber-attackers, increasing cyber-attack situations, and also the industry of security organization try to detect them. These affect cyber security which becomes too much expensive.

2.2 Frequent or Increased Occurrence of Cyber Security Breaches:

The cyber security products are increasing day by day, and also the number of cyber-attack situations still occurs frequently that effect increasing more risk of public data and information, increase public losses associated with cyber security breaches worldwide. According to ProConLtd the annual survey about information security shows that cyber security branches available everywhere. The same survey which was implemented by the Federal Bureau of Investigation (FBI) and Computer security Institute (CSI) in 2005, the result of this survey shows that about 50 present organization security employees that equivalent 693 computer security employees, these employees acknowledge that they did not have permission to use computer in their organization for 12 months in the last year.

CERT which is a Coordination Centre show that cyber-security vulnerabilities was rising about 35 present during the last ten years. In addition, the same center clams that 171 vulnerabilities occurred in 1995, and also 5,990 security vulnerability events occurred in 2005. Year by year most of people, organization, business sectors are attacked by cyber-attack and Malicious programs such as viruses, Trojans, worms and time bombs around the world without any perfect solution to stop these dangerous programs that have been a big issue in front of public data and information.

2.3 Increasing losses of cyber security-attacks or breaches:

Gradually, the number of cyber security events and vulnerabilities occurs frequently. Consequently, the losses of these cyber-security attacks and vulnerabilities are rising as soon. ProCon Ltd claims that the costs of cyber security can classify into two main categories which include direct losses and indirect losses. ProCon Ltd writes that it is not easy to know what the costs of cyber-attacks are. On the other hand, the losses of these attack events are increasing regularly. The Metro online newspaper claims that cumbersome costs Britain almost £1,000 every second, this newspaper show that cyber-attacks are costing the British economy £27billion a year.

These losses just occurred in the UK. We can ask how many losses occur every day around the world via cyber-attack and cumbersome that is not easy to measure all these costs. Everyone probably can imagine that is a big issue in front of cyber-security. The direct losses are occurring by cyber-attackers directly for instance attack the security and access control of business sectors, recovering business systems and update data and information, this kind of losses directly involve with cyber-attacks. However, the indirect losses indirectly involve with cyber-criminals, for examples, decreasing of stock prices. Cyber-security causes losses for different sectors, organization and government second by second that will produce negative points for public economy in future. This study has explored that a main effect of cyber-security has been economic costs and public losses.

According to McGuinness, the effects of cyber security attacks come in four flavors: disclosure, theft, integrity, and denial of service.

2.3.1 **Disclosure:** this is a kind of security threats which illustrate the dangerous security situation that describes specific events when secrete information is obtained by dangerous gays through one kind of cyber-attack. This secret data may be business, national security and government information. This threat may be influenced from individual person to public and national security.

2.3.2 **Theft:** which describe about that when attacker steal some valuable information by using a specific attack technique via the internet. This useful information may include credit card number, user name, passwords, personal information and business data. In this type of cyber security threats, most time attackers use frauds to attack victims to obtain their aim.

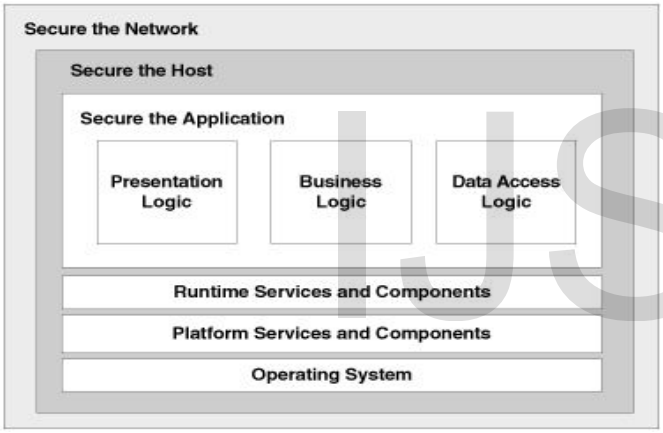
2.3.3 **Integrity:** involve with several types of attacks which make negative impacts of the system, these may be directly damaging, modify the system attributes and broke some system components. In the integrity threats, the cyber attacker use different attack tools and malicious programs like virus, worm, time bomb and Trojan. Each of these attack programs produces some problems with computer base system components.

2.3.4 **Denial of Service:** This is full blocking of online web services via using several professional hacking mechanisms with perfect hacking techniques to access specific network. For instance, denials of service mechanisms which are very critical technique to broke communication technology services such as websites, telecommunication and phone services. Most security technology experts suggest that denial of services is more threat than other cyber-attack techniques.

3. Protecting the web: what makes it so challenging

Developers cannot build confidential web projects without knowing threats and vulnerabilities in there web

application. Web application developers have to identify their web application vulnerability area that may assist them to prevent malicious programmer who want to exploit web application security. In addition, developers should follow threats modelling to identify their system vulnerabilities. The main goal of using threats modelling to analyze their web system architecture, and also finds threats area. The threats modelling assisted developer to know what are the web application vulnerability that helps them to build the system with using security principles. They have to use secure coding technique to prevent vulnerability areas. Web developer have to use secure network to support web application layer, and also they have to use secure host, best configuration technique and confidential web server that assists application layer which become more comfortable. In general, web programmer has to follow three security layers, which are network, host and web application layers **(Meier, et al, 2007)**.



Three layers of web application security - figure .1 **(Meier, et al, 2007).**

Carlos Lyons from Corporate security in the Microsoft Company writes that "A vulnerability in a network will allow a malicious user to exploit a host or an application. A vulnerability in a host will allow a malicious user to exploit a network or an application. A vulnerability in an application will allow a malicious user to exploit a network or a host." ***(Meier, et al, 2007).***

3.1 Securing your network:

A confidential web system refers to secure network components. The security of network infrastructure involves with network elements such as firewall, router and switch. This layer of security includes security administration interface, strong security number, ensuring the integrity of the traffic and protecting networks from TCP/ IP attacks.

3.2 Securing your host:

A secure host involves with the security of host infrastructure which consists of software and hardware elements. The security of hosts according to different type web hosts such as web server, application server and database server. Each one of them has some specific threats and vulnerability area, and also they have different security layers like patch, ports, services, directory, registry, auditing and login. Therefore, the web service developer should concern about all these layers to prevent an attacker and *malicious programs*.

3.3 Securing your application:

Evaluating of web application vulnerabilities is an efficient approach to make confidential web application security. The following bullet points show all security layers which are very critical to **make challenge web application security**, these security layers involve with different type of web application vulnerabilities: ***(Meier, et al, 2007).***

3.3.1 **Input validation:** this layer of web application security can filter and check input data before any additional processing. This layer assists web application to know which input data are safe.

3.3.2 **Authentication**: which involve with this question" who are you?" This security layer identifies who is user or who is not user that assists web application to accept user accounts and reject someone who is not used, such as, password and user name are a real example to authentication layer.

3.3.3 **Authorization**: which mean that "what can you do"? This layer of web application security shows the access control for web application resources and operations.

3.3.4 **Configuration management**: this security layer describes that how manager configures the administration level of web application, and also how the administration properties is secured.

3.3.5 **Sensitive data:** this security layer concern about that how web applications can keep and protect sensitive data and information in front different level of users.

3.3.6 **Session management:** this layer illustrates that how web applications can protect sessions which

are the set of interactions between users and web application services.

3.3.7 Cryptography: this security layer explains that how web applications can protect secrets through encrypting data and information.

3.3.8 Auditing and login: this describes that how web applications can monitor and capture any events which related to web application security. Moreover, parameter manipulation and exception management are two further security layers which affect web application security.

In addition, the developer has to concern about all these web threat areas and *vulnerabilities to build secure web applications, these security layers assist web application to prevent* malicious codes and dangerous software's.

4. How cyber-attacks are made?

In general, intruder has used a different approach to attack victim's system. The type of attack involves the goal of attacker to obtain gain. Day by day, intruder invents new attack approach. Therefore, it is not easy to measure and identify all methods of cyber-attacks. This paper tries to describe most common attack methods.

4.0 Computer and internet cyber-attack methods:

4.1 First method of cyber-attack: Class of Malicious software:

Malicious software's, malwares or crime-ware are harmful programs which are produced to crash, spies and disrupt computer system software's. Most types of malware able to produce negative effects for computer system software. However, these programs cannot absolutely impact on the computer hardware elements. Some of them can install, reproduce and hide themselves by using other computer programs which known by host programs for instance Kaza, iMesh.

Malwares can change their location, and move from computer to other. Some kind of crime-ware like worms able to install themselves without using other execute programs that assist them spread in different hosts very quickly. Another kind of Malicious programs such as Trojan which allows an intruder to access and control complete part of the victim's computer system. Further type of malware programs is spyware which able to monitor victim activity. In general, the most common type of malicious programs is:

- Computer viruses
- Worm
- Trojan
- Spyware

4.1.1 Computer viruses:

In general, viruses are dangerous programs which are produced by intruder to attack victims, obtain gain. Computer viruses able to install itself in victim's computer system; they can become a part of other programs. Viruses can reproduce themself by using other system executable files. They can move from a specific part of hard drives and memory units to other, they able to spread from specific computer to other, this mean that viruses can change their location through communication services such as internet, networks, E-mails and external hard disks that assist the cyber-attacker to publish them around the world. However, viruses are not able to publish until a victim open excusable file "host file". They can hide themself that keep them in the live, normal users cannot detect them without anti viruses. Some types of viruses are dangerous programs which can crash complete victim's computer system. Some kind of them just decreases the speed of the system; change a system too busy through using power of system units which relate to the speed of victim's computer system. Some of viruses, which are produced just for funny, do not make any risk for system. (Cisco website).

4.1.2 Worms:

Worms are similar with the computer viruses in more aspects as both of them are type of malicious programs. Worms are able to replicate and copy themselves. They can install and run themselves in the victim's computer system. They are able to produce negative effects for the system that may cause some type of system damages. Worms are not dependent with other programs "host programs". The main property of worms is that they try to discover other computer addresses that assist them to move from one computer to other in the same network, they publish from specific network to other for instance LAN to LAN networks. This behaviour assists them to spread around the world very quickly.

The key dissimilarity between worms and virus is that worms are independent programs, and also worms do not require other programs "host programs" to spread in different systems. Viruses depend with other programs which known as "host programs", they cannot work without host program. (Erbschloe, 2005).

4.1.3 Trojan:

Trojan is a dangerous part of specific program. The main purpose of creating Trojan is that intruder produces Trojan to access another system to stealing sensitive information. Trojan able to create back-doors, this program assists

malicious users to inter other systems. Trojan can damage victim's system files such as dropping files, stealing sensitive data, alter file setting and publishing other malwares. Moreover, Trojan dissimilar with worms and viruses as Trojan cannot copy, install and reproduce itself. Trojans have to spread via user activity like sending e-mail. For instance, when a victim checks an E-mail attachment, download and execute malicious files from the internet. According to (Erbschloe, 2005) Trojan can achieve or create the following attacks on the infected system:

- Trojan can remove files from the infected system.
- Trojan can download files to the infected system.
- Trojan can alter the registry of the infected system.
- Trojan can drop files from the infected system.
- Trojan can change the name of files "rename files" from the infected system.
- Trojan can stop some components of infected system such as mouse, keyboard.
- Trojan can lock, shut down and restart the infected system.
- Trojan can disable computer security tools such as Anti-Viruses.

4.1.4 Spyware:

Spyware is a malicious and crime-ware programs. These type of program uses to steal information from infected systems. Nowadays, numerous online thefts, cyber-attacker uses spyware to obtain knowledge about victims. This program able to use different methods to spread itself on the infected systems; Spyware can spread itself through freeware programs, via shareware computer applications. File sharing is another approach to spread spyware in peer to peer networking. Most kind of spyware probably has not produced to harm and crush victim's systems, but the main purpose of producing this program is spied other system by intruder obtain sensitive data, for instance, user name, password, credit card numbers, birth date and social identification. In general, spyware can do the following acts: (Jakobsson, 2008).

- Spyware can gather sensitive information from storage devices of infected system.
- Spyware able to monitor victim activity such as typing on the keyboard, browsing websites and so on.
- Spyware able to steal personal information from infected computer such as user name, password and credit card number.
- Spyware can collect information about infection system like hardware and software properties, what programs are installed by the victim.

4.2 Second method of cyber-attack:

4.2.1 Denial-of-services attack techniques (DOS):

Denial-of-services attacks are professional techniques to attack hosts and online services through using a flood of packets. These techniques are more critical than other type of attacks to prevent networks. Most professional cyber-intruders probably use denial of service method to occur cyber-crimes. These techniques have produced numerous risks to online users, organization services and the infrastructure of worldwide web services. The major purpose of this technique is that

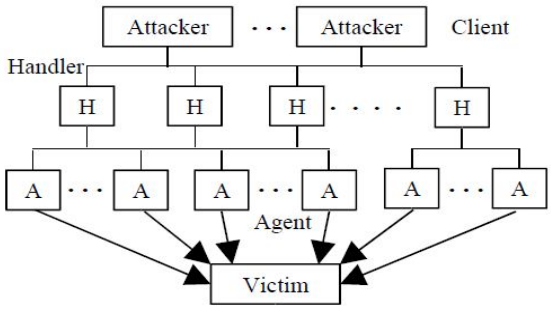
- Intruder able to obtain secrete data through DOS techniques.
- Intruder can use DOS methods to prevent and control hosts.
- Intruder able to prevent the internet, disable online services.
- Intruder able to monitor pocket traffics, broadband.
- The Intruder uses DOS to prevent most computer system components and network systems.
- Intruder able to install and execute their programmers, modify data on the victim's systems.

In General, most cyber attackers' probably use distributed denial of services DDOS techniques to control numerous computer systems together, prevent huge area of network system to obtain different goals from the victim's machine. The aim of cyber-intruder to using DDOS is stop online web services without deleting, modifying data. However, some of them use DDOS to alter and defect sensitive data like international information security. Consequently, user accounts cannot access the online service provider, this make more risk for web users to doing their daily works online, these produce non normal situations which affect other online service sectors such as business, education sectors, and also privet and government sectors cannot comfortable to use the Internet. Specht claims that DDOS include two most common techniques, the Agent-Handler model technique, and the Internet Relay Chat (IRC) Technique:

4.2.1.1 Agent – Handler attack model technique:

The Agent – Handler model technique consist of three main elements which have role to occur these types of attacks. The first part is a client which is a specific computer system. This part is used by an intruder to connect to the DDOS attack system. Second part is a Handler; the handler is a

software package which has role to make relationship between intruders "clients" and agent. Last part of this technique is an agent, the agent is a cyber-attack software which install on the other computer system which known "Compromised system" or first victim, this system is used by an intruder to attack the other destination which known second victim. In this technique the intruder uses one or more handler to attack destination through the client system without any knowledge of Handler user. In this attack technique, the first victim is handlers, and the second victim is agents which are attacked by a cyber-hacker through using a client system (figure .2). (Specht, 2004).



DDOS Agent – Handler Attack Model technique - figures .2 (Specht, 2004).

4.2.1.2 IRC – based DDOS technique:

IRC – based is a second technique which is used to attack network and hosts. IRC which is a short of Internet relay chat. IRC – based DDOS have same processes which are available in the agent – handle attack technique instead of that the handler software has to install and execute on the destination network server. The architecture of this cyber-attack technique consists of client, IRC and agent. IRC is a communication channel or web servers, these web servers use to make the relationship between cyber-attacker "client and agent", agent is a first victim which is the main approach to attack second victim. IRC channels have some advantage which assists cyber-intruder to attack specific dispensations. (Specht, 2004).

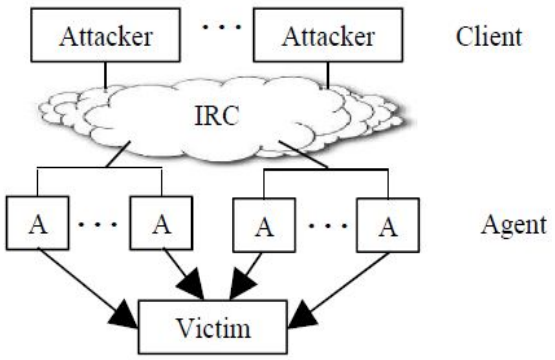
IRC channels include "legitimate" IRC ports which can be used by a cyber-intruder to send attack commands.

- IRC channels able to change DDOS attack commands to more strong which help cyber-intruder in the attack process.

- IRC web servers provide the list of all available agent web servers that assist the cyber-intruder to discover, select their destination, hosts.

- The IRC network server support agent software packages which installed by cyber-attackers on the IRC network servers.

In general, the cyber-attacker uses an IRC channel to attack the first victim which is agent web server, and also they use agent web server to attack the second victim which is specific host and more, and also an agent has a good role to produce connect between cyber-attacker "IRC channel " and second victim. (Figure.3).



IRC – based DDOS attack technique - figure .3 (Specht, 2004).

4.3 Third method of cyber-attack: XSS attack technique:

XSS is a short of cross site script which is the most common technique to attack web application today. This technique is the use of attacks client side or particular part of websites. This technique cannot make a negative point for website structure, prevent and stop websites. The architecture of cross site script consists of three main parts which include attacker, client and website. The main purposes of cross site scripts are:

- Intruder can use XSS to steal cookies from the client side.
- Intruder can obtain sessions from the client side.
- Intruder able to obtain sensitive information from client side such as credit card number.

In addition, Java scripts have a good role in cross site script attack techniques. The intruders use malicious script codes to attack clients. They execute malicious java script cods in client's browsers. These malicious codes able to obtain sensitive data from victim browsers, for instance, sessions, cookies, and sending back to the attacker. (Klein, 2002).

5. Protect web system against cyber-attacker, catch the attacker

Cyber security which contain of several professional technique that involve with decreasing the risk of cyber-attacks to information technology elements such as software, computer hardware and network. Cyber security provides different useful tools which are very important to detect dangerous programs like viruses, Trojans and malware. This includes common security techniques such as encoding and decoding data. **ProConLtd** states that cyber security is a comparison among dissimilar security techniques and measurers. Cyber security describes the comparison among security and attack techniques. In recent years, cyber security has become a big issue in front of private sectors, researchers and governments, because the risk of cyber-attacks increase day by day that involve with using technology tools everywhere to process all kinds of data. In general, there are several security techniques to decrease cyber-crime or cyber-attacks. This research tries to describe the most common cyber-security technique like spyware protection technique, firewall and router. (Amoroso, 2007).

5.1 Spyware protection technique: (catch or defect spyware):

There several spyware protection approaches which are very useful to protect computer data, for instance, toolbar solutions, free ware solutions and licensed solution. These solutions are very critical to defect pop-up programs. Some of anti-spyware are free, everyone can use them without any licensed. However, some of them are not free, you have to pay licensing key. According to (Baskin, et al, 2006) spyware solution classifies to three main categories.

5.1.1 Toolbar solution: these types of anti-spyware like Yahoo anti spy toolbar, 12Ghosts popup-killer and Google toolbar work with browser to catch spyware. Toolbar anti-spyware tries to protect computer browser of pop-up programs. These toolbars defects spyware before you process them.

5.1.2 Freeware solution: this category of anti-spyware is free, they work without any licensed. These tools cannot catch whole type of new model of spyware.

5.1.3 Licensed solution: licensed solutions are another kind of scanner which can protect computer data. This anti-spyware is very critical to catch spyware and popup-programs. However, licensed solution tools are not free, you have to pay to obtain licensed key as they cannot work without licensed key such as MacAfee anti-spyware, Webroot spy sweeter.

5.2 Firewall and router protection technique:

Firewall is a useful network security system which is very critical to protect computer system and networks of cyber-attacks. Firewall can limit, filter and monitor all types of pockets which want to pass from fire wall; packets are small element of data which can transfer between different computer systems via network protocols. Firewall systems decide to which pocket can access to computer, network, and also which packet has not permitted that depending on the configuration of the firewall. Moreover, firewalls can reject malicious traffics, dangerous data from or to a computer system to other computers and networks. This may be a software program or hardware devices. For instance, a router is a hardware device which can filter, monitor data and network pockets because the router can configure to define a set of IP addresses or specific IP addresses, and also router can monitor network malicious traffics. Therefore, router and computer firewall systems are very important to protect, prevent computer and networks of dangerous programs, cyber-attacker. (Sriram, 2002).

5.3 XSS attacks protection technique:

In recent year, cross site scripting security has become a complex problem in front website developer. There is not complete solution to avoiding this complex problem, because browsers run every piece of Java script cod and other type of scripting language, and also the browser do not know which script code is useful cod or which one is malicious script code. Web browsers cannot defect all kinds of malicious java script cod. Most programmers cannot build a fully secure website that assists cyber-attacker to discover their Variability. Consequently, an intruder can inject their script cods into a browser that assist them to obtain sensitive data to attack victim website. Victims do not have any idea, when intruder attacks their browser. All security tools such as anti-viruses, anti-spyware and other security tool probably cannot prevent, defect malicious script code or XSS attacks, because all these security tools focus on earlier malicious, they do not know anything about current malicious scripts. According to Grossman there are two main approaches to decrease the risk of cross site scripting: (Grossman, et al, 2007).

5.3.1 Data input and output filtering technique: Input and output filtering is a critical approach to stop cross site scripting attacks. This is checked of input and output data through using specific script programming language, for instance, java script programming. Using script language is a critical approach to check malicious codes. Programmer use Java script to filter input-elements of the

webpage interface like "text boxes" that decide which form of data is suitable to enter through text boxes and which kind of data is not suitable and danger.

5.3.2 **Web browser security technique:** this technique involves with the type of web browsers. The most common point is that which browser is very secure, and which one of them has more vulnerability. Today, a huge number of security tools and plug-in available to protect web browser such as No-script, Safe Cache, E-boy tool and Google toolbar. This browser plug-in assists web user to protect themselves of cross site script variability such as certain suffers.

6. Cyber-security challenges:

6.1 Multiply Entry points: entry points are one of the most common challenges in front of developer to build secure web applications. Web 2.0 is a new generation of web application which have more entry points than older web applications. Increasing the number of entry points causes an increased number of variability. Therefore, web 2.0 applications have more threat than web 1.0. Multiply the number of entry point's affects developers to become busier that probably makes more coding errors. Therefore, each entry point has to be tested by developer to decrease the number of security problems. (Shreeraj, 2007).

6.2 Dependencies: older generation of web application which is web 1.0 application, this generation had a limited number of technological dependencies. However, a new generation of web technologies has numerous technology, data sources and protocols. These technologies dependently work together that make more risk of web security issues. Multiply technologies cause increasing Vulnerability. Therefore, the dependency between different web application technologies is one of the challenges in front of cyber-security issues about web 2.0 application. (Shreeraj, 2007).

6.3 Vulnerabilities: Older version of web application had a limited number of vulnerabilities which involve with server-side security that made a limited number of risks. However, the risks of web 2.0 application involve with different aspect of web technology which includes vulnerabilities of server-side and client-side. These vulnerabilities cause of increasing new cyber-attack techniques which are very critical to attack client-side. Nowadays, profession techniques are used to attack client-sides such as Cross site script, SQL Injection. Most cyber-intruder probably use cross site script technique to steal secure information via using client-side vulnerabilities. An increasing number of vulnerabilities in front of web 2.0 applications have become the main challenge in front cyber-security. (Shreeraj, 2007).

6.4 Exploitations: A web 2.0 application has provided a complex structure of web technology that has made more new vulnerabilities in the web infrastructure. This cause increases exploitation in client-side and server-side. A new generation of web application has produced new threats, provided a new mechanism for old threats. Cyber-attacker use soft exploits to attack victims system by using client-side vulnerabilities that make more risk in front web cyber-security. (Shreeraj, 2007).

7. Conclusion:

In conclusion, cyber security is a comparison among dissimilar security techniques and measurers, and also it describes the comparison among security and attack techniques. Using ICT services by private sectors and electronic governments cause too many threats that produce a new type of crime, illegal behaviour and bad activities like stealing, attacking and broking data. Complexity of new technology infrastructure has more entry points, data sources and protocols. These dependently work together that make more risk for cyber-security, and also increasing the number of entry points causes an increased number of vulnerability. This cause increase exploitation in client and server side technologies. Cyber-attacker use soft exploits like cross site scripting, SQL Injection to attack victims system by using client-side vulnerabilities that make more risk for web cyber-security.

In closure, this study explores that it is not easy to measure and identify all methods of cyber-attacks. Cyber security programs and tools cannot be perfect tool to detect whole risks of cyber-attacks, because day by day new techniques of cyber-attacks are invented by cyber-attacker. Increase occurrence of cyber security breaches caused raising the number of internet users, and also increasing losses of cyber events regularly.

REFERENCE

[1] Amoroso, A. (2007) *Cyber security*. London: Silicon Press. [Online]. Available at: <http://library.books24x7.com.libaccess.hud.ac.uk/toc.aspx?site=MVJ2L&bookid=15450>. [Accessed 23 NOV 2011].

[2] Bayazit, A., Huang, Q. And Specht, S. (2002) *Distributed Denial of Service Attacks*. [Online] available at:

<http://www.scribd.com/doc/54150438/18/DDoS-Case-Study-GRC-com-7>. (Accessed 12 NOV 2011).

[3] Baskin, b., Bradley, T., Faircloth, J., A Schiller, C., Caruso, K., Piccard, P. And James, L. (2006) *Combating Spyware in the Enterprise.* Rockland: Syngress.

[4] Cisco website, ( ) *Cisco Security Intelligence Operations: what is the difference: Viruses, Worms, Trojan and Bots. Available at :<* http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html#3>. [Accessed 23 NOV 2011].

[5] Erbschloe, M. (2005) *Trojans, Worms and spyware A Computer security professional's Guide to Malicious Cod.* Oxford: Elsevier Butterworth-Heinemann.

[6] Grossman, J., Hansen, R., D. Petkov, D. And Rager, A. (2007) *XXS Attacks: Cross Site Scripting Exploits and Defense. [Online]. Available at* <http://library.books24x7.com.libaccess.hud.ac.uk/toc.aspx?site=MVJ2L&bookid=25446>. [Accessed 3 DES 2011].

[7] Jakobsson, M., Ramzan Z. (2008) *Crimeware: Understanding New Attacks and Defenses*: Addison-Wesley Professional.

[8] Klein, A. (2002) *Cross Site Scripting Explained.* [Online] available at: <http://crypto.stanford.edu/cs155/papers/CSS.pdf>. [Acceded 30 NOV 2011].

[9] Meier, J.D., Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R. And Murukan, A. (2003) *Improving Web Application Security: Threats and Countermeasures* . [Online]. Available at :< http://msdn.microsoft.com/en-us/library/ff648636.aspx#c01618429_004>. [Accessed 12NOV 2011].

[10] McGuinness R. (2011) *Cyber-crime costs Britain £27bn a year.* [Online web site]. Available at: <http://www.metro.co.uk/tech/855887-cyber-crime-costs-britain-27bn-a-year>. [Accessed 20/11/2011].

[11] ProCon Ltd. Sofia (2006*) information and security: cybercrime and cyber security*, volume 18 [online journal].

[12] Sriram M. S. (2002) *Firewalls.* [Online]. Available at: < http://library.books24x7.com.libaccess.hud.ac.uk/toc.aspx?site=MVJ2L&bookid=13502 > [Accessed 30 NOV 2011].

[13] Specht, S., Lee R. (2004) *Distributed Denial of Service: Taxonomies of Attacks, Tools Available at:*<http://palms.ee.princeton.edu/PALMSopen/DDoS%20Final%20PDCS%20Paper.pdf> [Accessed 27 NOV 2011].

[14] Shreeraj, S. (2007) *Web 2.0 Security: Defending Ajax, RIA, and SOA. Boston: Course technology.*

MSc. Karwan M. Kareem
Karwanmus@yahoo.com
University of Sulaimani
Faculty of Physical and Basic Education
Department of Computer Science