Towards A Safe Internet Usage In Iraq

A.L. Eng. Hassan Harith Jameel
Department of Computer Technologies Engineering\
Al-Turath University College
Email:hassnjameel@gmail.com

Abstract

High percentage of the Iraqi people are using computers, most of these people use Internet applications.

Many computer problems facing these people. Majority of these problems are software, related to improper work of operating system, loss of response, corruption then loss of data, etc. These problems mostly came from bad computer usage when dealing with Internet, or using a bad copies of operating system or Internet security programs, or bad habits that are now familiar.

This paper discusses the way that most Iraqi users behave when using the Internet, and suggests that implementing proper security together with good behavior will lead to safe computer and Internet usage, through improving the user's knowledge of security, and raising the standards of knowledge of the computer itself.

Keywords:
Computer Security, Hackers, Crackers, risk, threat, attack, vulnerability, Internet Security, embedded scripts, ISP (Internet Service Provider).

نحو استخدام امن للانترنت في العراق

المدرس المساعد المهندس حسن حارث جميل

hassnjameel@gmail.com

المستخلص:

هناك نسبة عالية من العراقيين يستخدمون الحاسبات, معظمهم يستخدمون تطبيقات الانترنت.

وهناك مشاكل كثيرة تواجه هؤلاء المستخدمين. غالبية المشاكل هي مشاكل برامجية, تتعلق بسوء اشتغال نظام التشغيل, او فقدان استجابة الحاسبة للاوامر, او تخريب وضياع المعلومات, الخ. هذه المشاكل تاتي غالبا من الاستخدام السيء للحاسبة عند التعامل مع الشبكة العالمية (الانترنت), او استخدام نسخ غير جيدة من نظام التشغيل او برامج امن الانترنت, او العادات السيئة التي اصبحت شائعة في الوقت الحاضر.

هذه الدراسة تتناول السلوك الذي اعتاد معظم مستخدمي الحاسبة في العراق اتباعه عند استخدام الانترنت, وكيف ان التامين السليم للحاسبة الى جانب السلوك الصحيح سيؤدي الى استخدام آمن للحاسبة والانترنت, من خلال تحسين معرفة المستخدم بامن الحاسبات وبالحاسبة ذاتها.

Introduction

Today when talking about computers, computer networks and using them safely, security is the most important issue that needs to be addressed. The threat of cracking is obvious in organizations that incorporate computers in their job; of course today almost all the organizations and companies include the use of computers and computer networks. Cracking may face the company from individuals within the organization, Employees or former employees with malicious intent or who wants to obtain information are also a threat to an organization's computers and networks. [1].

Dangers like virus, worm, cracking, and any term that many people here in Iraq and all over the world talking about need an inside help to be able to get inside the networks and hence the computers, these terms depends highly on the user's ignorance in computer work or in computer security. Bad intention people depend on the user's ignorance in important or small details that may lead to compromise his computer in any way. Crackers may use some primary information to crack computers or tell any user about wrong information making this person open his security measure in some way. The problem is that people talking with these terms and want to avoid them but they behave in a way which is so friendly to them!!

In the early 1990's, when the Internet usage was not spread like today, no one would hear about security vulnerability except perhaps in a major magazine or newspaper. At that time news release typically applied to an old version of software that most of the users no longer used anyway [2].

This paper will first introduce some general information in section one, some facts must be defined and stated, since this paper is for any person who is working on computers.

Section two will include the problems here in Iraq and solutions that can fix these problems.

1. General Information

1.1 Security definitions

Many definitions have been suggested for the term security, some said that "It is freedom from risk", others said that "It is absence of risk", and others said that "It is freedom of the risk's negative effect". The definition which mentioned "it is the freedom of the risks negative effect" may be nearer to what is needed than the others because the risk might still exist, but you are free to act or not in spite of that risk. Sometimes you can eliminate specific risks; sometimes you cannot eliminate that risk but still act with that risk looming [3].

Three key principles can be considered as the axis that network security revolves around, confidentiality, integrity, and availability. The importance of each principle can vary from application to another, i.e. confidentiality may be the important principle in some places, while availability may be the important factor in other places, and so on. For example, an agency would encrypt an electronically transmitted classified document to prevent an unauthorized person from reading its contents. Thus, confidentiality of the information is the highest priority principle here. If an individual succeeds in breaking the encryption cipher and, then, retransmits a modified encrypted version, the integrity of the message is compromised [4].

1.1 Security issues in the Internet

The Internet insecurity may refer to many reasons; according to [5] these reasons may include:

A. *Lack of education*: since the education is the most important aspect of security, learning about what is happening inside the Internet and the risk that may face the networks and computers will help to reduce the effect of these risks on the network.

B. *Internet's design*: which include for example the client/server model and certain amount of anonymity is allowed; add to that the heterogeneous networking is now confusing, for example, if a file need to be retrieved, there are many protocols which can handle this issue, FTP, electronic mail, HTTP with browser, and other protocols. Each of the protocols mentioned forms one aspect of the modern Internet. Any machine running modern implementations of TCP/IP can utilize all of them and more. Security experts have for years been running back and forth before a dam of information and protocols, plugging the holes with their fingers. Crackers, meanwhile, come armed with ice-picks, testing the dam here, there, and everywhere.

C. *Proprietarism:* is a practice undertaken by commercial vendors in which they attempt to inject into the Internet various forms of proprietary design. By doing so, they hope to create profits in an environment that has been previously free from commercial reign. A good example of proprietarism in action is Microsoft Corporation's ActiveX technology [5].

D. *The trickling down of technology*: today cracker has tools at his disposal that most security organizations use in their work; add to that the powerful machines that the crackers can use to run these tools which allow an efficient hacking.

E. *Human nature*: human by nature, is lazy. To most users, the subject of Internet security is boring and tedious. They assume that the security of the Internet will be taken care of by experts [5].

1.2 Terms must be avoided: risk, threat, attack, and Vulnerability

Dealing with security means first knowing some terms that are frequently used in conjunction with security, namely risk, threat, attack, and vulnerability.

Risk can be defined as the chance of something going wrong, the danger that injury, damage, or loss will occur [6]. Someone can say the risk of losing the file, or the risk of compromising the computer, no matter how this risk is done.

Threat can be defined as declaration of intent to cause harm, the expression of an intention to cause harm or pain [7]. From the computer security point of view threat is an action or potential occurrence (whether or not malicious) to breach the security of the system by exploiting its unknown vulnerabilities. It may be caused by either gaining unauthorized access to stored information, or denial of service to the authorized users, or introduction of false information to mislead the users or to cause incorrect person, trusted or mistrusted, who want to break into, steal, cause damage, manipulate, or deny access to your information assets [3].

The term attack is an assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system. Attack can be active or passive, by insider or by outsider, or via attack mediator [8].

The term vulnerability in computer security is the weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. To be vulnerable, an attacker must have at least one applicable tool or technique that can connect to a system weakness. In this frame, vulnerability is also known as the attack surface.

A security risk may be classified as vulnerability. Vulnerability with one or more known instances of working and fully-implemented attacks is classified as an exploit [9].

2. Problems and Solutions

2.1 Security issues in using the Internet

Getting secured 100% is hard to reach, in section 1.1 there was an agreement that the security is "The freedom of the risk's negative effect" since the risk is existing and developing exactly like the development of the security, here the question can be changed, are users behaving in a way which makes them free of the risk's negative effect? Unfortunately, the answer is no.

Today high percentage of Iraqis are using computers, and most of the applications used today need the world wide web, these users may be divided into four categories:

I. Users who don't care how the computer works, what are the risks of using the Internet, and if their computers works properly. This is reflected by using computers without thinking of the meaning of security. Unfortunately, this category probably represents most of the users in Iraq.

II. Users who think that they know what a computer is and they may hear of the Internet and its security. These users may be categorized into two subcategories:

   A. Users who care to put a robust and reliable Internet security application in their computers, at least they are trying to get an original and well known application, but their ignorance to what they think it is correct makes their behavior sometimes dangerous.

   B. Users who also care to put an application which makes them feel secure, but these users don't care to the source of this application, they may get it through the Internet for free, or may took it from some computer stores by using flash memory with a crack!

III. Specialized users with computers such as computer engineers or computer programmers. These users have studied the computers and computer applications and they behave badly. Unfortunately users of this category behave exactly like category number one and two, since they don't believe or even they did not understand well what they have studied. The major problem here is that they are guiding users of category number one and two to the wrong way of using the computers and Internet, since they are assumed to be experts!

IV. Well educated specialized users with computers such as computer engineers or computer programmers, or even users from other branches. These users have studied the computers and computer applications and they well know what risks may face them. They behave correctly and professionally with the computers and they are doing their best in avoiding Internet risks, by installing good Internet security applications and their good behavior which optimizes the risk to its lowest percentage.

The problem here, the existence of the first three categories will affect the entire security of the Internet especially with users in the same broadcast domain. The fourth category may be affected since Internet risks will exist in the domain they are working with.

This is the way that may affect all computers in the same network or domain. Any computer which has poor security will be the easy way to the risk to affect all the computers in the network. Because of that, professional people have studied the way of securing computers using hardware firewalls inside the network as well as in the perimeter of the network.

2.2 Internet security Application

Internet security application is an application which can recognize risks, vulnerability, attack, and threat with the Inbound or outbound stream, and try to either remove them directly, or tell the user that certain program or website has one of the dangers mentioned above.

So can we say that the Internet security application is the only way to protect the computer? Is it enough? The following example will show that it is not.

In 2000 DARPA and Sandia National labs tried to prove that Internet security application is sometimes the way which makes the user of the computer feels secure [10], but in reality it is not. They let the Red team to craft an email message, with an embedded script, and then they sent it to the workstation protected by software firewall. When the user opened the email, the script executed with all of the privileges of the user. The script turned off the firewall completely, but left the firewall icon on the screen. So now the firewall is turned off and the user has a false sense of security [10].

The goner worm circulated in 2001, this worm disabled then deleted anti-virus and software firewalls.

Some of the most effective ways to compromise a client in 2007 is by enticing the user to activate a malicious executables, send the user a link that may host a malicious content [10].

It is obvious that Internet security application is not enough by itself, this subject can take many paths of discussion, one of these paths is how to improve security by putting another security measure other than Internet security application inside or even outside the computer[11, 12], but the aim of this paper is to discuss how good user behavior can improve the work of the Internet security application and help it work effectively, this may be the start of all other paths that this subject may take, since putting additional security measure maybe costly, or difficult to implement.

2.3 Computer is a System

Most of the computer users do not know what is the importance of getting a genuine operating system or genuine Internet security application. On the contrary these people may laugh if you asked them to buy original software, but they don't know the risk of installing a cracked programs, and they think that it will not affect the proper work of the computer.

Here there is a need to make a point clear, that the computer is a system, consists of hardware and software, the software drives the hardware, and if anything wrong with this software will lead to the wrong point when executing a program, or requesting for website, because dangers always trying to find holes. Cracked applications or operating systems provide these holes.

In the previous sections there was a talk about embedded scripts, these scripts are executed once the user install the software containing them, so with a software which is not original there is a possibility that a cracker put an embedded script which will use it to compromise the computer, and this will lead to unfixable risk since no Internet security program or firewall will detect this type of risks and will consider this script as part of the system that the computer need to run properly. Many people face a continuous problems which cannot be fixed even with formatting the device and installing a fresh copy of operating system, when asking a professional users it appears that they are using the same cracked copy of operating system and they avoid using an original copy of operating system, or using a cracked Internet security.

Operating systems represents the platform that applications work onto, the application depends on the operating system in carrying the user commands to the hardware, and get the appropriate response. Using non-original operating system lead to noticeable or not noticeable bugs that will affect the proper work of the application, also using a cracked Internet security may lead to affect the proper work of the entire system.

There is another point, that most of the commercial operating systems like Windows, and all the Internet security programs have an update system and servers. These servers are connected to computer through the Internet, once the operating system or the Internet security installed, these servers will check for the genuineness of the operating system and the Internet security, if they find out that they are cracked or copied in some way, they will block them and will send bad executables which harm the proper work of the computer. Knowing that those companies are the programmers of this operating system or Internet security application, compromising the computers containing their programs is a matter of opening a locked door with its keys!

2.4 Solutions to be secured

Being secured as seen from the previous sections is a behavior more than an application to be installed, it is thought that there must be some disciplines that users must stick with them to be secured, like any disciplines for any system such as the traffic system.

Essentially the following points must be taken into consideration if there is a need to start a new behavior lead to secure networks:

1. Users must have a good introduction to computers as a system, and the difference between using an Internet and non-Internet application, since using the Internet means that this computer is now dealing with the external world which may contain good and bad servers and computers.
2. Users must be educated correctly. Education here comes from two resources, either by specialized institutes which have instructors who are authorized to answer any question correctly and professionally. Or by reading specialized books with well reputations and professional authors, which give. Many people depend on the Internet in learning, this is not correct behavior especially if this person is trying to understand a subject for the first time. Internet is an open environment anyone can write any information without any responsibility. Selecting a reliable site for learning is so difficult especially for the first time learning people.
3. Who to ask if a problem exists: this point has two branches:
   A. Anyone trying to answer any question: there is a bad habit in our society, that if a person want to ask a question corresponding to any branch of life many people will volunteer to answer. Unfortunately this is applies to computer and security issues, people who may hear with any information whether correct or not will volunteer to answer with it which will mislead the person who asked the question. So there is need to find the correct person to ask.

B. Category three in section 2.1: this is worse than the previous point, since users think that these people are professional, and their advice is a rule. But no one can recognize that scientifically their advice is wrong, this will be more catastrophic than people of the first point.

Avoiding these two branches is by self education, it is possible that a person ask about what is not clear to him, but knowing a little by following points one and two will make the answer reasonable or not when they ask, and it is better that they read by themselves and find the correct answer. Also it is better that users who did not study a certain branch and have a little experience don't answer any question, unfortunately, this is difficult.

4. **Learning how to deal with the Internet: if a discipline is followed in the way of dealing with the Internet, this will lead to make the person thinking more maturely in dealing with the Internet, what to open? How can bad sites affect the computer? Opening attachments only from known people, after making an agreement with them to send or receive certain attachment? and so on.**
5. **Using genuine operating system for each computer and original Internet security.**
6. **Implementing risk management: ISPs and Internet companies, and even organizations or companies with big networks must secure their networks and users by implementing the correct security measures in their control rooms. Intrusion detection systems, firewalls, professional administrators, and may be more security measure must be implemented so that with the above points taken into consideration users can be secured from any bad intention people.**
7. **Security measure computers are purely work for security: this point related to the previous point, companies implementing security measures must know that the firewall computer must used just for the firewall not**

anything else, intrusion detection computer also must be used for that purpose without adding any other job or saving any data on it and so on.

8. Securing every computer in the network: many people think that securing their computers only will protect them from all the danger. Leaving a single computer in the network without security will lead to be the door for the attacker or danger to enter the network and reach any important computer attacker wants to compromise, or let certain worm or virus to spread inside the network. Hence every computer must be treated as an important computer.
9. Removable devices carry problems: even if the computer is secured from the Internet dangers and following the above points, still using flash memory with unknown sources or flash memory from a person don't care to security or have a bad intention, will destroy all the work of the previous points, in this way the risk or any danger will bypass all the above points and come easily to the computer and will play any of the dangerous roles that will affect the computer and the network.
10. There is an important thing that everyone must keep in mind: opening any website or attachment or any executable means that the user agree to accept all the data coming from this place, and here the security application may warn us but it will obey user desire of opening and executing everything inside it. This means that existence of the security measure inside computer will not prevent attacks to be achieved by deceiving the user to open and hence accept the contents of anything, here the user will usually be surprised and blame the security application and discuss professional people that these applications are useless!

Conclusion:

Security is the platform for safe usage of the Internet, security applications can see all the traffic which comes from the external world to the computer then decide what to do with each packet, dropping it, passing it or rejecting it. But this platform needs cooperation from the good behavior of the computer user so that they can accomplish a safe Internet usage. Security is useless if the user bring problems from the inside of the computer which can easily bypass this security. So security plus educated behavior, plus studying the computer and how tricks can be made to compromise them are the key factors for using the Internet and the computer safely and securely.

It is important for computer users to have some background knowledge in computers hardware and the relationship with its software, and to know that the Internet applications installed in the computer differ in many points from non-Internet applications. Since dealing with the Internet applications means that the computer will open a door to the external world telling it that it is ready to accept data, so there is a need to get some knowledge in protecting the computers from the affect of this door by using security measures and by knowing what behind any action the user may do.

Using a genuine copy of Internet security application will give a better chance in finding what is unwanted in the stream of data, since using a cracked copy may corrupt some files inside the application or may block some updates, which lead to the security system to work improperly and hence affect the computer security.

Also using a genuine operating system is an important aspect since operating system is the platform that all the applications including Internet security applications are installed on to it, and operating system is the connection between this application and the hardware that application is working on, cracked operating system means that its built in firewall may be corrupted and this will affect the proper work of the Internet security application and the operating system will be a source of infection to all computer applications, and the Internet security application will consider this infection as a trusted traffic. Add to that operating system and Internet security application are connected to a remote servers, these servers are responsible on fixing reported problems and providing the system with updates, files responsible on this connection may be corrupted due to cracking, so this computer will face many problems that cannot be fixed or explained.

It is important to mention here that telling people to use a genuine operating system and Internet security application is not a matter of advertisement to their companies, it is a matter of obtaining a system working correctly, and there is nothing can replace the proper work of the system even if a professional people created the crack.

Education and the place that information are obtained is also an important aspect, taking information from any place is a wrong behavior, information and technology must be learned through authorized institutes or from books with well known authors.

This paper recommends putting disciplines in using the Internet, it looks like a license, these disciplines are so important since using the Internet looks like going to the external world while sitting at home, office or even café. This requires that this person be armed with knowledge, security, and education, so that any problem, attack or any danger can be avoided when facing it. Internet became a necessity in the life that many people are doing their jobs or using credit cards, or register using Internet, so the existence of users like the first three categories in section 2.1 is so dangerous on the whole network.

In Iraq all the mentioned steps in solving the problems plus the discipline are highly recommended so that the society can be evolved and reach the point of protecting the whole network, and to use the Internet safely and securely.

References:

[1] John E. Canavan. "Fundamentals of network security", Artech House Inc. Boston-London, 2001.

[2] Chris Brenton, Cameron Hunt. "Active Defence. A comprehensive Guide to network security", release TeamOR 2001, web.security 2001.

[3] Michael Shinn, Scott Shinn. "Troubleshooting Linux Firewalls", Pearson Education, Inc. 2005.

[4] Dr. Eric Cole, Dr. Ronald Krutz, and James W. Conley. "Network Security Bible", by Wiley publishing, Inc., Indianapolis, Indiana. January 2005.

[5] Mark Taber. "Maximum Security: A Hacker's Guide to protecting your Internet Site and Network. Copyright, Angel722 Inc. Computer publishing.

[6] http://www.bing.com/dictionary/search?q=define+risk&FORM=DTPDIA.

[7]

http://www.bing.com/dictionary/search?q=define+threat&FORM=DTPDIA.

[8] http://www.terena.org/activities/tf-csirt/iodef/docs/i-taxonomy_terms.html.

[9] http://en.wikipedia.org/wiki/Vulnerability_(computing).

[10] Michael Rash. "Linux Firewalls, Attack Detection and Response with IPTABLES, PSAD, and FWSNORT", San Francisco, publisher: William Pollock production. Editor: Christian Samuell. 2007.

[11] Ahmed Abou Elfarag, A. Baith M., Hassan H. Alkhishali. "Description and Analysis of Embedded Firewall Techniques". CESSE, Venice, Italy, 28-30, October, 2009.

[12] Hassan H. Alkhishali, Ahmed Abou Elfarag, and Abd El- Baith Mohamed. "Design and Implementation of Portable, Multi Mode of Operation Embedded Firewall", ITI2010, 32nd International Conference on Information Technology Interfaces, Cavtat/ Dubrovnik, Croatia, June 21-24, 2010.