Have You Been Hacked? A Primer to Cyber Security and Cyber Forensics

Arif Ahmed

(The author is a technical expert. He can be reached at a_ahmed@vsnl.com)

If our computer is connected to the web or if others can access the computer, it is important for us to understand the basic concepts of cyber security. We also need to know how such security can be violated and how to identify such infringement. In our ability to identify who committed such a breach lies the final frontier of cyber security. This article will take us on a tour of these facades of cyber security.

Do you have a feeling that somebody else is using your computer without your knowledge or altering the files you have been working on? Do you find e-mails advising you to update your records on bank accounts, which you never had in the first place? Do you find Internet connection working very slowly or sudden pop-ups coming on your computer though you have done nothing to install them?

Welcome to the world of Cyber Security!

To understand the concepts of cyber security, we need not have any technical expertise with computers. If we can switch a computer on, use the popular windows based software packages, and check e-mail, we are more than equipped to understand the basic concepts of cyber security.

Confidentiality, Integrity, and Availability are the cardinal pillars of cyber security. Confidentiality refers to the fact that the information assets are made available only to such people who are authorised to use or access it. Integrity refers to the fact that the information assets have not been altered in any manner without the knowledge of the authorised users. Availability refers to the fact that the information assets are available to the authorised user when asked for in a legitimate manner. The objective of Cyber security is to ensure that Confidentiality, Integrity, or Availability is not compromised in any manner. In other words, any compromise in confidentiality, integrity or availability in information assets is a security incident.

So what do we do to build a safeguard against security incidents? First and foremost we need to design a security policy. A security system without a policy is a well-traversed road to disaster. We should not even dream of stepping on the same. There is a process and minimum cost of having any system running efficiently. Designing of a security policy is a necessary cost of owning and maintaining an information system. The designing and delivery process should recognise the size of the information system operation and criticality of the same in the main line of organisations activity. Thus the small office of a sole proprietorship firm of Chartered Accountants may have a policy, which is not even written but surely made known to all, as to when one can use the Internet and who all can use the computer. That is the policy for the firm! For large organisations having IT dependent critical operations viz. banks, the policy would be a well-documented book approved by the Board of Directors. There are international guidelines and quality standards on Information Security Management System (ISMS), which can be consulted for the purpose of designing such policy. BS7799 is one such globally respected standard that can be used while designing a policy.

Does designing of a policy ensure that there would be security incident or the security incidents would come down? Not at all! What it does is to reduce the probability of such incidents happening and explicitly states that the organisation considers any security breach as an offence calling for all such actions that an organisation offence merits. In countries where there is an Information Technology Act – These offences may even attract a penalty or imprisonment! India has enacted Information Technology Act in the year 2000. In case all of us have not read it, it would be worth spending an hour knowing it than to commit something, which is defined as an offence under the Act and pay a hefty fine for it. Incidentally, the Act also provides for imprisonment.

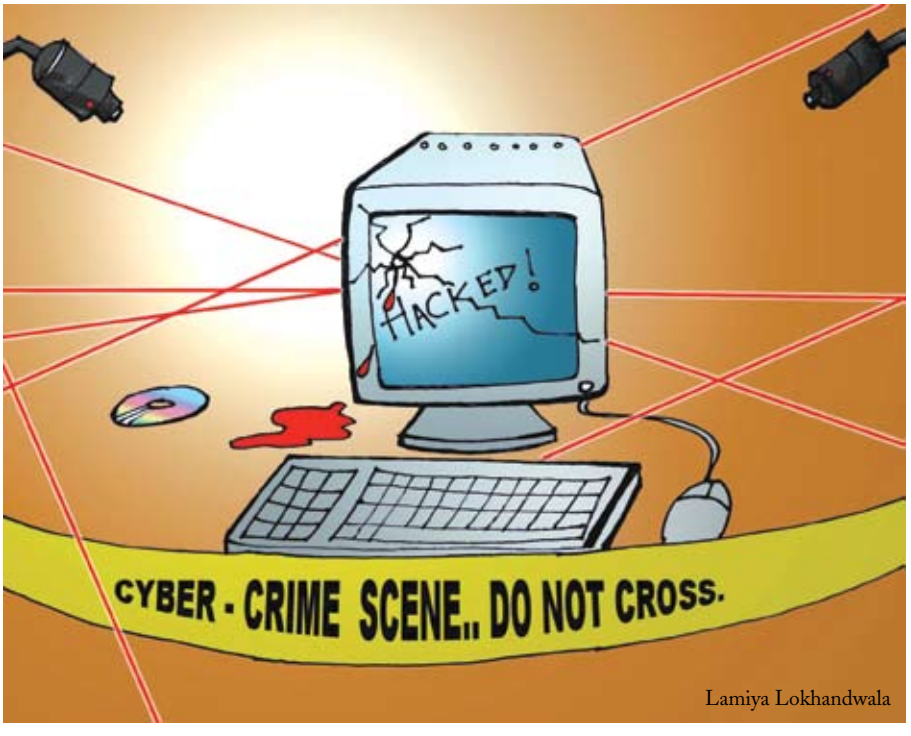
Now that we have information policy, which is being monitored regularly, what are the possible ways through which a security breach can take place? Welcome to the world of Cyber Crime! Cyber Crime can be classified in three groups.

(1) Crimes directed against a computer
(2) Crimes where the computer contains evidence
(3) Crimes where the computer is used to commit the crime

A cyber criminal tries to compromise the security of information assets of the target by using any of the other three aforesaid classifications. There are various methods through which the crime can be committed. These would involve usage of various methods through which the crime can be committed. These methods involve usage of various degrees of technical and social engineering skills. These skills involve the ability to extract personal information of the target without using any technical tools. Let us not deny the fact that a large majority of us use a combination of names of people important to us and the dates and numbers that are important to us as passwords. A still larger majority uses the same password for almost all computer-based services used. Knowledge of the personal life of the target and better still an access to personal communications or documents can be useful in building a profile that can then be used to compromise information assets owned by the target victim. Do we remember whether the promotional mails from our bank, which we threw away, state our account number as well? Many of the documents that we carelessly throw away contain personal information. Cyber Scavengers pick up these materials to develop a profile of the target victims. Having developed the profile, one can access information residing on the computer of the target victim; send e-mail to the target victims with fraudulent commercial offers; or worst still use the computer of the target victim and commit a cyber crime where all the evidence would point out to the hapless target victim. Just imagine someone deleting past records of our clients from our computer, altering the accounts that were prepared and submitted for audit, or send an e-mail using our e-mail ID to our client stating that we would not like to act as their auditor for the next year. Possibilities of this nature, alas, are restricted only by lack of imagination. History stands witness that almost all great criminals of the world were endowed with extraordinary intelligence. Let us make no mistake about that.

A cyber criminal tries to compromise the security of information assets of the target by using one of three main classifications of cyber crime.

So how are cyber crimes committed? We have just learnt about the non-technical version of cyber crime. Let us now look into the technical methods. Irrespective of the nature of the crime one would need to have an access to the information assets to be able to commit a cyber crime. Without a physical access or a logical access to the information asset a cyber crime cannot be committed against the owners of the information asset. Physical security is a well-understood concept. But how does one gain a logical access. Let us start with perhaps the simplest way— sending an e-mail with an attachment. The attachment may contain a programme that would now reside on our computer and snoop information about our working habits and us and send them to the cyber criminal whenever we connect to Internet. Incidentally, one can achieve similar end even without sending any attachment but by asking us to follow some commands described on the e-mail or in a site referred to in the e-mail. Let us know for sure that most of the e-mail messages we receive use the same technology that a web page employs. All precautions adopted while



Lamiya Lokhandwala

viewing a web page should be adopted while opening an e-mail.

A smarter cyber criminal would not want the planted files to be activated when we are reading the e-mail or surfing a page. They would change our system settings so that the file is activated subsequently whenever we start our computer. Whenever we switch on our computer, it follows a series of commands while we stare at the start-up screen. If we want to know that range of possibilities in greater details, we need to hit the 'F5' key on the keyboard after the booting and before Windows start loading and see the range of options that we get to decide how we want our Windows to start. We should select only 'Start Windows Normally' option unless we know what we are doing. The assumption here is that we are using some variant of Windows XP. If we are using an earlier version of Windows, we can simply hit the 'Esc' key when the start-up screen is displayed.

The boot-up process consists of two distinct sections – one where the registry information is read and second where the system files are read. Ensure that we do not type anything other than what is mentioned here. To see these commands we should click on the 'Start' button and select the 'Run' command. Now we type 'regidit' there and we will see a screen popping up. Top of the screen will proclaim 'Registry editor' and the left hand side pane will have options like HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_CURRENT_CONFIG. Let us not go any further as we may damage the process by which our computer starts. But if we must, we can click on the various options described and look at the values appearing on the right hand side panel. Let us not alter anything there unless we know what we are doing.

Let us repeat the Start| Run sequence and type 'sysedit' and watch a screen pop up. The top of the screen will proclaim 'System Configuration Editor' and inside it we will find four windows names – Autoexec.bat, Config.sys, Win.ini, and System.ini. Information contained here is processed during booting. We can read them to see their content but let us not go any further unless we know what we are doing.

A smart cyber criminal alters these files and ensures that the planted software gets activated whenever we start the computer. Once it is activated it would start working silently. To see what processes the computer is pursuing we just need to press the 'Ctrl-Alt-Del' keys on our keyboard simultaneously and see a screen proclaiming 'Windows Task Manager' popping up. Now we click on the tab stating 'Processes' and see what processes our computer is running. If you click on the tab 'Applications' we would find a list of applications being rung on our computer. If we find any unknown process being run we must find out about it. It could be a plant. However, we must note that a seasoned cyber criminal can hide their plant from being identified easily. Here we will need specialised tools to identify the 'plant'.

Let us be reaffirmed that no cyber crime involving our computer is possible without having a program running on our computer or using our computer to commit the crime. The effort of a cyber criminal is to have this carried out without getting identified and our effort is, firstly to prevent such activity and failing that, to identify at the earliest that such an activity has taken place. Of course we know that virus attacks are one of the most common methods of accessing our computer and we have an updated version of reliable anti-virus package. Latest of the worries are spywares, which enter the computer in the same way as a virus does. It usually does not damage the computer but collects and transfers data from our computer to a predefined address. Just imagine the exposure we may have when the spyware picks up our e-mail ID, passwords, credit card numbers and similar critical personal data! The worst part would be that we would have a very difficult time convincing appropriate authorities that somebody made an unauthorised access to our bank account producing confidential information, which only we are supposed to know. We need to prove a criminal breach of our information assets if we want our allegation to hold any water. Incidentally there are many free anti-virus and anti-spyware available and they would give us an improved protection against most of these common threats.

So we have arrived at the stage of identifying cyber crimes. What we now need to do is to see if we can recognise such a crime and better still identify who caused the same. Welcome to the world of Cyber Forensics.

Computer forensics involves the preservations, identification, extraction, documentation, and interpretation of computer media for using them as evidence and / or to rebuild the crime scenario. Please note that by deleting a file to maintain secrecy we are only as comfortable as a child denying having had an ice cream with ice cream dribbled all over the dress. Just imagine that by deleting the Internet history we thought that we removed all evidence of our surfing! A deletion, including removing it from the recycle bin, merely means we can't see it. The file would still be there for an uncertain length of time awaiting somebody to unearth it.

One of the common tricks that cyber criminals use is to allure us through an e-mail tempting us with great offers and business deals.

Let us take two case studies to understand the working of cyber forensics. One of them deals with unauthorized access to our files while the other deals with e-mail hoaxes.

One of the threats that we are exposed to is unauthorised changes being made in our digital file which we have used for some statutory purpose. For example accounts, income tax returns, copies of agreements, etc. stored on computer for subsequent use. How do we ensure that the files that we stored are the same files that we have retrieved? Cyber forensics comes into play in such cases. There is software that can create digital value of a file, which can be stored in our mobile phone also. When we wish to reuse the file, we need to use the software once again and compare the digital value. Our comfort of password protecting important files is essentially theoretical. Cracking passwords or accessing password-protected files is among foundation level skills that cyber criminals acquire. Imagine the comfort that a file integrity checker would give us by enabling us to know that nobody has entered any data in the accounts package when we were not present! One of the false comforts that we have is that if anything is changed, the file size and the date stamp on the file would change. Keeping the file date stamp same is a child's play and a cyber criminal of any consequence can cause material changes in the file keeping the size same.

One of the common tricks that cyber criminals use is to allure us through an e-mail tempting us with great offers and business deals. Using fundamental techniques of computer forensics we can identify the hoax. Let us see how an e-mail can be tracked. Right here we must note that we can reconstruct the path only till the point for which we have forensic evidences. Computer forensics is a science and no magic should be expected from it.

Whenever we receive an e-mail, it comes with a header. Majority of us do not even notice it and some of us do not even know that it exists. If you are using a web mail, search around for an option called 'Show Full Header' or statement to similar effect. If you are using a mail client like Outlook Express simply select the message and click on 'Properties' that you would find under the 'File' menu. We will see a screen popping up with a series of lines preceding the text of the message. That is the header information. A typical header would have a host of information including when the mail was sent, what path the mail travelled through before it reached us, and if we are lucky it would also identify the computer from where the mail was sent. Remember, cyber criminals would do their bit to cover their track by providing us with misleading information.

Let us look at the following excerpt of the header of a mail sent by me.

Return-path:	a_ahmed@vsnl.com
Envelop-to:	knowledge@south-asian.org
Delivery-date:	Fri, 09 Sep 2005 20:29:12 +0530
Received:	From [203.200.235.232] (helo+smtp2.vsnl.net) By 1x18.net4india.com with esmtp (exim 4.43#1) Id 1EdkLO-0000Na-Tc For <knowledge@south-asian.org>; Fri, 09 Sep 2005 20:29:12 +0530
Received:	from aa (localhost [127.0.0.1]) by smtp2.vsnl.net (vsnl mail server) with ESMTPA id 01MK007VK1166L@smtp2.vsnl.net for knowledge@south-asian.org; Fri, 09 Sep 2005 20:26:32 +0530 (IST)
Date:	Fri, 09 Sep 2005 20:26:04 +0530
From:	Arif Ahmed a_ahmed@vsnl.com
Sender:	a_ahmed@vsnl.com
To:	knowledge knowledge@south-asia.org
Message-id:	<00e201c5b54e$9cbb6310$05b441db@aa>

The first three lines are very clear and give the e-mail ID where the mail is to be returned if it cannot be delivered, to whom the mail has been addressed, and when it was delivered. Please note the time mentioned there. The time is the local time and 0530 gives us the time zone of the country of origin. +0530 means that the time zone is 5 hours 30 minutes ahead of GMT. If we click on the clock on the task bar of our computer and go to the Time Zone section, we will find the countries that correspond to the time zone. We will find +0530 corresponds to India.

An e-mail is not delivered directly from the sender's computer to the recipient's computer. It goes through various servers and at each stage some information about the handling of the mail is attached to the header. Thus it gives us a clue as to how the mail was routed.

The information against first Received: gives us an IP Address 203.200.235.232. This is the IP address of the server, which handled the mail.

We must observe the best practices suggested by various international standards and experts to face the threats in the Cyber World.

If we query to find out who owns the IP address we will find it is owned by smtp2.vsnl.net. There are many sites that provide this service. HELO identifies the sending machine; "HELO smtp2.vsnl.net" can be read as "Hello, I'm smtp2.vsnl.net". However, the sender can give false information. The line continues and identifies who received the mail and what mail programme it runs along with the version number and what ID number the message was allotted.

The next line tells us from where the mail was received. 'aa' refers to the name of the computer from where it was sent and what its IP address is. Local host and 127.0.0.1 refers to an internal address of the computer and that cannot be found on the Internet. The text further tells us how the mail was handled by the VSNL server, what ID was allotted to it, and when was it received. Please note that this address can be fabricated.

Thus we can find out the geographical territory from where the mail was sent, enough information to get back to the service providers and identify from where the mail was sent, and even identify the computer from where mail was sent. A large majority of the hoaxes can be identified by observing this simple process. Naturally, serious cyber criminals would take care so that they cannot be traced back, but then we are not going to do anything based on an unknown e-mail, which can expose us to financial loss or legal breach.

Now that we are aware of the threats in the Cyber World what do we do? We must observe the best practices suggested by various international standards and experts. We must note that some of the legislations explicitly and implicitly ask us to have appropriate information asset security policies designed. In case our information assets are valuable to us and are worth protecting, we must carry out a regular security audit to ensure that security of our information assets has not been compromised. We must also recognise the situations where we may not be in a position to provide an opinion or certification unless we are sure that the information provided to us has come from a trusted source having adequate internal control to ensure its integrity. If in doubt, we may insist upon a security audit to be carried out before we can provide our opinion.

Let us conclude by reminding ourselves that when we become a member of the cyber society we must recognise that this society has its own set of rules of safe conduct. As a member of that society we must observe them and ensure that our existence as a member of the cyber society is a rich and rewarding experience.❐