Cyber Security: Issues and Way Forward

B M Mehtre

...security largely depends on people involved, and less on technology. Technology installed and configured properly will work as designed, but humans behave differently, at different times. This requires important culture change and adhering to process and procedure, which depends on human beings

Technological advances have brought many conveniences to modern society. One of the most important benefits is the ''any where any time'' paradigm. That is, you can carry out your work in the cyber world, from anywhere and at anytime. For example, you can do your tasks like buying a ticket, bill payment, placing order for goods and merchandise online. All such business transactions can be done from anywhere and anytime. The first such system, i.e. all electronic transaction, was first demonstrated in Hyderabad in 2001 [1]. The all electronic eco system was established, and house hold water bill payment was made electronically. The payment was through e-cheque issued by Andhra Bank to a resident account holder, Water Board who made their bills presentment and payment in collaboration with Andhra Bank.

The aim of Information Security is to provide confidentiality, integrity and availability of information. These (CIA) three parameters are also called security goals or security services. The other security objectives also include such other parameters as authenticity, authorization, accounting and nonrepudiation. This is illustrated as shown in Figure1.

Cyber security is a process, technique or procedure to ensure information security goals. Various terms used to mean information security or cyber security, include IT security, digital security, electronic security, systems security, internet security etc.

Let us take an example of online banking. The customer account details (like name, address, bank balance, and transactions) forms important information for any bank and its customers. This information needs to be kept confidential (secret) from others, and to be known to only the customer and to the authorized/ designated staff in the bank. Any leakage of this information (somebody else having access / knowing this info) is called a security breach. Similarly, communication between the customer and the bank has to be secure, that is, exactly the same message has to reach the bank (and vice versa), and it should not get altered in anyway during transit. This is called message integrity (or quality) of information or message. One of the methods to achieve integrity and confidentiality is by encryption, a cryptographic process in which clear text is scrambled using a mathematical function. The scrambled text message is decrypted at the receiver's end using similar or related cryptographic (mathematical)

The author is Professor at the Center for Cyber Security, Institute for Development and Research in Banking Technology, established by Reserve Bank of India. His areas of interest include Cyber Security, Digital Forensics and Technologies for Cyber Defense. His seminal work on fingerprint identification led to the development of the first automated fingerprint identification system in India, which was later deployed in many states in India and some countries abroad.

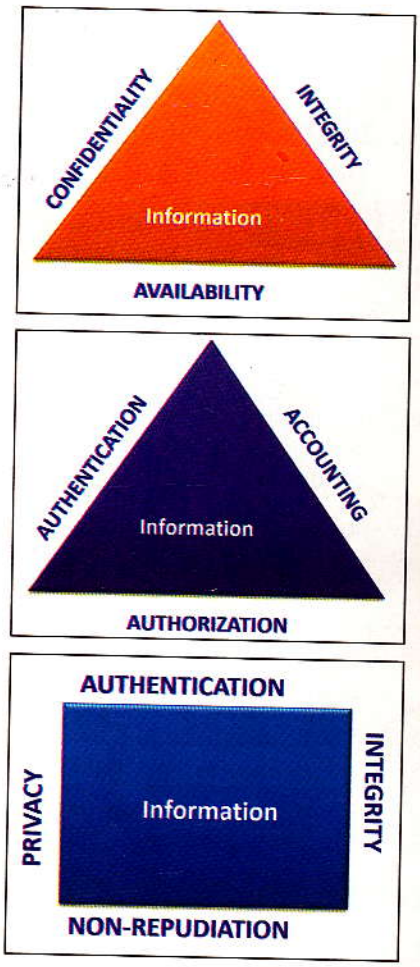

Figure 1. Information Security goals – different views

function. "Availability" service provides Customer access and use of the information at any time and from anywhere. This forms an important part of secure systems.

One of the methods of accessing computers and other digital devices in cyber space, on internet, is through a valid user name (customer id) and a valid password. This is normally issued the first time, through a process called registration or enrollment. Once enrolled, subsequently the user id and password is used to access the account (or information) by the enrolled user. Most applications available today on internet are web applications. Login into such systems is through a secure (encrypted) mechanism. Figure 2 shows a secure login site. Please note the lock sign in green along with the bank name. This indicates that you are going to login into a secure system.

To login to a system, you need user id and the password. Password is like a lock and key. You need to keep it secret and not share with anybody, because for computer systems, it is the user name and password that represents the user. Whoever has these credentials is the real owner for the system. Many attempts are made to steal these credentials by cyber criminals, also called, hackers. One of the popular methods is to send hundreds of emails announcing 30 M$ lottery (or such other alluring mails) to unsuspecting users. Once you respond to such emails, they will lure you to reveal your credentials or ask for registration fees etc. Such attempts to extract credentials is called phishing. Other methods to steal credentials through cyber attacks involves steps like social engineering, scanning, finding vulnerabilities and exploiting the vulnerabilities in the system. Such attempts to steal credentials and gaining access to the systems are called cyber attacks.

Important and Mission critical systems employ several measures to counter the cyber attacks. In large organizations cyber security operating centers are necessary to be established, which can monitor security incidents and events and generate alerts. The alerts are for system administrators to look into the matter, as there are quite often false alarms. Normally, several layers of defense (defense in depth) is employed – to take care of data, applications, hosts, and network or perimeter assets and infrastructure. This is illustrated in Figure 3.

Cyber security is managed and administered through a mechanism called people, process and technology. As shown in Figure 4, security largely depends on people involved, and less on technology. Technology installed and configured properly will work as designed, but humans behave differently, at different times. This requires important culture change and adhering to process and procedure, which depends on human beings.

Cyber security is a skill based technology and thrives on knowledge of underlying infrastructure, operating systems, computer networks and applications which are built using programming language. There are large opportunities for our young engineers in the coming years in this area to work and make a professional career. In fact, such opportunities are worldwide, as the whole world is dependent on cyber space and cyber security is every body's concern.

Suggestions for Password Protection

- It should be 8 to 10 characters or longer, preferably mix of alphabets and numerals

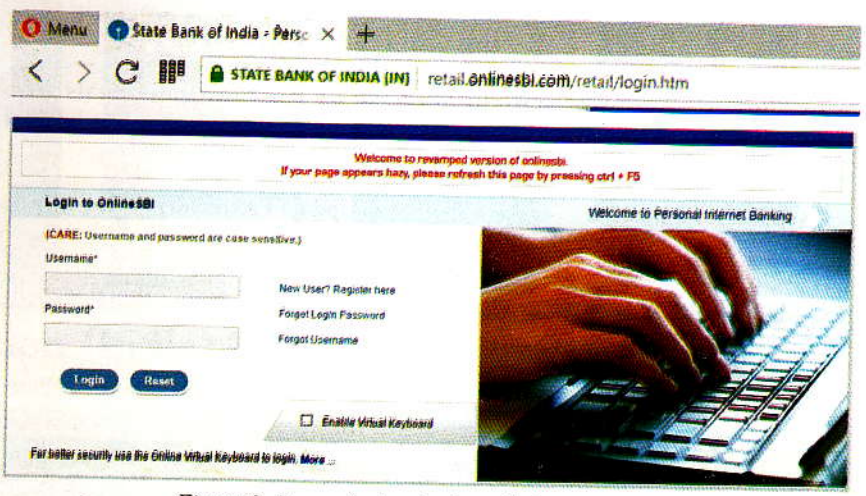

Figure 2. Secure login – lock symbol in green color

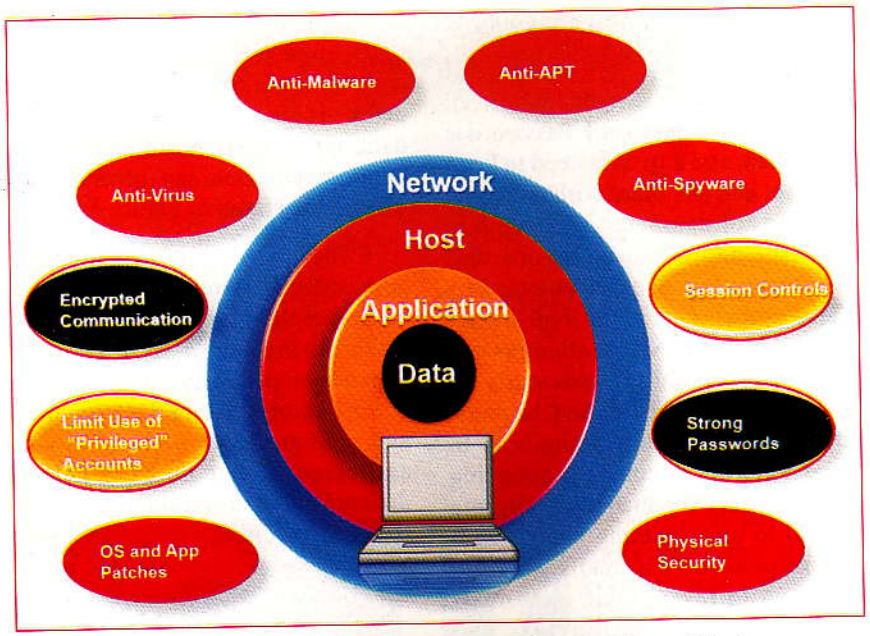

Figure 3. Defence in Depth - Multi Layer cyber security architecture

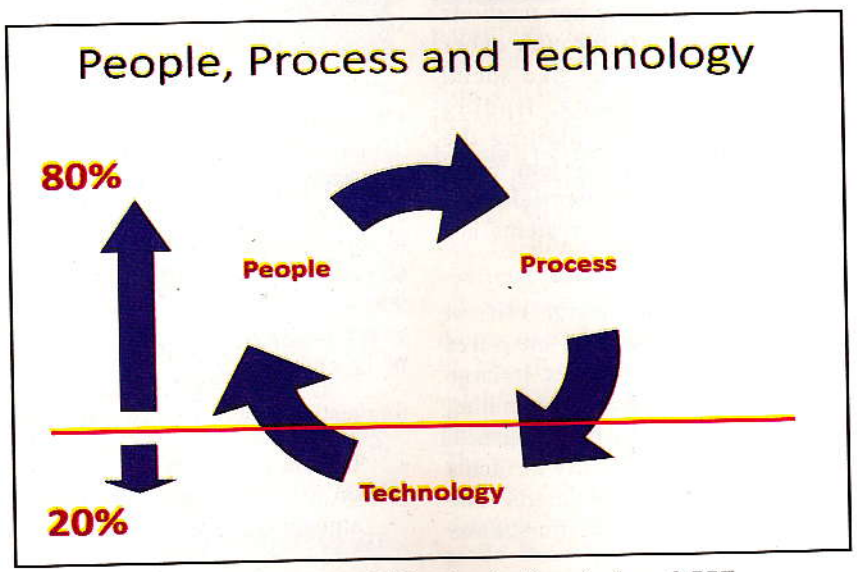

Figure 4. Managing and Administering Security through PPT.

- Should use lower case and upper case mix
- Mix (allowable) special characters in the password
- Use your own favorite multilingual passwords, which are hard to guess
- Change password frequently
- Do not use name, address, date of birth, etc as passwords as they can be guessed easily
- Do not use dictionary words
- Solutions

Security Tips for individuals (end users -desktop, laptop, mobile internet users)

- Update Frequently
- Passwords
- Downloads from official website
- Administrator
- Turn off
- Encrypt
- Be Careful while using USB drive
- Do Sensitive browsing (like online banking) only from your computer
- Take Backup frequently
- Think before sharing on social networks/media

Security Tips for Organizations/ System, Network Administrators

- Need to have a security policy approved by top management
- Ensure that Security policy is read and understood by every employee
- Revisit controls / counter measures periodically
- Apply security patches regularly
- Plan diversity in data center and disaster sites environments
- Take system backup regularly and test backups for restoration
- Need to have a suitable password policy for multishift system admin personnel
- Refer to Cyber security check list IDRBT July 2016 doc at www.idrbt.ac.in site.

In summary, a brief introduction to cyber security is given along with the convenience it provides and the precautions one has to take. This is especially important for online banking and the present era of less cash economy. This is also an area for our young engineers to make a career in the field of cyber security.

Readings:

1. NN Murthy, BM Mehtre, KPR Rao, GSR Ramam, PKB Harigopal, & KS Babu: Technologies for eCommerce: An Overview, Informatica 2001
2. Cyber Security Check list, IDRBT Document July 2016 https://idrbt.ac.in/assets/publications/Best%20Practices/CSCL_Final.pdf.

(E-mail:bmmehtre@idrbt.ac.in)