Open access Journal International Journal of Emerging Trends in Science and Technology

Cyber-Security Measures in Ivy League Colleges and Other Higher Educational Institutions

Author
Kanika Dhameja
VIT University,Vellore
Email: *Kanika_30oct@hotmail.com*

Abstract

Driven by a growing concern for the potential vulnerability of important data together with an increasing number of disruptions in the cyber- domain, many organizations have tried to study the various possible threats to their infrastructure and most of these organizations have even proposed security measures for the protection of their assets and valuable information. This paper investigates the various cyber security measures that have been enforced by the Ivy League Colleges mainly Harvard University as well as institutions of higher education in Israel and China. The Ivy League Colleges are known to be the most prestigious Colleges for higher education in the United States. The Ivy League is a collegiate athletic conference composed of sports teams from eight private institutions that offer higher education in the Northeastern United States. The name is commonly used to refer to those eight schools as a group. The eight institutions are Brown University, Columbia University, Dartmouth University, Harvard University, Princeton University, the University of Pennsylvania, and Yale University. Further this paper also looks at some of the latest cyber security tools that are being implemented and used at these institutions.

Keywords – *Cyber-domain, Ivy League, Higher Education, Harvard University, Israel, China, tools*

1. Introduction

Until recently, cyber security has primarily attracted just the geeks. The Internet's creators have always been part of a very small and enclosed region or space. They were very comfortable with an open system in which security was not a primary concern. But, with approximately three billion users on the Web in today’s date, that very openness has become a serious vulnerability. Instead, it is endangering the door of opportunities that the internet has opened for us. What makes cyberspace an enticing arena to criminals is that the attribution in cyberspace is difficult, especially given that the cyberspace is borderless and cuts across jurisdictions. It allows criminals to launch attacks remotely from anywhere in the world, without being exposed. With this growing threat landscape, cyber-readiness of the security systems has been constantly put to test.

2. The Ivy League Association

The **Ivy League** is an athletic conference composed of sports teams from eight private institutions that offer higher education in the Northeastern United States. The name is commonly used to refer to those eight schools as a group. The eight institutions are Brown University, Columbia University, Dartmouth University Harvard University, Princeton University, the University of Pennsylvania, and Yale University. The Ivy League Schools are also known to be the most prestigious Colleges for higher education not only in the United States, but also worldwide. These colleges are in the northeastern region of the United States. For many years now, the Ivy League Colleges have become a hub for cyber attackers and hackers, precisely because of the sensitive information stored in their databases and the huge revenues generated by these institutions.

This information if obtained or tampered with, by anyone except the authorized personnel could have disastrous and appalling effects on the economic conditions of the United States.

3. Hacking Harvard

Harvard University is a private Ivy League University in Cambridge, United States. It is also the oldest University for higher education. From Social Security numbers to health records to research papers, all of which are very valuable and important bits of informational data to the faculty and the student body gets stored in Harvard's computer system. This system undergoes a barrage of cyber security attacks almost every single day. Harvard fits the bill precisely because of these few main reasons. The servers of Harvard are so strong and powerful that they can almost effectively be used as a weapon against other not so powerful systems. They can be re-programmed to include illegal as well as malicious data. The working of the University's main operational unit largely depends on the proper and systematic working of the main server, which if breached could bring down the whole system at once. “We're seeing things in the tens of thousands a day,” said Christian Hamer, Harvard University IT Department's chief information security officer. Every time a student connects to the Harvard University's wireless network, he creates a pathway into the Harvard's system, a pathway that could be potentially exploited by a hacker. Thus, Harvard University faces a very precarious mission, which is to maintain and balance its academic reputation demanding an unfettered flow of safe and secure information to the students and the faculty and at the same time ensuring the safety of this valuable information.

4. Incidents of Cyber Crimes at Harvard University

Over the years Harvard has reported the breach of its cyber security twice. Both these times have lead to the leak of very valuable and sensitive information from the University's servers. This number has been rising sharply. One such incidence has been mentioned here. One morning in September 2011, as high school seniors began thinking about their college plans, visitors to Harvard's website were greeted not with images of professors or students participating in community service projects, but rather a photograph of Syria's President Bashar al-Assad. The Syrian Electronic Army, a group of hackers had maliciously gained notoriety by defacing prominent websites to show support for the Syrian government. They had altered the University's website, and the website now read “Syrian Electronic Army Were Here,” and alongside it displayed al-Assad's image. This attack was one of the most shocking attacks on the Harvard's security system which lead to a lot of embarrassment and brought the reputation of this prestigious University into limelight.

5. The Cyber Security team at Harvard

Incidents like these often drag the terror of cyber crimes from the depths of those IT server rooms to the public eye. Security of valuable information has always been an issue of very major concern at the Harvard University. What makes it even more challenging to prevent these crimes is that these potential hackers make it almost impossible for the cyber security professionals to even detect the presence of a malicious intruder inside their system. They become “invisible” and enter the system, and remain so while they are inside the system. Some of these attacks aim at disrupting the valuable information, some at stealing that valuable information and others at altering and modifying the data according to the need of the intruders.

Eleven employees of Harvard work within its information security department. They are assigned to secure information systems in the Faculty of Arts and Sciences, Harvard's central administration, and the Medical School, Dental School, and Divinity School. The University's other schools handle their own IT security. They also advise the students and the faculty to ensure that their accounts are protected by putting strong passwords on them for their security, passwords that cannot be cracked. They also insist that the students update their operating systems regularly and avoid navigation to sites which seem suspicious.

6. The Risk Equation

Risk management is a fundamental requirement of the concept of cyber security. Without this crucial tool, the safety of the information or system always remains in jeopardy.

Risk management provides a way for the universities of higher education to understand and handle the risks that are optimal for security, IT, and education. It creates a common language to identify, assess, and understand potential threats and vulnerabilities and at the same time identifying means for mitigating, accepting, or avoiding that risk.

One such equation used by the educations institutions in the United States is stated as follows:

Risk= Impact X Probability / Cost.

where Impact is the disastrous effect on the organization should a risk event occur.

Probability is the likelihood of that event occurring within a given timeframe.

Cost is the amount of money the institution must invest in order to mitigate or reduce the risk to an acceptable level.

7. The Equation Group

The **Equation Group** is a highly advanced secretive computer espionage group that has been discovered by **Kaspersky Lab's Global Research and Analysis Team (GReAT) in February 2015.** According to the researchers at the Kaspersky Lab, the equation group is unique almost in every aspect of their activities. They use tools that are very complicated and expensive to develop, in order to infect their victims, retrieve sensitive data and hide activity in an outstandingly professional way. To achieve this target, they utilize classic spying techniques in order to deliver malicious payloads to the victims.

To infect their victims, the equation group uses a powerful arsenal of "implants" called the Trojans which include an array of malicious tools, the main ones being the ones stated below as per the reports obtained from the Kaspersky Lab: Equation Laser, Equation Drug, Double Fantasy, TripleF antasy, Fanny and Gray Fish. They aim at reprogramming the hard drive firmware of various popular HDD brands. They fanny worm developed by the equation group has the ability to retrieve data even from isolated networks. They also use infected USB sticks to map out the air gapped networks. They create programs that would create malicious hidden areas on an infected USB stick. If that stick is then connected to a computer with no Internet access, it would scoop up the data about the system and save it in that hidden area. If now the USB stick is reconnected to a computer with Internet access, it will send that information off to its controllers.

The equation group uses universal methods to infect their targets. They do so not only through the web, but also in the physical world. For achieving that, they used an interdiction technique where they intercept the physical goods and replace them with Trojanized versions. The technical and hacking skills that the equation group possesses, rival the groups that developed Stuxnet and the Flame espionage malware.

Kaspersky has been tracing the activities of the equation group since a long time and they have recently passed a law which will be implemented in the coming year to tackle this espionage group to ensure cyber security measures especially in all the higher educational institutions in various countries that this group targets.

8. CASE STUDIES

8.1 ISARAEL- Ben Gurion University

Israel is known as the hotbed of tech startups. It is also ranked near the top of several recent Bloomberg innovation metrics. The effects of computerization in the recent decades have not exempted national security concerns of Israel. There is an ever growing dependence of all the sectors on the Information Technology sector and this growing dependence means that the damage to computers and the processes of Information flow would result in actual physical damage and colossal economic losses. Various cyber security programs have been developed by the institutions of higher education in Israel. The goal of these Cyber Security programs is to develop the basic knowledge and expand the public debate on the topic of cyber security, at the same time focusing on the following key aspects:

□ The conceptualization and creation of a common language in the contexts of national security in Israel.

□ The development and examination of a national policy that has already been proposed but has not yet been implemented.

□ The identification of guidelines for a doctrine of warfare in the field, which would collectively operate both at the national and the inter-organizational level in Israel.

AIRHOPPER FOR DATA THEFT

The Security researchers at the Cyber Security Labs at Ben Gurion University in Israel have found a new and an impressive way to snoop on a personal computer that has no network connection. This new technology is known as the AirHopper, which is basically a key logger app to track the data and text that is being typed on the computer or the mobile phone. This technique is capable of infiltrating a closed network in such a way that it lifts data from a machine that has been kept in isolation from the internet or any Wi-Fi or Ethernet connection by using a mobile phone's frequency modulation radio signals.

Air Hopper is capable of capturing keystrokes by intercepting certain radio wave emissions from the monitor or the display unit of the computer that has been kept in isolation.

The security researchers then pick up the Frequency modulated signals on a nearby smart phone and translate these received signals into typed text that can be read.

Air Hopper works well for a range of 1-7 meters with a bandwidth of 13-60 (bytes per second) which is enough for hackers to steal a secret password. This technique of data theft was developed by the Ben Gurion University in order to protect itself against potential intrusions of its kind in the future.

8.2 CHINA- Sun Yat-sen University

The government of China in collaboration with China's Internet regulator has announced a new mechanism to screen the major information technology products before they can be approved for use in the institutions of higher education in particular and other institutions in general. This new mechanism is known as the "Cyber Security Vetting System". Products will not be allowed to enter the institution or the country for that matter, if they aren't deemed safe and controllable. This step has been taken to prevent future malware invasion and wiretapping that the Chinese Institutions have always been a victim of. The Sun Yat-sen University situated in Guangdong, China is the first Chinese University that plans on implementing this law at its IT department starting this year.

9. CYBER SECURITY TOOLS

The tools that cyber criminals use are mostly the same tools that security experts use to audit their systems. Here we will look at some of the tools that are currently been used by the security researchers in the IT department at some of the IVY league colleges.

Back box- Back box is the perfect security solution which provides pen-testing, incident response, computer forensics as well as an array of intelligence gathering tools. Its latest version includes software solutions for vulnerability analysis/assessment and pen-testing.

Kali Linux- Kali Linux is the most advanced and versatile penetration testing distribution tool.

SiLK – SiLK which is short for System for Internet-Level Knowledge, is a collection of traffic analysis tools that has been developed by the CERT Network Situational Awareness Team in order to facilitate security analysis of large networks. The SiLK tool suite supports the efficient collection, storage, and analysis of network flow data.

Avast- Avast is an anti virus developed in 1991.
Its features include antivirus with antispyware, streaming updates, hardened mode, Deep Screen as well as Secure DNS.

Sanity Check- Sanity Check goes to incredible lengths to detect processes which usually hide themselves from the Windows task manager and programming interfaces. The tool typically uses seven unmentioned safe techniques to reveal hidden processes in both user mode as well as the kernel mode. Sanity Check is also configured to detect processes which do efforts to obfuscate their real names. This is necessary because obfuscating the real name is a typical activity associated with malware.

Wire Shark- Wire shark is a free and open-source packet analyzer. It is used for the purpose of network troubleshooting, analysis, software and communications protocol development, as well as education.

10. Techniques for securing the systems at Institutions of Higher Education

- **Strong Passwords**

Cyber intruders and Hackers have developed programs that automate the ability to guess your password. Passwords generally provide the first line of defense against unauthorized access to your computer. The stronger your password is the more protected your computer will be from hackers and malicious software. While you are creating a new account, you should make sure you have strong passwords for all accounts on your computer. Using a very strong password and changing it often can prevent your system from being attacked. Passwords are not unbreakable but very often stand as a wall between the intruder and your sensitive information. Password strength is basically a measure of the effectiveness of a password in resisting guessing and brute-force attacks. It estimates how many trials an attacker who does not have direct access to the password would need to guess the password correctly. The strength of a password is a function of its length, complexity, and unpredictability. The strength of a password largely depends on the number of times an intruder will have to guess the password to finally arrive at the correct one.

- **Random passwords**

Random passwords consist of a string of symbols of some specific length taken from a set of symbols using a random selection process in which each symbol is equally likely to be selected. There is an equal probability for each of the symbols to be selected. Let us consider a process which selects a random password of length L from a large set of N symbols. Then the number of such possible passwords can be found out by using the equation:

$$H = log_2 N^L = L \log_2 N = L\frac{\log N}{\log 2}$$

Where
H is the number of randomly generated passwords
L is the length of the randomly generated password
N is the length of the total set from which we will select the random password.

- **Installation of Firewalls**

The installation of a firewall enables the institution to decide which types of messages should be allowed to enter the system from the external sources. It should also be made sure that if an institution's web server is intended to provide information and services to the students, it should not be located on the private side of the firewall so that in case of a breach of security, the private information is not compromised.

- **Use Secure Sockets Layer (SSL) Servers**

SSL is used to ensure that the financial and information transactions that are made with the web browser are secure and threat free. In a secure Web session, your Web browser generates a random encryption key and sends this key to the Web site host which is to be matched with its public encryption key. Your browser and the concerned web site then encrypt and decrypt all transmissions in order to ensure a secure transaction.

- **Installing Anti-Virus software**

Viruses are the most well known computer attackers, and they can do all sorts of damage to a secure computer system. There are many types of viruses that have the ability to compromise a computer's security in different ways. In most cases users acquire a virus by downloading questionable files that are falsely presented as other things in an email scam, or by visiting a suspicious website. Once these viruses have infected your computer, they can drastically slow down your processing speeds, and delete critical and important information. Harvard University advises all its students and faculty to secure their laptops with a strong anti-virus software. An anti-virus periodically scans your system and secures all your data and files by deleting any virus that has infected your computer. It warns you when you are about to navigate to a potentially dangerous site. It filters all your email messages and ensures that you don't receive spam mails.

Authentication of sensitive messages through the use of digital signatures

A digital signature used to authenticate a message is analogous to the fingerprint of a person. It depicts the message in such a way that if the message was to be altered in any malicious way, the fingerprint would reflect it. This technique makes it possible to detect counterfeits and security breaches.

- **Encryption of messages sent over the Internet**

Encryption refers to the process by which the sensitive information is transformed into an unreadable format which cannot be deciphered by the receiver unless he/she possesses the appropriate key for decryption. As more and more messages are sent over larger and larger networks these days, sensitive and precious information becomes increasingly vulnerable to assault by intruders. Encryption has thus become a leading tool to combat this vulnerability.

Conclusion

As cyber attacks become more frequent and sophisticated the Information Department at various institutes of higher education may be forced to implement more rigorous security measures to protect the entire system from potential threats. There is a need for understanding the threats that linger over the internal working of these prestigious institutions and well as taking corrective and quick measures to ensure that they are fully protected. If these security measures are adopted by the Indian Universities, then we can minimize cyber crimes in India as well. This would be a huge step towards ensuring the security of the entire economic as well as the Educational system.

References

1. Background paper on the comparative analysis of cyber security initiatives worldwide by Myriam Dumm.http://www.itu.int/osg/spu/cybersecurity/docs/ Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf
2. Hacking Harvard published in The Harvard Crimson http://features.thecrimson.com/2013/hackers/
3. The Mouse Click That Roared published in the Korea Times. http://belfercenter.ksg.harvard.edu/publication/23396/mouse_click_that_roared.html
4. http://www.aljazeerah.info/News/2014/May/22%20n/China%20to%20Start%20Security%20Vetting%20IT%20Products,%20Following%20Charges%20of%20Cyber%20Attacks%20with%20US.ht
5. http://searchsecurity.techtarget.com/magazineContent/The-real-information-security-risk-equation
6. http://www.theinquirer.net/inquirer/news/2395638/kaspersky-fingers-nsa-style-equation-group-for-hard-drive-backdoor-epidemic
7. http://en.wikipedia.org/wiki/Equation_Group
8. http://cyberwarzone.com/cyber-security-tools-list-2014/
9. http://nces.ed.gov/pubs98/safetech/chapter9.asp