IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 1, Ver. III (Jan – Feb. 2016), PP 18-21
www.iosrjournals.org

Cyber Security in the Era of Networking: A Review

Ms. Manjiri N. Muley
Dharampeth M.P. Deo Memorial Science College, Nagpur

Abstract: *Cyber security is an intricate issue, affecting many application domains and straddling many disciplines and fields. Securing the critical infrastructures entails protecting not only the physical systems but, just as important, the cyber portions of the systems on which they rely. Cyber attackers can disrupt critical infrastructures such as financial and air traffic control systems, creating effects that are similar to terrorist attacks in the physical space. They can also carry out individuality theft and financial fraud; steal commercial information such as intellectual property; recruit criminals and others to carry out carnal terrorist activities. What makes cyberspace even more attractive to criminals including non-state actors is that provenance in cyberspace is complex, especially given that cyberspace is borderless and cuts across authorities. Cyber Security Research is one context where the solution to deal with cyber criminals is germinating.*

Keyword*: cyber security, Types of attack, Threat intelligence, next generation firewall, cyber forensics, regular surveillance, mobile cyber security, security awareness.*

I. Introduction

Cyber security competence building is a rising phenomenon globally and India is no exception, Academia is playing a crucial role in India to build a healthy ecosystem for the cyber security research.

The **Cyber Security Research** identifies the following seven hard problems
a. Scalable trustworthy systems
b. System evaluation life cycle
c. Combating malware
d. Global-scale identity management
e. Situational understanding and attack attribution
f. Privacy-aware security
g. Usable security

Trustworthy Cyber Infrastructure

It focuses on ensuring that the nation's precarious infrastructure – such as the oil and gas pipelines, information setup, and the Internet – become more secure and less susceptible to malicious and natural events.
- Internet Capacity and Attack Modeling
- Process Control Systems (PCS) Security
- Secure Protocols

Cyber Security User Protection & Education

It emphases R&D activities on emerging ways to help all types of users – from improving the security and safeguard of user online activity, toattracting the next generation of cyber security warriors, to providing the tools needed for examiningcyber-criminal and terrorist movement.
- Cyber Security Competitions
- Cyber Security Forensics
-Identity Management &RecordsConfidentialityTechnologies
- Insider Threat

Cyber Technology Evaluation and Transition

It provides a synchronized process of valuations, estimations, and operational experiments and guides to switch the fruits of research into practice.
- Cyber Security Assessment and Evaluation
- Cyber Security Experiments and Pilots
- Transition to Practice

Concept of cyber security

Cyber security refers to one or more of three things: A set of activities and other measures proposed to protect—from attack, Interruption, or other threats computers, computer networks, associated hardwareand devices software, and the data they contain and communicate, including software and data, as well as other components of cyberspace.The state or quality of being protected from such threats.The wide field of workintended at employing and improving thoseactivities and quality.

Types of cyber attack

1. **Denial-of-Service Attack** – A denial-of-service or a DOS attack generally means confronting the network to bring it down completely with useless traffic by affecting the host device which is connected to the internet. A DOS spasm targets websites or services which are hosted on the servers of banks and credit card payment gateways.
2. **Spoofing** – Spoofing is a cyber-attack where a person or a program impersonates another by creating fabricated data in order to gain illegal access to a system. Such threats are commonly found in emails where the sender's address is spoofed.
3. **Malware** – Malware refers to malicious software that is being designed to damage or perform unwanted activities into the system. Malware is of many types like viruses, worms, Trojan horses, etc., which can cause havoc on a computer's hard drive. They can either remove some files or a directory or simply gather data without the actual knowledge of the user.
4. **Exploits** – An exploit attack is basically software designed to take advantage of a flaw in the system. The attacker plans to achieve easy access to a computer system and gain control, allows privilege escalation or creates a DOS attack.
5. **Indirect attack** – Indirect attack means an attack launched from a third party computer as it becomes more difficult to track the origin of the attack
6. **Information Disclosure**– Information disclosure breach means that the information which is thought to be secured is released to unscrupulous elements that are not trustworthy.
7. **Eavesdropping** – eavesdropping means secretly listening to a conversation between the hosts on a network.

What Are the Threats?

People who perform cyber-attacks generally fall into:-
Criminals*:* -intent on monetary gain from crimes such as theft or extortion.
Spies*:*-intent on stealing proprietary information used by government or private entities.
Terrorists*:*-engage in cyber-attacks as a form of non-state or state-sponsored conflict.

What Are the Vulnerabilities?

Defenders can often defend against weaknesses, but three are particularly challenging:Inadvertent or purposeful acts by insiderswith access to a system; supply chainvulnerabilities,which can permit the inclusion of malicious software or hardware during the acquisition process.

Where's the risk?

Everywhere! If there's a transaction system that involves a cardwith a magnetic strip and a swipe, there's a transaction that embraces a risk. And if there's a computer system with software intended to allow access by multiple userswithout security in mind, then there's a foremostrisk of being hacked for malicious or competitive purposes. Mobile devices, every so often containing sensitive information, are lost or stolen every day. If we use e-mail or our company's systems are associatedto the Internet, we are being glance at, probed, and attacked constantly.

What about cyber crisis planning/management?

IT (Information Technology) systems are susceptible to a variety of disruptions from
a variety of sources such as natural disasters, human error, and hacker spasms.
These interruptions can range from mildto severe.

Thecyber crisis planning management process covers the following:

Identify the Crisis at Hand

For example, a customer data breach privacybreach, virus outbreak, and targeted malicious code attack, denial of service attack, phishing attack, or third party data compromise.

- **Analysis and Assessment –** Triage of the incident to determine the severity (Chan Scale of Insecurity) and impact on the business.
- **Response Plan –** Decide whether to protect or prosecute includingcontacting the proper law enforcement authorities.
- **Recovery Plan –** Restore affected systems to normal business operation.

Mobile Cybersecurity

Mobile industry is committing significant assets to cyber security solutions to protect devices and networks and the data they store and carry.

Security policies and risk management:-

Among the safeguards are providing enhancements to security policies and risk management protocols; casing definitions and documentation; ongoing scans of the threat environment; and security assessments.

Monitoring and vulnerability scans –

The goal of these tools and processes is to assess threats in real time and stop problems before they happen.Monitoring trends, staying ahead of threats and providing advanced solutions in this vibrant environment demand continual efforts in technology innovation. The wireless industry conducts regular threat assessments and trends analysis. Cyber threats to these devices are increasing, and include a range of malware and rogue programs, often disguised assumingly legitimate updates, utility and productivity tools anddownloadable applications. The biggest difference between threats to smartphones and tablets is based on how the devices are principally used

Tablets	Smartphones
Tablets appear to be used more for media consumption, including video, games, e-books and accessing the Web	Smartphones are used more for data communications activities such as SMS, email, mobile financial transactions and voice calls.

Mobile Banking Services

Consumers use mobile wallet services to get information, such as checking a bank balance; to conduct transactions, such as making a purchase or transferring funds; or to gain a value-added service, such as receiving alerts or coupons. The cybercriminalis after the stored credit card or bank account information, and the key identifiers consumers use to access these accounts.

Threat Intelligence

Cyber threat landscape is expanding enormously in the cyberspace. Research is also being carried out on advancement of automated tool to simulate human hackers, one of the ways to create the threat intelligence. Some of the organizations are also working in the domain of antivirus and anti-malware research & development. Research related to mitigating cyber threats is already being undertaken by the researchers as a priority item. Some activities are already underway at various research organizations in India in areas such as threat research & response, specifically for Malware research analysis, Worm Propagation and Detection, Targeted remote malware clean-up, Advanced Persistent Threat Countermeasure, anomaly detection for zero-day attack, Intrusion Detection Systems, SPAM Detection & Filtering, exploitation and Reverse engineering.

Next Generation Firewall

Research organizations are also working in Multi identity-based technology such as Next Generation Firewall that offer security intelligence to enterprises and enable them to apply required and best suited security controls at the network. Integration of technology with other security solutions such as threat intelligence and management systems, Web Application Firewall, Web filtering, Anti-Virus, Anti-Spam etc will help in creating more efficient and secure ecosystem.

Secured Protocol and Algorithms

Research in protocols and algorithms is an important aspect for strengthening the cyber security posture at a technical level. Protocols and algorithms define the rules for information allocation and processing over cyberspace.

Cyber Forensics

In India, the research is being carried out to build indigenous capabilities for cyber forensics. Some of the specific areas in which research is taking place in the country are: Disk Forensics, Network Forensics, Mobile Device Forensics, Memory Forensics, Multimedia Forensics and InternetForensics.

What access controls are to be taken?

Sometimes employee's access is supplemented as theyarestimulated, relocated, or temporarily assigned to alternative department within theorganization. Users that drag such excess access into their new role may create holes incorporate security or create other business risks. Organizations should consider putting automated controls in place for cyber-access toensure that user privileges are suitable to their particular job function or process role. Access to personally identifiable information must be administered by the need; there mustbe a legal business reason for access.

What about regular surveillance?

A successful surveillance program embraces
practices such as:

1) Surveillance on each layer of security will help ascertain the severity of a securityevent; warnings coming from the internal corporate network might be more urgentthan on the external network.
2) Placement of Network Intrusion Detection/Prevention Systems throughout the corporate network to help detect suspicious or malicious activity.
3) Theguiding norm of "minimum privilege access" should constantly be implemented with respectto sensitive information and logs should be revised regularly for suspiciousactivity.

Security Awareness

- Do not share or write down any "passphrases."
- Never click on links or attachments in e-mail from untrusted sources.
- Do not send sensitive business documents to personal email addresses.
- Having suspicious/malicious action reported to security personnel immediately.
- Educate employees about attacks and how to report fraudulent activity.

II. Conclusion

The risks of cybercrime are very factual and too ominous to be overlooked. Every franchisor and Licensor, indeed every business owner, has to look up to their liability and do somethingabout it.At the very least, every company must conduct a specializedscrutiny of theircyber security and cyber risk;insureagainst losses to the greatest extent possible; and gadget and endorse a well-thought-outcyber policy, including crisis management.

References

[1]. World Economic Forum report on Risk and Responsibility in a Hyper connected World. McAfee 2013 Threats Predictions Report, McAfee Labs. http://www.mcafee.com/ca/resources/reports/rp-threat-predictions-2013.pdf.

[2]. Study of the Impact of Cyber Crime on Businesses in Canada.' International Cyber Security Protection Alliance (May 2013). The study was sponsored by Above Security, Blackberry, Lockheed Martin and McAfee.

[3]. Government of Canada Cyber Security Strategy(2010) http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf

[4]. Deibert, Ron.Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace. Prepared for the Canadian Defense& Foreign Affairs Institute, August 2012.

[5]. https://www.cybercrc.com/programs/next-generation-cyber-security-technologies.

[6]. Center for Applied Cyber security Research, Indiana University. Roundtable on Cyber Threats, Objectives, and Responses: A Report. December 2012.

[7]. OPC Speech: New Platforms, New Safeguards: Protecting Privacy in Cyberspace.

[8]. Fall Report of the Office of the Auditor General (2012), Chapter 3 - Protecting Canadian Critical Infrastructure against Cyber Threats.