International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 7, ISSN No. 2455-2143, Pages 178-181
Published Online November 2019 in IJEAST (http://www.ijeast.com)

INTRODUCTION TO CYBER SECURITY

Durgesh Raghuvanshi
B. Tech, department of computer science,
IILM Academy of higher learning
Greater Noida, Uttar Pradesh, India

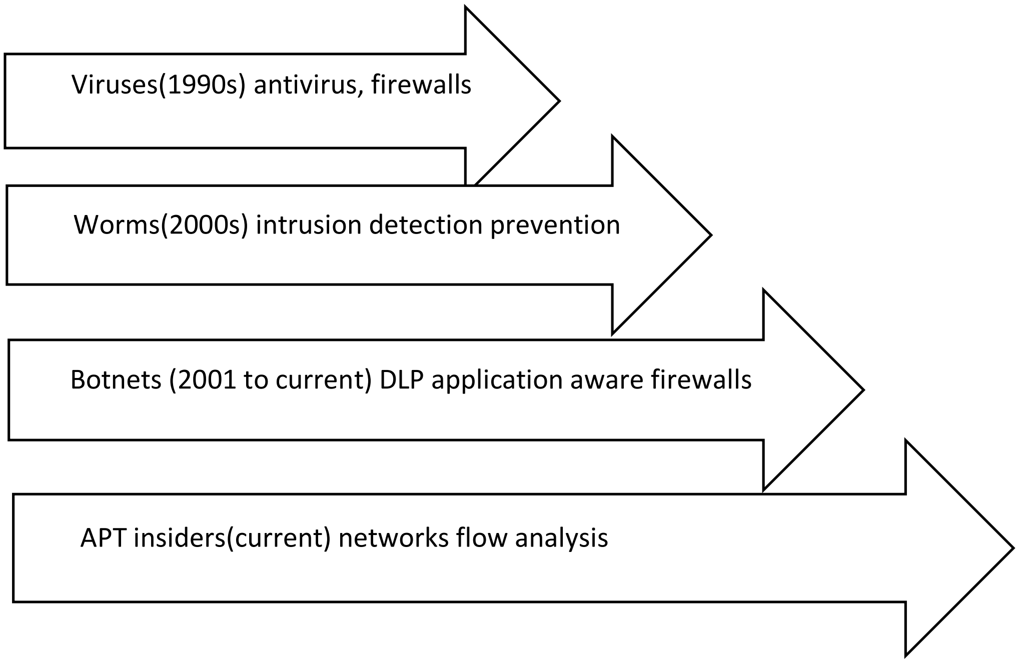
ABSTRACT - This paper describes the basics fundamentals of cybersecurity. A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace is vast in this materialistic world. So there should be security for cybercrimes which are now on upgraded version than the previous condition of the world. The term cybercrime is used to describe an unlawful activity in which computer or computing devices such as smartphones, tablets, Personal Digital Assistants(PDAs), etc. which are stand-alone or a part of a network are used as a tool or/and target of criminal activity. Cyber-Physical System (CPS) are more complex systems, with coordination and deep collaboration between physical and cyberspace. It will involve the various perspective of social and industrial life to bring larger influence and lead computer science to a higher level. CPS may show a discrepancy based on where it applied such as Transport, Defense, Finance, Large scale infrastructure, Process control, Smart grid, and Healthcare. This Paper attempts to summarize the role of Cyber-Physical System in Healthcare/Medicine (MCPS) field, focus on architecture and key challenges for securing MCPS and examinations on how to secure a medical data to improve the life of a human.

KEYWORDS: *malware, cyberspace, cyber-physical system, personal digital assistants, superkeys, proliferation*

I. INTRODUCTION

Internet is among the most important inventions of the 21st century which have affected our life. Today internet has crossed every barrier and has changed the way we use to talk, play games, work, shop, make friends, listen to music, see movies, order food, pay the bill, greet your friend on his birthday/ anniversary, etc. You name it, and we have an app in place for that. It has facilitated our life by making it comfortable. Gone are the days when we have to stand in a long queue for paying our telephone and electricity bills. Now we can pay it at a click of a button from our home or office. The technology has reached to an extent that we don't even require a computer for using the internet. Now we have an internet-enabled smartphone, palmtops, etc. through which we can remain connected to our friends, family and office 24x7. Not only the internet has simplified our life but also it has brought many things within the reach of the middle class by making them cost-effective. It was not long back while making an ISD or even an STD call, the eyes were stricken on the pulse meter. The calls were very costly. ISD and STD were used to pass on urgent messages only and the rest of the routine communication was done using letters since it was relatively very cheap. Now internet has made it possible to not only talk but use video conference using popular applications like skype, gtalk, etc. at a very low price to a level where a one hour video chat using the internet is cheaper than the cost of sending a one page document from Delhi to Bangalore using speed post or courier service. Not only this, the internet has changed the use of typical devices that were used by us. Cyberspace is the connected Internet Ecosystem Cyber Intrusions and Attacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy Cyber Security is protecting our cyberspace (critical infrastructure) from attack, damage, misuse, and economic espionage. Cyberspace has inherent vulnerabilities that cannot be removed.

II. EVOLUTION OF CYBERSECURITY


Viruses(1990s) antivirus, firewalls
Worms(2000s) intrusion detection prevention
Botnets (2001 to current) DLP application aware firewalls
APT insiders(current) networks flow analysis

Virus

A virus is a malicious code written to damage/harm the host computer by deleting or appending a file, occupy memory space of the computer by replicating the copy of the code, slow down the performance of the computer, format the host machine, etc. It can be spread via email attachment, pen drives, digital images, e-greeting, audio or video clips, etc. A virus may be present in a computer but it cannot activate itself without human intervention.

Worms

They are a class of virus which can replicate themselves. They are different from the virus by the fact that they do not require human intervention to travel over the network and spread from the infected machine to the whole network. Worms can spread either through the network, using the loopholes of the Operating System or via email. The replication and spreading of the worm over the network consume the network resources like space and bandwidth and force the network to choke.

Firewalls

An additional tool to protect against Internet threats is the use of a firewall. It is simply a security tool that controls which applications have access to the Internet and which connections are allowed to access our computer. Firewalls are usually programmed to automatically recognize threats, which means they are usually easy to use and do not interfere with the way we use the computer.

Antiviruses

And of course, having an antivirus. It is essential to keep our operating system updated and use the best antivirus to alert and protect us against possible threats. It is also important to run it periodically in order to find and remove malware, as well as perform automatic updates.

If you are debating whether to buy an antivirus license or get one for free, we must bear in mind that although most of the free software is of high quality and offer a reasonable level of security for home users, they do not always offer the same level of protection.

The best option would be to consult with an expert, and if possible, choose an antivirus that has technical support to help us with the configuration.

Indian cyber solution

- India ranks 3rd in terms of the highest number of internet users in the world after the USA and China, the number has grown 6-fold between 2012-2017 with a compound annual growth rate of 44%.
- India secures a spot amongst the top 10 spam-sending countries in the world alongside the USA

- India was ranked among the top five countries to be affected by cybercrime, according to a 22 October report by online security firm ”Symantec Corp”.

III. CYBER THREATS AND SOURCES SOURCES

a) Nation States
b) Cyber Criminal Organisations
c) Terrorists, DTOs, etc., Hackers / Hacktivists

Threats

a) Malware – Malicious software to disrupt computers Viruses, worms, … Theft of Intellectual Property or Data
b) Hacktivism – Cyber protests that are socially or politically motivated Mobile Devices and applications and their associated Cyber Attacks
c) Social Engineering – Entice Users to click on malicious links
d) Spear Phishing – Deceptive Communications (e-mails, texts, tweets) Domain Name System (DNS) Attacks
e) Router Security – Border Gateway Protocol (BGP) Hijacking
f) Denial of Service (DoS) – blocking access to websites.

Hardware cybersecurity concerns

Most equipment and technology for setting up Cyber Security infrastructure in India are currently procured from global sources. These systems are vulnerable to cyber threats just like any other connected system.
Hardware Cyber Security Concerns: There are various types of hardware attacks which includes the following.

- Manufacturing backdoors may be created for malware or other penetrative purposes. Backdoors may be embedded in radiofrequency identification (RFID) chips and memories.
- Unauthorized access to protected memory
- Inclusion of faults for causing the interruption in the normal behavior of the equipment.
- Hardware tampering by performing various invasive operations
- Through the insertion of hidden methods, the normal authentication mechanism of the systems may be bypassed.

Above hardware, attacks may pertain to various devices or systems like:-

- Network systems
- Authentication tokens and systems
- Banking systems
- Surveillance systems
- Industrial control systems
- Communication infrastructure devices

IV. FUTURE SECURITY DESIGN

- Security innovation must deliver more capable solutions to keep pace with threats
- Platforms and security standards must be open to promote collaboration and accelerate adoption
- Technology and security providers must be trustworthy in the creation and operation of their products
- Products and services must be hardened to resist compromise and make security transparent to users
- Security must protect data wherever it exists or is used, for all parties and devices across the computing landscape.

V. CONCLUSION

This paper concludes with basic information of our privilege society which should aware about cyber crimes and its security. The Internet has changed the use of typical devices that were used by us. Television can be used not only for watching popular tv shows and movies but can be used for calling/ video chatting with a friend using the internet. The mobile phone is not only used for making a call but viewing the latest movie. We can remain connected to everyone, no matter what our location is. Working parents from the office can keep an eye on their children at home and help them in their homework. A businessman can keep an eye on his staff, office, shop, etc with a click of a button. It has facilitated our life in more than one way. Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.

VI. REFERENCE

1. Farberov, S. (2014). Russian hackers attacked the US financial system stealing gigabytes of data in suspected retaliation for Ukraine sanctions. Mail Online.
2. Fisher, M. (2013). Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism? The Washington Post.
3. Gollin, G. (2003). Unconventional University Diplomas from Online Vendors:

Buying a Ph.D.University That Doesn't Exist.

4. Gonsalves, A. (2014). How hackers used Google to steal corporate data. www.infoworld.com.
5. Guidance of our faculties of my college department of computer science greater Noida, Uttar Pradesh, India.