Cyber Security - Are we ready for advanced Internet applications?

Sourabh Raja, Prakhar Kumar Singh, Atikant Negi

***Abstract*— The paper focus on the vulnerability of internet towards hacking, internet attacks and how much is our data and privacy safe. It lays emphasis on the effect of such cyber attacks over our society and how people's trust over internet is decided by their geographical location. The paper is going to tell about various techniques through which our internet's security is challenged. It is also going to show how new safety measures are being taken in order to prevent any cyber crime and provide fear free internet and internet applications usage.**

***Index Terms*—Phishing, Key Logger, Internet of Things, Cyber theft, IP Addresses, Remote play, Trends, Security.**

I. INTRODUCTION

HE Internet is becoming the town square for the global village of tomorrow" -Bill Gates. From a Personal computer, to a laptop to a mobile phone and even a gaming console, in today's world every device that has an operating system needs to stay connected to internet if we want an optimal use of its facilities. One cannot use a hardware device for a long period of time without getting connected to internet. The reason is because it's not just our needs that we want to look for on the internet it's also the machine that needs an update every now and then so as to keep up with the everyday changing technology. So if we own a device which connects to the internet quite often it becomes a major concern that whether our device or the data the device is carrying, safe and secure in terms of privacy.

Well the truth is that it is not. Not just the data, even the hardware device is not safe when it comes to connectivity over the internet. Which makes things a little confusing. What should we do then. Should we not use internet or should we leave our resources for open exploitation. Let us know about how are data and device are insecure when it comes to internet usage and how it is effects our daily life decisions. Let us also know whether any measures are being taken in order to provide maximum security and are we ready to accept the change.

II. INTERNET HACKING

A. What is Hacking

When we hear or read the word hacking a lot of things come up in our minds. Mainly like - What is Hacking, Am I a victim of hacking, how I can learn hacking and many more. Let us know about hacking. Hacking is the in use meaning of the word Hack. To hack is to take control over others property with or without their knowledge. In terms of internet, to hack to is to gain authority through genuine or illegal way over a person's data by gaining access to hardware or online accounts. A hacker is someone who commits the act of hacking. It's then the hacker's decision whether it wants to manipulate the victim's data or just have it. Well all such things sound fascinating when read and seems quite dramatic or cinematic but the truth is this is all real. A lot us don't even get to know when they were hacked and how much deep a hacker has its roots inside the victim's system.

B. Techniques for internet security breach

There are a lot of techniques through which one can perform the task of hacking or in simple words get an access to one's privacy. The techniques which we are going to know about know are common ways by which we get attacked and how even a non expert can learn the art of hacking. We will also discuss about how the internet has made changes to prevent such techniques from succeeding and also how we as a user can save ourselves from being a victim. We will also get to know that is the act of hacking just for fun or is our information useful to someone anonymous.

The two very common and highly used ways of hacking are namely Phishing and Key Logging.

C. 1 Phishing

It is a very old and highly used technique. In the process of phishing a fake webpage is designed and sent to people as link for any purpose the user will be interested in. The reason of making the link a desirable to open is very important as if a link will not be worth useful a user might not open it. After the link is opened the user is asked to enter his or her details on web page which is already familiar to the user, like Facebook or Google login. The user falls for the trick and enters the details in order to login while the fake page sends all the data to the person who sent the link. This is a very common practice of getting a users important login information. Even if it is a very old trick not just public users but even professionals fall for this trick making it a very useful technique.

India has emerged as the fourth most targeted country by phishing attacks, receiving 3% of the total; attack volumes, said findings by security firms RSA.
The third quarter 2013 Fraud Report, brands in the US, UK, India and Australia were targeted almost 50% of phishing attacks. India ranked third with the 7% of total phishing attacks volume world wide on brands.

All this has meant that India Inc has lost about $52.9 million(about 328 crore) due to phishing attacks. Globally corporations have lost a total of 1.66 billion for third quarter of the year 2013.

Sourabh Raja is currently pursuing Bachelors degree program in Information Technology engineering in Maharaja Agrasen Institute of Technology Rohini, New Delhi, India, PH-+919911264628.

Prakhar Kumar Singh is currently pursuing Bachelors degree program in Electrical Engineering in Maharaja Agrasen Institute Of Technology Rohini, Nre Delhi, India PH-+9891222776.

Atikant Negi is currently pursuing Bachelors degree program in Northern India Engineering College, Delhi. PH-+9891621836

Fig. 1. Growth rate in Phishing attacks

Countries with highest growth rate - US, India, Vietnam. China with the least.

D. Key logger

In the world of computer science this method of accessing information of or about a user is one of the most deadly and highly used way. A key logger as the name suggests is a small program that can record every keystroke to make over a keyboard. From alphabets to numbers to even an 'ENTER' press, everything can be recorder in the form of a text. And a really hard fact to believe is that a key logger program cannot be detected by an antivirus because it is just another .exe file that will run in your computer without even touching the directory files of the computer making it unnoticeable to an antivirus.

How a key logger is made ? Well its no rocket science to develop a key logger program . All one needs is an operating system that provides a software development environment for different computer languages. In order to create a key logger program we just need to assign a variable with the the key's ASCII value and print it in a text file. In order to run the program we need to convert it into a .exe file and attach it to a often used already existing application such as Google chrome. One also needs to make sure that the program need to run silently in the background. And just within 10 minutes we can make something so powerful that it can record every thing a user does over it's computer. As it can read the key strokes our searches over search engines, our chats, and even our account detail entries.

It is possible to know about a victim of phishing technique as one gets to know about it after the fake web page disappears but there is no known way to tell whether a user has been entering all what it does into a text file because it's only the developer of the key logger who knows when to inject and when to retrieve the information without the user's knowledge.

Now let us know about a few advanced technologies that are going to use internet as a mode of functioning.

III. Internet of Things

What is Internet of things ? " A proposed development of the Internet in which every day objects have network connectivity, allowing them to send and receive data". "If one thing can prevent the internet of things from transforming the way we live and work, it will be a breakdown in security". So are we ready to accept the change the way we live and work by accepting the change in the devices and appliances we install in our houses. Well this question cannot be answered by the people only because as a user everyone would like to be surrounded by advanced technology.

In this proposed concept of internet of things the basic idea is to make most of the devices inside our house to come under a single network. By coming under a single network it means all the devices and the appliances and even home circuitry will be connected to the internet wired or wirelessly 24 hours a day. The use of it, well it will convert every human effort into remote play. One could switch his lights on or off by mere voice commands. All the things wich will come under the internet of things will not just work remotely under a user's commands in fact they will designed as smart devices which will sense its surroundings and act accordingly. For example Refrigerators in the network of internet of things will take updates over the internet to know about the outside weather and change the inside cooling status accordingly.

All of this seems very useful and desirable but it is a point to think upon that why the internet of things is still a prototype.

IV. Advantages and Disadvantages

The advantages of internet of things is very clear :

1.) Remote play - A user will be able to control almost every activity in his house via remote. And this remote need not to be a separate device. Today almost everyone has a smart phone. And it's that smart phone via which access will be gained.

2.) Smart activity - As explained with an example of a refrigerator before smart devices will be able to act even more smartly. They will not just adjust their activity by the information gathered by the sensors from inside the house but also would make changes depending on the update of the world and place provided to them over the internet.

Well there may be very exciting features that come with the concept of internet of things which makes it easier to explain its advantages but there is one major disadvantage which alone is strong enough in preventing this concept turning into a reality. And that disadvantage is :

1.) Security Breach - This paper's sole purpose was to focus on the security of internet, then why did the concept of internet of things was even brought up. Well, to mainly discuss about this disadvantage.

Security breach of a network of internet of things will have a severe effect on the user. If a hacker hacks into the network and gains access over the house hold devices of a person the hacker can play with the user's lifestyle. It could manipulate the working of appliances giving the user a hard time. A hacker will then be able to play with a house's lighting system and circuit switching.

Such kind of an act will turn the boon of such an amazing facility into a bane. We fear to give away our online account details to any other person, think about the situation when the control of a whole house would be someone's hands other than the rightful owner.

So if the network is not safe then what are the innovators of tomorrow going to do. They are not going to sit back and let the world wait for the next big thing.

But what makes the Internet of things still a possibility. How can it be implemented with assured security. In order to do that the manufacturers and the service provider will have to bring a substantial change in the way a device get s connected to a network. And that change is being brought by the change in IP Address of a device. Lt us know more about IP Addresses.

V. IP ADDRESS

An IP address is a fascinating product of modern computer technology designed to allow one computer(or other digital device) communicate with another over the internet. IP addresses allow the location of literally billion of digital devices that are connected to the internet to be pinpointed and differentiated from other devices. In the same sense that someone needs your mail address to communicate a device needs an IP address of another device to communicate.
'IP' stands for Internet protocol, so an IP address is an internet protocol address. What does that mean ? An internet protocol is a set of rules that govern internet activity and facilitate completion of a variety of actions on the World Wide Web.
There are two types of IP addresses currently available to internet users.

.) IPV4
.) IPV6
The two types of IP Addresses namely IPV4 and IPV6 stands for Internet Protocol Version 4 and Version 6 respectively. What is the difference in the version ? Why have two versions ? Which one is better ? All these questions are need to have an answer.

A. Difference between IPV4 and IPV6

Let us first look at technical differences :
1.) IPV4 has a length of 32 bits while IPV6 has a length of 128 bits.
2.) IPV4 are binary numbers represented in decimals while IPV6 are binary numbers represented in hexadecimals.
3.) IPV4 follows Address Resolution Protocol (ARP) while IPV6 follows Neighbor Discovery Protocol (NDP).
Let us now look at some differences between IPV4 and IPV6 which serve as a reason why IPV6 is even brought up.
1.) Static or Dynamic configuration is required to configure IPV4 addresses.
Auto configuration of addresses is available in IPV6 addresses.
2.) Fragmentation is done by sender and forwarding routers in IPV4.
Fragmentation is only done by 'SENDER' in IPV6.

Well the differences do not tell the complete story. The reasons why IPV6 comes into picture are that IPV6 offers a significantly larger pool of addresses by using 128-bit addresses (3.4×10^{38}), compared with the 4.3 billion available in 32 bit IPV4 addresses. The world is running short of IPV4 addresses and a newer form of addresses had to be introduced to full fill the demands of IP address assignment.

B. IV.2 IPV6 : Solving security problems, FOR NOW

The extended pool of IP addresses provides scalability, but also introduces additional security by making host scanning and identification more challenging for attackers.
IPV6 can run end to end encryption. The encryption and integrity checking used in current VPNs is a standard component in IPV6 available for all connections and supported by all compatible devices and systems.
IPV6 also support more secure name resolution. The secure neighbor discovery protocol is capable of enabling cryptographic confirmation that a host is who it claims to be at connection time. This renders Address resolution protocol poisoning and other naming based attack more difficult. And while not a replacement for application or service layer verification, it still offers an improved level of trust in connections. With IPV4 it is fairly easy for an attacker to redirect traffic between two legitimate hosts and manipulate the conversations or at least observe it. IPV6 makes it very hard.

Fig. 2 IPV6 service availability and its service access point across the world. Europe as a whole in leading stage.

The above image shows the fact that India does not have IPV6 addresses available right now for public usage at full swing. Only telecom training centers and established MNCs in India currently run on IPV6. The Indian customers are still running IPV4. In 2012 the Indian Government promised a full IPV6 deployment by the year 2014 but no such significant change is observable even in 2015. Which makes the implement of the concept of Internet of things even more unrealistic to Indian users.

The phrase 'FOR NOW' was used to describe this content because the IPV6 assures security for only now. As the technology is growing it is giving more and more power to the attackers to succeed in their actions. So an ever lasting security promise is hard to make, never the less at least IPV6 solves the problem of shortage of IP addresses.

C. V. Effect on people's choice

The un secure nature of the internet makes the people to stick to conventional methods of daily life. Let us look at one of the major change the nature of trust over the internet makes.

A very innovative concept of - " CASH ON DELIVERY" was brought on by Flipkart, an online shopping website running in the shoes of already successful websites such as Amazon. Slowly and slowly online shopping websites started to increase their market in India giving a tough competition to Fliokart. Even company like Amazon found India to be a potential business hub but could never get a boost in sales as Indian users are afraid of using online transactions. Thus they followed the new concept of CASH ON DELIVERY and thus entered the Indian online sales market. Unlike Amazon and Flipkart various other companies started to show interest.

D. V.1 Trends across the world

It is visible at across the world people of developed countries such as US and UK are more comfortable in making online transactions while people in countries like India people are more comfortable in options like cash on delivery instead of online transactions. Let us have a look at trending nature of India.

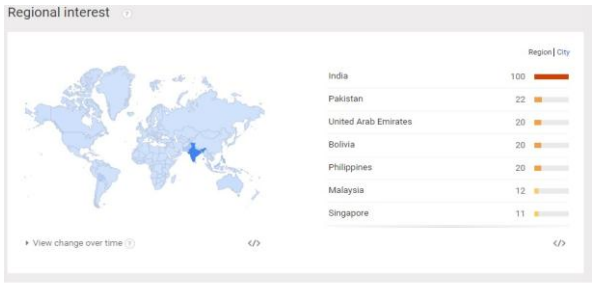

Fig. 3 India at the top in trends for COD

VI. CONCLUSION

The conclusion of this paper mainly concerns with what we can do in order to prevent ourselves from being the next victim of cyber attacks. As a user we should avoid filling any information into a web page opened from an anonymous link. We should keep a check on background running applications in order to know whether an application is running in one's system without his knowledge. The concept of Internet of things is very unique and interesting and will be a real world application very soon. India needs to bring in the change in order to give birth to cyber cities.

ACKNOWLEDGEMENT

The authors wish to thank the ALTTC centre services for information upon IPV6. We want to thank our colleagues from MAIT and Northern India to provided insight and expertise that greatly assisted the research.
We would also like to show our gratitude to our professors for sharing their pearls of wisdom with us during the course of this research.

REFERENCES

[1] .*Andrew S. Tanenbaum - A book over Internet and networking.*
[2] *J.F. Kurose and W.R. Ross, Computer Networking : A Top-Down Approach Featuring the Internet.*
[3] *Stallings and Brown, Computer Security : principles and practice, 3/e(2004 Prentice Hall).*

Sourabh Raja is currently pursuing Bachelors degree program in Information Technology engineering in Maharaja Agrasen Institute of Technology Rohini, New Delhi, India, PH-+919911264628.
Prakhar Kumar Singh is currently pursuing Bachelors degree program in Electrical Engineering in Maharaja Agrasen Institute Of Technology Rohini, Nre Delhi, India PH-+9891222776.
Atikant Negi is currently pursuing Bachelors degree program in Northern India Engineering College, Delhi. PH-+9891621836