Int. J. Chem. Sci.: 14(4), 2016, 2911-2917
ISSN 0972-768X
www.sadgurupublications.com

PROMPT DISCLOSURE OF IP ADDRESS BY INTERNET

V. SRIDEVI*, S. LEELAVATHY, R. SHOBANA and K. SHANTHA SHALINI

Department of Computer Applications, Aarupadai Veedu Institute of Technology, Vinayaka Missions University, CHENNAI (T.N.) INDIA

ABSTRACT

For more than a decade, with the rise in numbers of users, the internet has become an extremely fraught site that has been frequently used in India for the perpetration of a range of 'cyber crimes' from extortion to defamation to financial fraud. Law enforcement authorities in India have not exactly lagged behind in bringing these new age cyber criminals to book, and have installed special 'Cybercrime cells' in different cities to combat crimes on the internet. These cells were particularly adapted at using IP Addresses information to trace individuals who are responsible for crimes. Briefly, an Internet Protocol address (IP address) is a numeric label which is a set of four numbers like 202.54.30.1 which is assigned to every device like computer, printers and all that are participating on the internet. Each website operators and ISPs typically maintain data logs that track the online activity of each IP address that are accessing their services. Although IP Addresses refer to particular computers, not necessarily individual users, it is possible to trace these addresses backwards so that we can expose the individual behind the computer. Even a casual Google search would reveal police authorities in different cities in India that have been quite successful in employing this technology to trace culprits. Along with its utility in the detection of crime, the tracking of persons by their IP addresses is potentially invasive of individual's privacy. Here we will be reviewing the statutory mechanism regulating the retention and disclosure of IP addresses by internet companies in India. In order to provide context, we study with a compilation of anecdotes on how various law enforcement authorities in India have used IP address information to trace individuals responsible for particular crimes.

Key words: IP address, Cyber Security, Data Security, IP Spoofing.

INTRODUCTION

The internet is being increasingly used as a place to commit crimes using personal computers, as well as network-based computers. Although cyber investigation is still in the early stages of its development, the burgeoning use of the internet has increased the

*Author for correspondence; E-mail: sridevi.pranavam@gmail.com, leelasatyam@gmail.com

necessity for digital investigations. Here, this paper is to increase awareness of the latest in digital comparison for cyber-crime investigation with the studies of IP-address and time in computer systems. The approach to improving a cyber-crime investigation is proposed in three stages: independent verification of digital clues, corresponding information from different sources, and preparation of a valid argument.

As network is expanded day-by-day, Internet Protocols are increased in a same manner. Different mechanism and devices are used and a lot of research work is carried out in this area. An Internet Protocol (IP) address is a network address which is unique for every host connection on an IP network. It is numerical values which is assigned to each device and are used in computer network for data communication. It is a transmission mechanism used by the TCP/IP protocols. It is an unreliable and connectionless datagram protocol. It provides host-to-host communication between the users on the internet. There are two versions of Internet Protocol which are basically used, IPV4 (Internet protocol Version 4) and IPV6 (Internet Protocol Version 6). Each computer on the Internet has an IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data, the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. And is sent first to a gateway computer (networking device named router) that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain that gateway then forwards the packet directly to the computer whose address is specified.

EXPERIMENTAL

Literature review

Data security and cyber security

Data security: Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption. Data security is the main priority for organizations of every size and genre. Data security is also known as information security (IS) or computer security. A key data security technology measure is scrambling, where digital data, software/hardware, and hard drives are scrambled and rendered unreadable to unauthorized

users and hackers. It is the practice of keeping data protected from corruption and unauthorized access. The focus behind data security is to ensure privacy while protecting personal or corporate data.

Data is the raw form of information stored as columns and rows in our databases, network servers and personal computers. This may be a wide range of information from personal files and intellectual property to market analytics and details intended to top secret. Data could be anything of interest that can be read or otherwise interpreted in human form. The unauthorized access of some data that are not intended to leave the system, could lead to numerous problems for the larger corporation or even the personal home user. The bank account detail stolen is just as damaging as the system administrator who was just robbed for the client information in their database. There has been a huge emphasis on data security as of late, largely because of the internet. There are a number of options for locking down the data from software solutions to hardware mechanisms.

Encryption

Encryption has become a critical security feature for thriving networks and active home users alike. This security mechanism uses mathematical schemes and algorithms to scramble data into unreadable text.

Strong user authentication

Authentication is a part of data security that is encountered with everyday computer usage. The single sign-on process is a form of authentication that allows you to log into applications, files, folders and even an entire computer system. When logged in, we have various privileges until logging out. Some systems will cancel a session if your machine has been idle for a certain amount of time, requiring that to prove authentication once again to re-enter.

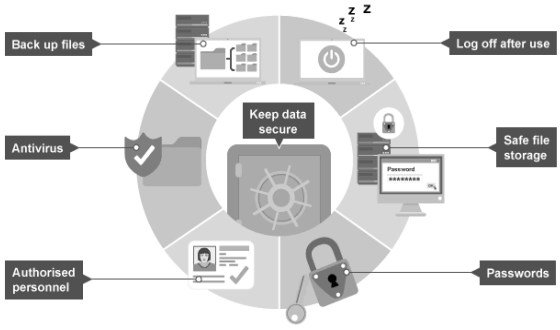

Fig. 1: Data security

Backup solutions

Data security will not be complete without a solution to backup the critical information. Though it may appear secure while confined away in a machine, there is always a chance that the data can be compromised. It could suddenly be hit with a malware infection where a virus destroys all of the files.

Cyber security

Cyber security, also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction. Cyberspace and its underlying infrastructure are vulnerable to a wide range of risk stemming from both physical and cyber threats and hazards. Sophisticated cyber actors and nation-states exploit vulnerabilities to steal information and money and are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. Cyber security will only become more important as more devices, 'the internet of things', become connected to the internet.

Cyber risks can be divided into three distinct areas:

Cyber crime: Conducted by individuals working alone, or in organised groups, intent on extracting money, data or causing disruption, cyber crime can take many forms, including the acquisition of credit/debit card data and intellectual property, and impairing the operations of a website or service.

Cyber war: A nation state conducting sabotage and espionage against another nation in order to cause disruption or to extract data. This could involve the use of Advanced Persistent Threats (APTs).

Cyber terror: An organisation, working independently of a nation state, conducting terrorist activities through the medium of cyberspace.

Cyber criminals operate remotely, in 'automation at a distance', using numerous means of attack available, which broadly fall under the umbrella term of malware (malicious software).An effective cyber security posture should be proportional to the risks faced by each organisation, and should be based on the results of a risk assessment.

http://www.itgovernance.co.uk/shop/p-1434.aspx concentrate at the cyber security challenges faced by business today and proposes a fully structured approach in achieving both cyber security and cyber resilience.

IP Address

An IP address is designed to allow one computer (or other digital device) to communicate with another via the Internet. IP addresses allow the location of literally billions of digital devices that are connected to the Internet to be pinpointed and differentiated from other devices. In the same sense when someone needs our mailing address to send a letter, a remote computer needs the IP address to communicate with the computer. 'IP' stands for Internet Protocol, so an IP address is an Internet Protocol address. 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. Therefore an Internet Protocol address is part of the systematically laid out interconnected grid that governs online communication by identifying both initiating devices and various Internet destinations, thereby making two-way communication possible.

An IP address consists of four numbers, each of which contains one to three digits, with a single dot (.) separating each number or set of digits. Each of the four numbers can range from 0 to 255. Here's an example of what an IP address might look like: 78.125.0.209. This innocuous-looking group of four numbers is the key that empowers you and me to send and retrieve data over our Internet connections, ensuring that our messages, as well as our requests for data and the data we've requested, will reach their correct Internet destinations. Without this numeric protocol, sending and receiving data over the World Wide Web would be impossible.

IP addresses can be either static or dynamic. Static IP addresses never change. They serve as a permanent Internet address and provide a simple and reliable way for remote computers to contact you. Static IP addresses reveal such information as the continent, country, region, and city in which a computer is located; the ISP (Internet Service Provider) that services that particular computer; and such technical information as the precise latitude and longitude of the country, as well as the locale, of the computer.

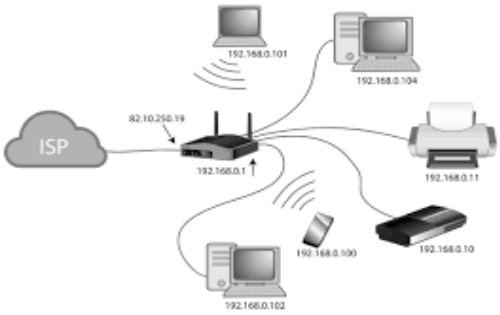

Fig. 2: IP Address

IP Spoofing

IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a false source IP address, for the purpose of hiding the identity of the sender or impersonating another computing system.[1] One technique which a sender may use to maintain anonymity is to use a proxy server. IP spoofing involving the use of a trusted IP address can be used by network intruders to overcome network security measures, such as authentication based on IP addresses. This type of attack is most effective where trust relationships exist between machines. For example, it is common on some corporate networks to have internal systems trust each other, so that users can log in without a username or password provided they are connecting from another machine on the internal network.

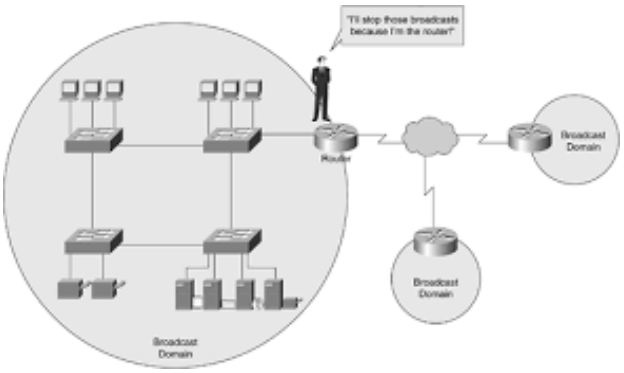

Fig. 3: IP Spoofing

CONCLUSION

The paper describes about the use of IP addresses, the misuse of IP address and the crimes associated with it. IP Address is proved to track down a range of cyber-criminals – from various crimes like financial frauds, to vengeful spurned-lovers, to blackmailers and terrorists. It also gives a description on various security and the threats faced in the society. The summary is that in the future, the Internet should preserve their online privacy and freedom of speech, which will prevent unauthorized access to our data and enable secured access of network in the day to day life.

REFERENCES

1. S. Staniford-Chen and L. T. Heberlein, Holding Intruders Accountable on the Internet. Proc. of the 1995 IEEE, Symposium on Security and Privacy, May, Oakland, CA (1995).

2. D. Schnackenberg, K. Djahandari and D. Sterne, Infrastructure for Intrusion Detection and Response, Proc. of the DARPA Information Survivability Conference and Exposition (DISCEX '00) (2000).

3. D. Piper, The Internet IP Security Domain of Interpretation for ISAKMP, RFC 2407, IETF (1998).

4. D. Maughan, M. Schertler, M. Schneider and J. Turner, Internet Security Association and Key Management Protocol (ISAKMP), RFC 2408, IETF (1998).

5. D. Harkins and D. Carrel, The Internet Key Exchange (IKE), RFC 2409, IETF (1998).

6. A. Keromytis and N. Provos, The Use of HMAC-RIPEMD-160-96 within ESP and AH, RFC 2857, IETF (2000).

Accepted : 31.10.2016