International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

CYBER WARFARE PENETRATION & DESIGN OF PROPOSED GPS HASH KEY ALGORITHM FOR AUTHENTICATION

Harmeet Singh
Research Scholar
Department of Computer Science and Engineering
Ganpati Institute of Technology and Management
Bilaspur, Yamunanagar, Haryana, India

Er. Sandeep kumar
Assistant Professor
Department of Computer Science and Engineering
Ganpati Institute of Technology and Management
Bilaspur, Yamunanagar, Haryana, India

ABSTRACT

By the turn of the century, information, including access to the Internet, will be the basis for personal, economic, and political advancement. The popular name for the Internet is the information superhighway. Whether you want to find the latest financial news, browse through library catalogs, exchange information with colleagues, or join in a lively political debate, the Internet is the tool that will take you beyond telephones, faxes, and isolated computers to a burgeoning networked information frontier. The Internet supplements the traditional tools you use to gather information, Data Graphics, News and correspond with other people. Used

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

skillfully, the Internet shrinks the world and brings information, expertise, and knowledge on nearly every subject imaginable straight to your computer. This research paper focuses on the security and integrity aspects in the cyber security and forensic analysis.

Keywords – Cyber Security, Cyber Warfare, Dynamic Hash Algorithm, Network Security

INTRODUCTION

The World Wide Web (also referred to as WWW or W3) is the fastest growing area of the Internet. While gopher was an important step in allowing users to "browse" through the Internet's vast resources, the World Wide Web has raised excitement about the Internet to new heights.

What makes the World Wide Web appealing and innovative is its use of hypertext as a way of linking documents to each other. A highlighted word or phrase in one document acts as a pointer to another document that amplifies or relates to the first document. When looking at a WWW document, the reader doesn't have to follow every pointer, or link (also called a hypertext link), only those that look interesting or useful. In this way, the user tailors the experience to suit his or her needs or interests. The other very appealing aspect of the World Wide Web is the use of graphics and sound capabilities. Documents on the WWW include text, but they may also include still images, video, and audio for a very exciting presentation. People who create WWW documents often include a photograph of themselves along with detailed professional information and personal interests.

The convergence of digital technologies including television, telephony, and computers has stimulated the reach of the innovations of the Internet. Digital video, audio, and interactive multimedia are growing in popularity and increasing the demand for Internet bandwidth. As yet, however, there has been no convergence or consensus on either the economics or the future

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

policy framework of the Internet. While advanced information and communication technologies make the Internet work, economic and policy issues must now be addressed to sustain the growth and expand the scope of the Internet. This has led to the emergence of the field of Internet Economics as a subject of academic and industry research.

The Internet is a global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link several billion devices worldwide. It is a network of networks that consists of millions of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries an extensive range of information resources and services, such as the inter-linked hyper text documents and applications of the World Wide Web (WWW), electronic mail, telephony, and peer-to peer networks for file sharing.

The origins of the Internet date back to research commissioned by the United States government in the 1960s to build robust, fault-tolerant communication via computer networks. The primary precursor network, the ARPANET initially served as a backbone for interconnection of regional academic and military networks in the 1980s. The funding of a new U.S. backbone by the National Science Foundation in the 1980s, as well as private funding for other commercial backbones, led to worldwide participation in the development of new networking technologies, and the merger of many networks.

Most people access internet content using a web browser. Indeed, the web has become so popular that many people incorrectly treat the internet and the web as synonymous. But in reality, the web is just one of many internet applications. Other popular Internet applications include email and Bit Torrent. The Internet has revolutionized the computer and communications world like nothing before. The invention of the telegraph, telephone, radio, and computer set the stage for this unprecedented integration of capabilities. The Internet is at once a world-wide

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location. The Internet represents one of the most successful examples of the benefits of sustained investment and commitment to research and development of information infrastructure. Beginning with the early research in packet switching, the government, industry and academia have been partners in evolving and deploying this exciting new technology.

Sources of threats

The nature of network incidents and threats has changed over the years as the technology has changed and the opportunities for crime also changed.

Threats to Computer Security

The Computer Systems are vulnerable to many threats which can cause different types of damages and loses which vary from errors harming databases integrity to destruction of entire computer system.

A threat is a indicator, circumstances and an event that has the potential to access resource, cause loss or damage to an asset. Threats generally originate from two primary sources like catastrophic events and human threats which again of two types:- 1. Malicious 2. Non malicious. Non –malicious attacks usually come from users and employees who are not comfortable with the computer security mechanism. These threats cause errors like software bugs, programming and development error, data entry error and administrative mistakes. Whereas malicious “attacks” come from external people or disgruntled employees and ex- employees who have a specific goal and objective to achieve. These attacks are extremely difficult to detect and protect because these persons are most familiar with the organization, computer and application, having knowledge of what difficulties and vulnerabilities may cause the most damage and loss to the

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

organization. According to computer security: - The NIST Handbook special publication 800-12 classifies the threats into nine categories:-

1. Malicious code
2. Malicious Hackers
3. Industrial Espionage
4. Employee Sabotage
5. Loss of Physical and Infrastructure Support
6. Fraud and theft
7. Errors and omissions
8. Foreign Government Espionage
9. Threats to Personal Privacy

Types of Cyber Crimes

When any crime is committed over the Internet it is referred to as a cyber crime. There are many types of cyber crimes and the most common ones are explained below:

Hacking: This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed. In the United States, hacking is classified as a felony and punishable as such. This is different from ethical hacking, which many organizations use to check their Internet security protection. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.

Theft: This crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage software piracy and many of these websites are now being targeted by the FBI. Today, the justice system is addressing this cyber crime and there are laws that prevent people from illegal downloading.

Cyber Stalking: This is a kind of online harassment wherein the victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make the victims' lives more miserable.

Identity Theft: This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history.

Malicious Software: These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.

Child soliciting and Abuse: This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography. The FBI has been spending a lot of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.

Cyber Crime in Modern Society

Today, criminals that indulge in cyber crimes are not driven by ego or expertise. Instead, they want to use their knowledge to gain benefits quickly. They are using their expertise to steal, deceive and exploit people as they find it easy to earn money without having to do an honest day's work.

Cyber crimes have become a real threat today and are quite different from old-school crimes, such as robbing, mugging or stealing. Unlike these crimes, cyber crimes can be committed single handedly and does not require the physical presence of the criminals. The crimes can be committed from a remote location and the criminals need not worry about the law enforcement agencies in the country where they are committing crimes. The same systems that have made it

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

easier for people to conduct e-commerce and online transactions are now being exploited by cyber criminals.

Categories of Cyber Crime

Cyber crimes are broadly categorized into three categories, namely crime against

- Individual
- Property
- Government

Cyber law is a term used to describe the legal issues related to use of communications technology, particularly" cyberspace" I e. the Internet. It is less of a distinct field of law in the way that property or contract are as it is an intersection of many legal fields including intellectual property, privacy, freedom of expression and jurisdiction. In essence, cyber law is an attempt to apply laws designed for the physical world to human activity on the Internet. In India, The IT Act.2000 as amended by the IT (Amendment) Act 2008 is known as the Cyber law. Cyber laws prevent or reduce large scale damage from cybercriminal activities by protecting information access, privacy, communications, intellectual property (IP) and freedom of speech related to the use of the Internet, websites, email, computers, cell phones, software and hardware, such as data storage devices.

Cyber crime is a generic term that refers to all criminal activities done using the medium of communication technology components, the internet, Cyber space and world wide web (www).Cyber crime involve criminal activities that are traditional in nature such as theft, fraud, forgery, defamation and mischief, all of which are subject to the Indian Penal code. It has become a profession and demographic of a typical cyber criminal is changing rapidly from one person to another person form those who are more traditionally associated with drug –trafficking, extortion and money laundering.

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

Cyber law is a new phenomenon having emerged much after the onset of Internet. Internet grew in a completely unplanned and unregulated manner Internet is growing rapidly and with the population of Internet doubling roughly every 100 days. Cyberspace is becoming the new preferred environment of the world.

With the spontaneous and almost phenomenal growth of cyber space, new and ticklish issues relating to various legal aspects of cyberspace began cropping up. In response to the absolutely complex and newly emerging legal issues relating to cyberspace, Cyber law or the law of Internet came into being. The growth of Cyberspace has resulted in the development of a new and highly specialized branch of law called Cyber laws-Laws of the Internet.

There is one exhaustive definition of the term “Cyber law”, However, Simply put Cyber law is a term, which refers to all the legal and regulatory aspects of Internet and the World Wide Web. Anything concerned with or related to or emanating from any legal aspects or issues concerning any activity of netizens and others in Cyberspace comes within the ambit of Cyber law.

Problem Formulation

This study examines how Internet crimes intellectual crimes and cyber crimes are related to a large extent. It provides a definition of each of the terms and attempts to show how in actuality the use of the term ’cyber crime’ consider both the Internet crimes and the intellectual crimes. The intellectual crimes can occur without having the Internet, but with the application of the Internet. Cyber crime has become a serious problem for everyone who uses the Internet. The biggest threats to all Internet users are malicious users are malicious software programs known as crime ware and social engineering schemes often referred to as phishing and pharming scams. Global connectivity means that havoc can occur in a very short timeframe, throughout the world. The abuse of computer technology may threaten national security public safety and community well being and demolish the lives of affected individuals. A long list of traditional offending has

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

been greatly facilitated by technology advancements such as mobile telephony, the Internet and encryption. Further more new criminal opportunities or new crimes have been created by the development of electronic media. Denial of service attacks, viruses, unauthorized entry, information tampering, cyber stalking, spamming, page-jacking, dumping or phone-napping and computer damage are relatively new types of offending or undesirable behavior that did not exist in the precomputing environment. Likewise the development of computers has created new opportunities for services theft, manipulation of the stock market (through ramping up of stock prices schemes using the Internet) software piracy and other thefts of intellectual property. Because many telecommunications networks such as the public telephone network and the Internet are now connected globally there is an international dimension often added to the offending. It has been suggested that with modern mobile devices such as laptop, computers, mobile phones and modems crimes can also now be committed anytime anywhere with the potential scale of the crime scene and the impact of the offending potentially the entire network connected world.

Research Objectives

- To identify the emerging Cyber law trends and jurisprudence impacting cyberspace in today's scenario.
- To provide a platform for experts from all over the country working in the field of cyber crime , cyber security and cyber laws to control cyber attacks.
- To initiate a serious debate at the national level on how to reduce the cyber crime various ways to damage security trends.
- To address the latest threats, impacts, growing complexity and the emerging information on cyber laws cyber security and cyber crimes.
- To analyze whether the law enforcement mechanism setup in the country is effective in the prevention of cyber crime.

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

- To work in the direction of creating an international network of cybercrimes. Legal authorities could then be a significant voice in the further expansion of cyber-crimes and cyber law legislations throughout the globe.
- Proposed model for GPS based hash key table authentication

REVIEW OF LITERATURE

An overview of literature relevant to the present research work presents a brief introduction to the literature survey which was being performed to extract the available information related to the dissertation from various source like IJCSE papers, white papers, conference papers, journals and various books. Developing literature review survey scholarly articles, books and other sources relevant to a particular issue or theory with a description, summary of research work. To develop a literature cover four stags:-

- Problem formulation
- Literature search
- Data evaluation
- Analysis and interpretation

D Florêncio, C Herley said much of the information we have on cyber-crime losses is derived from surveys. We examine some of the difficulties of forming an accurate estimate by survey. First, losses are extremely concentrated, so that representative sampling of the population does not give representative sampling of the losses. Second, losses are based on unverified self-reported numbers. Not only is it possible for a single outlier to distort the result, we find evidence that most surveys are dominated by a minority of responses in the upper tail (i.e., a majority of the estimate is coming from as few as one or two responses). Finally, the fact that losses are confined to a small segment of the population magnifies the difficulties of refusal rate and small sample sizes. Far from being broadly-based estimates of losses across the population, the cyber-crime estimates that we have appear to be largely the answers of a handful of people

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

extrapolated to the whole population. A single individual who claims $50,000 losses, in an N = 1, 000 person survey, is all it takes to generate a $10 billion loss over the population. One unverified claim of $7,500 in phishing losses translates into $1.5 billion.[1]

D Halder et al said while women benefit from using new digital and Internet technologies for self-expression, networking, and professional activities, cyber victimization remains an underexplored barrier to their participation. Women often outnumber men in surveys on cyber victimization. Cyber Crime and the Victimization of Women: Laws, Rights and Regulations is a unique and important contribution to the literature on cyber crime. It explores gendered dimensions of cyber crimes like adult bullying, cyber stalking, hacking, defamation, morphed pornographic images, and electronic blackmailing. These and other tactics designed to inflict intimidation, control, and other harms are frequently committed by perpetrators who, for many reasons, are unlikely to be identified or punished. Scholars, researchers, law makers, and ordinary women and their supporters will gain a better understanding of cyber victimization and discover how to improve responses to cyber crimes against women[2]

LYC Chang discuss the rapid growth in Internet use in Asia, including a tenfold or more increases in access in China, Indonesia, and India since 2002 has also been accompanied by significant increases in cybercrime. The development of commercial-scale exploit toolkits and criminal networks that focus on monetization of malware has amplified the risks of cybercrime. The law-enforcement response in Asia is briefly reviewed in the context of the 2001 Council of Europe's Cybercrime (Budapest) Convention. We describe the nature of cybercrime (including both "hate" or content and "crime-ware" such as botnets) and compare the laws and regulations in Asian states with the provisions of the Convention. The challenges faced in developing effective cross-national policing of cybercrime in Asia are also addressed as problems emerge around cloud computing, social media, wireless/smart phone applications and other innovations in digital technology[3]

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

T Herr, S Romanosky discuss about Cyber crime covers a wide range of activities that includes theft, fraud and harassment; stealing valuable intellectual property as part of industrial espionage; committing financial fraud and credit card theft; and disrupting internet services for ideological goals ("hacktivism"). The crimes target both firms and consumers, and while they rarely result in physical harm or property damage, there can still be severe consequences. This paper frames the topic as a discussion of two markets: one of information security, occupied by victims (e.g., firms and consumers), and one of threats, where buyers and sellers of malicious software and stolen information trade their goods[4]

R Broadhurst said this paper explores the nature of groups engaged in cybercrime. It briefly outlines the definition and scope of cybercrime, theoretical and empirical challenges in addressing what is known about cyber offenders, and the likely role of organized crime groups. The paper gives examples of known cases that illustrate individual and group behaviour, and motivations of typical offenders, including state actors. Different types of cybercrime and different forms of criminal organisation are described drawing on the typology suggested by McGuire (2012). It is apparent that a wide variety of organisational structures are involved in cybercrime. Enterprise or profit-oriented activities, and especially cybercrime committed by state actors, appear to require leadership, structure, and specialisation. By contrast, protest activity tends to be less organized, with weak (if any) chain of command[5]

KKR Choo, P Grabosky said this essay considers how information and communications technologies (ICT) are used by organized crime groups. Three categories of groups are identified: traditional organized criminal groups, which make use of ICT to enhance their terrestrial criminal activities; organized cybercriminal groups, which operate exclusively online; and organized groups of ideologically and politically motivated individuals (including state and state-sponsored actors), who make use of ICT to facilitate their criminal conduct. We feel that it

is important to draw a distinction between these types of organized criminal groups, particularly when formulating cybersecurity policy, because cybercriminality is not a monolithic threat. The article will note the transnational nature of much organized criminal activity and will discuss mechanisms for the control of organized crime in the digital age[6]

KKR Choo illustrate Cyber threats are becoming more sophisticated with the blending of once distinct types of attack into more damaging forms. Increased variety and volume of attacks is inevitable given the desire of financially and criminally-motivated actors to obtain personal and confidential information, as highlighted in this paper. We describe how the Routine Activity Theory can be applied to mitigate these risks by reducing the opportunities for cyber crime to occur, making cyber crime more difficult to commit and by increasing the risks of detection and punishment associated with committing cyber crime. Potential research questions are also identified.[8]

J Warner Cybercrime perpetrated by pockets of citizens in the Global South is increasingly coming to light as a threat to U.S. national and global security; particularly, the West African nation of Ghana has recently come to be recognized as a major hub for cyber-criminal activity. This article argues that although a superficial examination of the process is instructive to a point, in attempting to understand the practice of Ghanaian cybercrime, a more profound investigation of local ground-level realities is necessary. As such, it presents a broad overview of the rise and practice of cybercrime in Ghana, before offering three ground-level case studies (relating to West African geopolitics, the techno-spiritual paradigm of Sakawa, and the justificatory philosophies of social justice) that are necessary for understanding Ghanaian cybercrime yet also largely under-recognized in Western discourses[8]

JP Farwell said that the discovery in June 2010 that a cyber worm dubbed ‘Stuxnet’ had struck the Iranian nuclear facility at Natanz suggested that, for cyber war, the future is now. Yet

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

more important is the political and strategic context in which new cyber threats are emerging, and the effects the worm has generated in this respect. Perhaps most striking is the confluence between cyber crime and state action. States are capitalising on technology whose development is driven by cyber crime, and perhaps outsourcing cyber attacks to non-attributable third parties, including criminal organisations. Cyber offers great potential for striking at enemies with less risk than using traditional military means. It is unclear how much the Stuxnet program cost, but it was almost certainly less than the cost of single fighter-bomber. Yet if damage from cyber attacks can be quickly repaired, careful strategic thought is required in comparing the cost and benefits of cyber versus traditional military attack. One important benefit of cyber attack may be its greater opportunity to achieve goals such as retarding the Iranian nuclear programme without causing the loss of life or injury to innocent civilians that air strikes would seem more likely to inflict. Nevertheless, cyber attacks do carry a risk of collateral damage, with a risk of political blowback if the attacking parties are identified. Difficulty in identifying a cyber attacker presents multiple headaches for responding. A key strategic risk in cyber attack, finally, lies in potential escalatory responses. Strategies for using cyber weapons like Stuxnet need to take into account that adversaries may attempt to turn them back against us[9]

T Maurer,Belfer illustrate Cyber-warfare is no longer science fiction and the debate among policy-makers on what norms will guide behavior in cyber-space is in full swing. The United Nations (UN) is one of the for a where this debate is taking place and the focus of this paper. The activity at the UN over the course of the past decade exhibits an astonishing rate of norm emergence in cyber-space relative to typical international relations timelines. Most recently, Russia together with China (and Tajikistan and Uzbekistan) proposed an "International code of conduct for information security" in September 2011. In 2010, the U.S. reversed its long-standing policy position by co-sponsoring for the first time a draft resolution on cyber-security that has been introduced in the UN General Assembly by the Russian Federation since 1998. Generally, two principal streams of negotiations regarding cyber-security can be distinguished at

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

the United Nations: a politico-military stream focusing on cyber-warfare and an economic stream focusing on cyber-crime[10]

N Choucri said almost everyone recognizes the salience of cyberspace as a fact of daily life. Given its ubiquity, scale, and scope, cyberspace has become a fundamental feature of the world we live in and has created a new reality for almost everyone in the developed world and increasingly for people in the developing world. This paper seeks to provide an initial baseline, for representing and tracking institutional responses to a rapidly changing international landscape, real as well as virtual. We shall argue that the current institutional landscape managing security issues in the cyber domain has developed in major ways, but that it is still "under construction." We also expect institutions for cyber security to support and reinforce the contributions of information technology to the development process. We begin with (a) highlights of international institutional theory and an empirical "census" of the institutions-in-place for cyber security, and then turn to (b) key imperatives of information technology-development linkages and the various cyber processes that enhance developmental processes, (c) major institutional responses to cyber threats and cyber crime as well as select international and national policy postures so critical for industrial countries and increasingly for developing states as well, and (d) the salience of new mechanisms designed specifically in response to cyber threats[11]

A Yassir, S Nayak said this research paper discusses the issue of cyber crime in detail, including the types, methods and effects of cyber crimes on a network. In addition to this, the study explores network security in a holistic context, critically reviewing the effect and role of network security in reducing attacks in information systems that are connected to the internet. As, all this adversely affects the efficiency of information security of any kind of security that exists and is used in information systems. Since hackers and other offenders in the virtual world are trying to get the most reliable secret information at minimal cost through viruses and other

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

forms of malicious soft-wares, then the problem of information security the desire to confuse the attacker: Service information security provides him with incorrect information; the protection of computer information is trying to maximally isolate the database from outside tampering. In other words, the Internet is a large computer network, or a chain of computers that are connected together. This connectivity allows individuals to connect to countless other computers to gather and transmit information, messages, and data. Unfortunately, this connectivity also allows criminals to communicate with other criminals and with their victims[12]

P Stephenson discuss in physical crime the concepts of crime scene assessment and offender profiling are well-accepted if occasionally controversial. Work by the FBI has put profiling into the mainstream of investigative theories. However, in the digital world no such progress has been made. Further, the notion of offender profiling addresses the psychological continuum whereas we are concerned with the criminological spectrum. The ongoing research reported in this paper will begin the process of translating physical crime scene assessment techniques into digital practice. The potential benefits of accomplishing this successfully are significant. Unfortunately, the translation between physical investigation and digital investigation is not straightforward. The addition of particular techniques pioneered by crime assessment experts in physical investigations has turned out to be far more promising than application of psychological profiling. This research-in-progress paper presents a new approach to cyber crime assessment. It views the computer as the crime scene and it applies a crime typology[13]

SM Nirkhi said internet has provided us a much more convenient way to share information all over the world. Cyberspace also opened a new platform for criminal activities. With increased access to computers across the world, cybercrime is becoming a major challenge to law enforcement agencies. Cybercrime investigation process is in its infancy and there has been limited success in prosecuting the offenders; therefore a need to understand and strengthen the existing investigation methods and system for controlling cybercrime is greatly needed.

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

Cybercrime is defined as Illegal computer-mediated activities that can be conducted through global electronic networks. One of the Problem in cybercrime investigation is identity tracing. It is difficult to trace identities due to the anonymity of cybercrime. Therefore tracing the identity of anonymous user has been identified as significant problems which hamper investigations.

There is an increase in the number of cybercrime incidents through anonymous emails. Nowadays, government, industries and individuals rely on email for communication. Criminals make use of the anonymity in the cyber world to conduct illegitimate activities. Mostly Such activities can be conducted via E-mail. Extracting knowledge and information from e-mail text & its analysis provides evidence for cybercrime Investigation. In this paper focus is on analysis of email messages using statistical analysis, social network analysis along with their implementation, and our proposed method to identify the most plausible author of email texts[14]

Reported Cyber Crimes Incident Report Summary 2011-2014

No.	Types of incident	2011	2012	2013	2014
1	Phishing	10	6	6	4
2	Abuse/Privacy	10	20	2	3
3	Scams	11	10	3	4
4	Malware	12	5	1	1
5	Defacements	15	8	20	3
6	Hate /Threat Mail	8	12	3	1
7	Unauthorized Access	3	10	3	2
8	Intellectual property violation	0	0	5	4
9	Dos Attack	0	0	1	0
10	Fake Accounts	0	80	1425	1500

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

	Total	69	151	1469	1522

The advanced speed of technology has made it easier for computer criminals to conceal information about their crimes. Due to the complexity of the digital environment, evidence is collected and handled differently that it was in the past and often requires careful computer forensic investigation. Crimes committed by computer users may cause damage or alteration to the computer system. Compromised computers may possibly be used to launch attacks on other computer crimes. The FBI is sensitive to the victim's concerns about public exposure so any decision to investigate is jointly made between the FBI and the United State Attorney in order to take the victim's needs into account.

Preventive or deterrent measures are difficult in the cyber world, partly because of the ability of attackers to remain anonymous. An unrestricted cyber war offensive however would almost certainly give a few clues as to their identity. Computer network designs should integrate notions of robustness and survivability, while contingency plans for the continued implementation of critical roles and missions with far less cyber connectivity are important. The federal Bureau of Investigation (FBI) Chief stated at a senate hearing that the number of computer crimes doubled in 2011. In 2000, 547 cases on computer intrusion were opened. Later the number of similar cases increased to 1156 in 2001. The FBI stated that the main threat came from the computer experts, hackers and virus founders who are not satisfied with their life or the way they life so they hunt for money. According to the United States of America's official statistics, it was found that of the 90% interviewed whose computer systems had undergone Internet attacks in 2011, 74% stated that penetration or financial fraud. Financial losses from information embezzlement and financial fraud result in $68 million respectively. Financial losses of the 273 interviewed resulted in more than 265 million dollars. In 1998 the loss from attacks such as service was $77,000 and dramatically increased up to $116,000 in 2000.

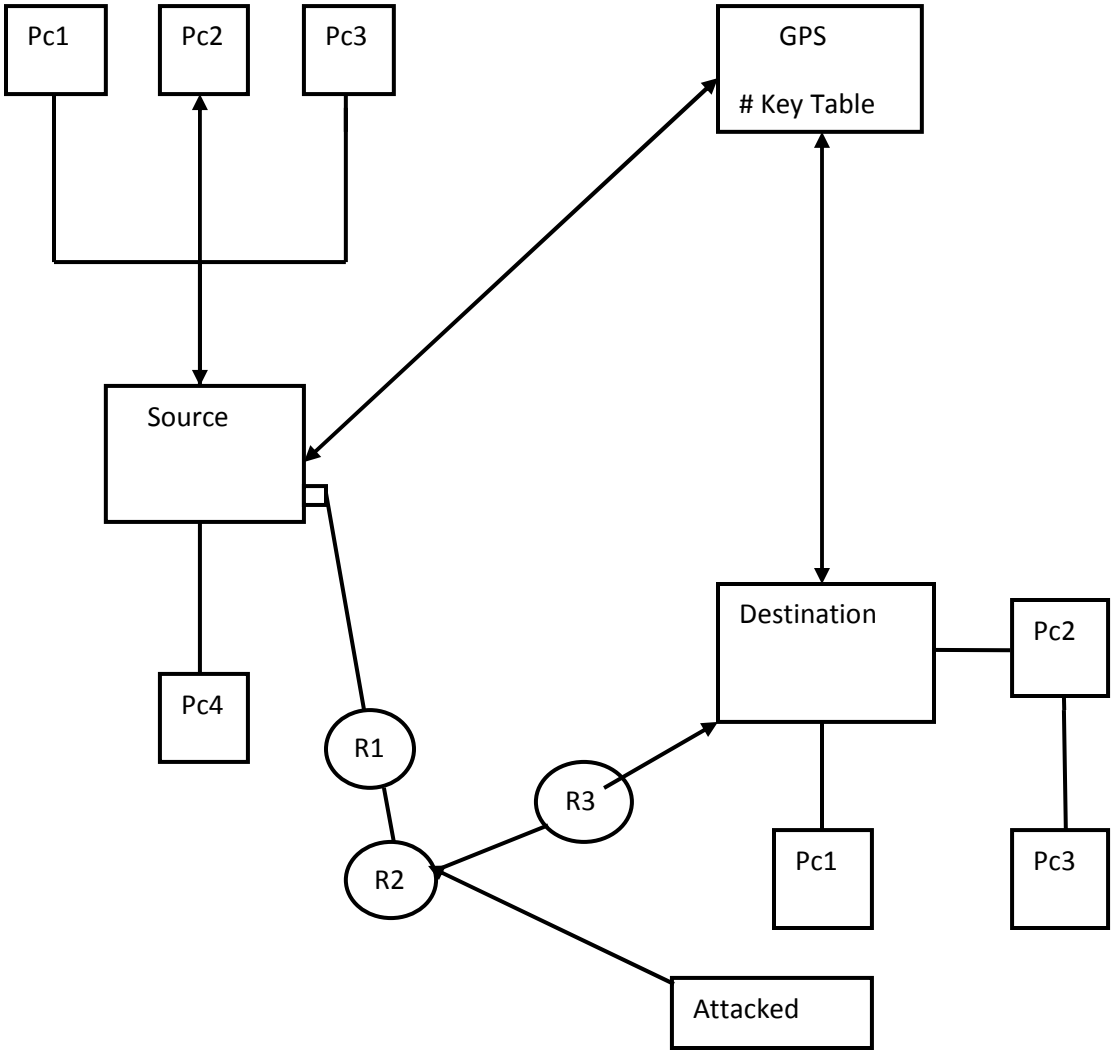
International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

GPS Based Hash Key Model For Authentication



P1 = Packet Source

K1 = Source Key Packet

G1 = k1 (G1-> gps # key table)

P1.K1 -> Destination

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

In Destination
D1= P1. K1
If P1. k1 = G1. K1
Open Packet Else
Reject Packet

Here in source the packet will be formed with its own authentication key a part from that a special authentication key will be generated by source which will be attached in packet as well as a copy of key will send to Gps based hash key table. When Destination received the packet with key it will compare the key with Gps base # table, if both the keys are same then it open the packet if packet get tempered the attached key will automatically changed and it will not match with destination key in such case the packet will get discarded.

If packet get tempered the K0 turned in K0.1 hence the linked key K1 will also changed to k1.1
The Original content of GPS base # key table = K1

Packet will be transmit from one source to destination with private key value after reach at the destination point a new hash key value be generated with maching mac address which would be match with before sending key value and hash key match with mac address on another end and message packet be decrypt after matching values If keyp value are different then packet rejected automatically and get request to source for sending message again to receiver end with new key value.

CONCLUSION

Nations are more robust that the early analyst of cyber terrorism and cyber warfare give them credit for and cyber attacks are less damaging than physical attacks. To understand the infrastructure a much more detailed assessment if redundancy normal rates of failure and

International Journal of Computing and Corporate Research

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

response the degree to which critical functions are accessible from public networks and the level of human control, monitoring and intervention in critical operations. Terrorists or foreign militaries may well launch cyber attacks, but they are likely to be disappointed in the effect. Digital Pearl Harbors are unlikely Infrastructure systems because they have to deal with failure on a routine basis are also more flexible and responsive in restoring service than early analysts realized. Cyber attacks unless accompanied by a simultaneous physical attack that achieves physical damage are short lived and ineffective. However if the risks of cyber terrorism and cyber war are overstated the risk of espionage and cyber crime may be not be fully appreciated by many observers. This is not a static situation and the vulnerability of critical infrastructure to cyber attack could change if three things occur. Vulnerability could increase as societies move to a ubiquitous computing environment when more daily activates have become automated and rely on remote computer networks. The second is that vulnerability could increase as more industrial and infrastructure applications especially those used for SCADA (Supervisory Control and Data Acquisition) move from relying on dedicated proprietary networks to using the Internet and Internet protocols for their operations. This move to greater reliance on networks seems guaranteed given the cost advantage of Internet communication protocols but it also creates new avenues of access. These changes will lead to increased vulnerabilities if countries do not balance the move to become more networked and more dependent on Internet protocols with efforts to improve network security, make law enforcement more effective and ensure that critical infrastructure are robust and resilient. From a broader security perspective nations now face a range of amorphous threats to their safety that are difficult for the traditional tools of national security to reach. The lines between domestic and foreign, private and public or police and military are blurring and the nature and requirements of national security are changing rapidly. The most important implications of these changes for cyber security may well be that national policies must adjust to growing interdependence among economies and emphasize the need for cooperation among nations to defeat cyber threats.

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

REFERENCES

[1] D Florêncio, C Herley (2013)- Sex, Lies and Cyber Crime Surveys Chapter: Economics of information security and privacy Vol. III, Page no.35-53 – Springer

[2] D Halder, K Jaishankar, K Jaishankar (2012) - Cyber crime and the victimization of women: laws, rights and regulations Chapter 9: Cyber Victimization of Women and Cyber Laws in India (pages 113-128)

[3] R Broadhurst, LYC Chang Cybercrime in Asia: Trends and Challenges Chapter: Handbook of Asian criminology,pp 49-63, 2013 – Springer

[4] T Herr, S Romanosky - Cyber Crime: Security Under Scarce Resources, American Foreign Policy Council Defense Technology Program Brief, No. 11, June 2015

[5] R Broadhurst, P Grabosky, M Alazab An Analysis of the Nature of Groups engaged in Cyber Crime, International Journal of Cyber Criminology January-June 2014, Volume 8 (1): 1-20.

[6] Kim-Kwang Raymond and Grabosky, Peter, Cyber Crime(October 15, 2013) Oxford Handbook of Organized Crime, L. Paoli, Oxford University Press, 2013

[7] KKR Choo The cyber threat landscape: Challenges and future research directions November 2011, Chapter: Computers & Security,Volume 30, Issue 8, Pages 719–731

[8] J Warner Understanding Cyber-Crime in Ghana: A View from Below, The International Journal of Cyber Criminology, 2011

[9] JP Farwell, R Rohozinski Stuxnet and the future of cyber war chapter: Survival : Global Politics and Strategy,Volume 53, pages 23-40 28 june, 2011

[10] T Maurer - Belfer "Cyber Norm Emergence at the United Nations—An Analysis of the UN's Activities Regarding Cyber-security." Discussion Paper 2011-11 Center for Science and International.

[11] N Choucri, S Madnick, J Ferwerda - Institutions for Cyber Security: International Responses and Global Imperatives, Chapter: Information Technology for Development,Volume 20,Pages 96-121 22 Oct , 2014

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

[12] A Yassir, S Nayak - Cybercrime: A threat to Network Security , IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.2, February 2012

[13] P Stephenson, R Walter - Cyber crime assessment, System Science (HICSS), 2012 45th Hawaii International Conference on 4- 7 jan 2012, Pages 5404 - 5413

[14] SM Nirkhi, RV Dharaskar… Analysis of online messages for identity tracing in cybercrime investigation Cyber Security, Cyber, 2012

[15] P Kumar, S Mittal The Perpetration and Prevention of Cyber Crime: An Analysis of Cyber Terrorism in India,International Journal of Technoethics (IJT), 2012 - Volume 3, Pages 1-10

[16] Y Joshi, A Singh - A Study on Cyber Crime and Security Scenario in India, International Journal of Engineering and Management Research, Pages: 13-18,Volume-3, Issue-3, June 2013

[17] VK Gunjan, A Kumar,A survey of cyber crime in India Advanced Computing Technologies (ICACT), 2013 15th International Conference on 21-22 Sept. 2013,Pages 1 - 6

[18] M Arora, KK Sharma, S Chouhan, Cyber Crime- International Journal of Recent Research Aspects, Special, Issue Feb 2015, pp. 35-37

[19] Nick Nykodym, Sonny Ariss, Brian A. Patrick, Cody Holman, (2013) "Workplace Violence and Cyber Crime Prevention," Journal of Applied Business and Economics, Vol. 15, pp.71 - 76

[20] JA McGee, JR Byington, Journal of Corporate Accounting & Finance, Vol. 24, Pages 45–49, July/August 2013

[21] KK Sindhu, BB Meshram Digital Forensics and Cyber Crime Datamining, JournalofInformationSecurity,Vol.3 (2012), Pages1-6

[22] H Chen, W Chung, JJ Xu, G Wang, Y Qin, M Chau, Crime data mining: a general framework, Vol. 37, Issue:4, Pages 50-56, April 2004

ISSN (Online) : 2249-054X

Volume 5 Issue 5 September 2015

International Manuscript ID : 2249054XV5I5092015-01

[23] B Sahu, N Sahu, SK Sahu, Systems and Network(2013), Communication Systems and Network Technologies (CSNT), 2013 International Conference on,8 April 2013,Pages- 450 - 452

[24] A Alkaabi, G Mohay, A McCullag, forensics and cyber crime, 2011, Chapter: Digital Forensics and Cyber Crime,Vol.53 of the series Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering pp 1-18

[25] A Tajpour, S Ibrahim, M Zamani, International Journal of Information Processing & Management . Nov 2013, Vol. 4 Issue 7, pages51-58

[26] C Edwards, Biometric Technology Today, Vol. 2014, Issue 2, February 2014, Pages 9–11