International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Interception in Information Communication Technology Special Reference to Cryptography, Information Security & Law

Srinivas Katkuri
Research Scholar University College of Law, Osmania University, Hyderabad, Telangana, India

ABSTRACT

A rapid increase in the use of Information Communication Technology has given rise to new forms of malicious activities and incidents. Threats emanate from a wide variety of sources, and their effects carry significant risk for public safety, the security of nations and the stability of the globally linked international community as a whole. The origin, identity of the perpetrator, or motivation for the disruption can be difficult to ascertain. Threat actors can operate with substantial impunity from virtually anywhere. Many malicious tools and methodologies originate in the efforts of cybercriminals and hackers. The growing sophistication and scale of criminal activity increases the potential for harmful actions. The technical defense like cryptographic techniques to prevent and control of the intruders and their activities, need of legal provisions discussion in the knowledge court and some suggestions are to be explored in this Research paper.

Key words: Cryptography, Intruders, Information Security, Computer resources, Threats.

I. INTRODUCTION

The number of threats exponentially growing, tools to hack or crack became more sophisticated and powerfully enhancing. More than 12,000 incidents of cybercrime were reported in 2016, but nearly the same number of such crimes carried forward from the previous years had not been investigated, the data released by the National Crime Records Bureau (NCRB) said. Only in 30% cases reported in 2016, the police or the investigating agency filed a charge sheet. In absolute numbers, 7,990 persons were arrested for the crimes, which included 147 women and charge sheets were filed against 4,913 accused. Illegal gain (5,987 incidents) and revenge (1,056) were the two top motives that accounted for cybercrimes. Sexual exploitation (686), insulting the modesty of women (569) and causing disrepute (448) constituted 13% of the crimes [1].

II. INFORMATION SECURITY

According to Peltier, Thomas R.[α], "**Information** security is the prevention of, and recovery from, unauthorized or undesirable destruction, modification, disclosure, or use of information and information resources, whether accidental or intentional." Section 2-D(nb) of Indian Information technology act, 2000[β] (as amended by The IT (Amendment) Act, 2008) defines "Cyber Security" as protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. Cyber Security synonymously used for

[α] Author of the book *Information security policies and procedures: a practitioner's reference,* 2nd Ed.

[β] Known as the Cyber law.

CSEIT1831145 | Received : 15 Jan 2018 | Accepted : 03 Feb 2018 | January-February-2018 [(3) 1 : 666-670]

Computer security or information security. Cyber Security threats spring from a number of sources and factors, few of them as follows:

- ✓ weaknesses in network and communication protocols,
- ✓ growth of cyber space
- ✓ growth of hackers and crackers
- ✓ operating system protocol vulnerability,
- ✓ insider effect,
- ✓ social engineering,
- ✓ physical theft,
- ✓ mass surveillance by intelligence agencies (like NSA).

III. CRYPTOGRAPHY

Until the1950s cryptography was essentially used only for military and diplomatic communication. The decryption of German messages by the English and of Japanese messages by the Americans played a very important role in the outcome of the Second World War. The great mathematician Alan Touring made an essential contribution to the war effort with his decryption of the famous Enigma machine which was considered absolutely secure by the Germans. Cryptography also played a vital role and strongly influence in the interception. Cryptography was used to keep the messages of governments, military and diplomatic organizations secret.

The art of keeping secrets resulted in victories in wars and in growth of mighty empires. Powerful rulers learned to keep secrets and pass information without interception; that was said to the beginning of cryptography. Although the basic concepts of cryptography predate the Greeks, the present word cryptography, used to describe the art of secret communication, comes from the Greek meaning "secret writing." From its rather simple beginnings, cryptography has growth in tandem with technology and its importance has also similarly grown. Just as in its early days, good cryptographic prowess still wins wars [2].

Nowadays, more and more commerce activities, business transactions and government services are taking place and being offered over the Internet, in particular, via World Wide Web-based tools. Many of these applications require security services. Shopping, billing, banking, administration of job or university applications, and tax assessments are a few such examples. For these applications, authentication, confidentiality and integrity are the most commonly needed security services.

Cryptography has become the main tool for providing the needed digital security in the information communication medium that far exceeds the kind of security that was offered by any medium before it. It guarantees authorization, authentication, integrity, confidentiality, and non-repudiation in all communications and data exchanges in the new information society.

How can we be confident that a cryptographic algorithm or a protocol is secure? Is it valid to say that an algorithm is secure because nobody has broken it? The answer is, unfortunately, no. In general, what we can say about an unbroken algorithm is merely that we do not know how to break it yet. Because in cryptography, the meaning of a broken algorithm sometimes has quantitative measures; if such a measure is missing from an unbroken algorithm, then we cannot even assert whether or not an unbroken algorithm is more secure than a known broken one [3].

There was widespread fear among government, networking manufacturers, security researchers, and IT executives because the component is vital in many communication grids including national critical infrastructures such as parts of the Internet, phone systems, and the electrical power grid. These networks were vulnerable to disruptive buffer overflow and malformed packet attacks [4].

Cryptographic algorithms for confidentiality and authentication assume greater importance. As well, designers need to focus on Internet-based protocols and the vulnerabilities of attached operating systems and applications. Security is a concern of organizations with assets that are controlled by computer systems. By accessing or altering data, an attacker can steal tangible assets or lead an organization to take actions it would not otherwise take. By merely examining data, an attacker can gain a competitive advantage, without the owner of the data being any the wiser.

A significant security problem for networked systems is hostile, or at least unwanted, trespass by users or software. User trespass can take the form of unauthorized logon to a machine or, in the case of an authorized user, acquisition of privileges or performance of actions beyond those that have been authorized. Software trespass can take the form of a virus, worm, or Trojan horse. All these attacks relate to network security because system entry can be achieved by means of a network. However, these attacks are not confined to network-based attacks. A user with access to a local terminal may attempt trespass without using an intermediate network. A virus or Trojan horse may be introduced into a system by means of a diskette. Only the worm is a uniquely network phenomenon. Thus, system trespass is an area in which the concerns of network security and computer security overlap [5].

IV. INFORMATION SECURITY THREATS

Ensuring the security of the global computer networks requires maintaining the highest intrinsic value of both the tangible objects and information the intangible one [6]. According to Daniel Bernstein,[φ] without cryptography, what people send via computers is the electronic equivalent of a postcard, open to view by many people while the message is in transit. With cryptography, people can put both messages and money into electronic 'envelopes,' secure in the knowledge that what they send is not accessible to anyone except the intended recipient. Continued development of cryptography promises to make it possible for the worldwide computer Internet to offer private, secure and protected communication among billions of people worldwide [7].

The principal objective of intruder should be either to gain access to computer systems or increase the range of privileges accessible on computer resources. Drawbacks in symmetric cryptographic ciphers enhanced in asymmetric cryptographic ciphers with revolutionary ‘concept of public key’, which playing vital role in confidentiality. According Bruce Schneier the National Security Agency (NSA) has the best cryptographers in the world, who were capable to break the any cryptographic ciphers. Recently Edward Snowden, a former US spy agency contractor who leaked details of major US surveillance programmes. The USAs security agency NSA developed the programmes of mass surveillance on global communication to malicious purpose, in such a programmes even RC4 ciphers and network layers protocol like Security Socket Layer (SSL) breaked to accesses the information resources and succeeded.

V. LAW & PROVISIONS

International conventions and Indian statutes like Indian Penal Code, Information Technology act and Electronics Communication Privacy Act (USA) defines that act of unauthorized access of global and domestic communication is a illegal, wrong full, and harm full criminal activity .

It is the fact that law and information security are related in number of ways, where statutes protect privacy and secrecy of individuals. Law and legal devices are regulates and protect the rights of developers and owners of program or data, and also to protect the confidentiality, integrity and

[φ] A Ph.D. candidate in mathematics at the University of California at Berkeley, Daniel Bernstein worked in the field of cryptography, and developed an encryption algorithm, or recipe, which he calls 'Snuffle.'

availability of computer resources and network. However law should not provide always an adequate control and protection whenever computer resources concerned, cyber laws complex in nature and are slowly evolving as one branch. Law enforcement agencies can access communication and information resources, if it proved to be probable cause. Such agencies if proved to Judge or judicial authority that interception needed in following purpose only:

- ✓ Matter of life or death,
- ✓ Public importance,
- ✓ Gain evidence on criminal activity, &
- ✓ Alert on terrorism.

In Indian legal scenario section 69 of Information Technology(IT) act (Substituted Vide ITAA 2008), which provides powers to central Government or a State Government or any of its officer specially authorized to issue directions for interception or monitoring or decryption of any information through any computer resource, in the interest of the sovereignty or integrity of India, defense of India, security of the State, for preventing incitement to the commission of any cognizable offence relating to Cyber Security. Whereas Section 69B of IT Act enumerates Central Government may authorize to monitor and collect traffic data or information through any computer resource for Cyber Security, by notification in the official Gazette.

VI. CONCLUSION

There is strong need to understand about advanced technology by law enforcement authority and at the same time industry must understand the motives of law enforcement. It is interesting to know that few days back Washington Daily revealed that the USA court permitted to allow the interception of communication in Indian while elections for loksabha in 2014 and election activities especially focused shadow on Prime Minister (PM) candidate from BJP, Sri. Narendra Modi(Present India PM). These are the illegal activities on the computer resources and network systems. It is big hurdle to convict the mass surveillance activity of intruders, even USA debates and justifies their malicious activity showing FISA[η] the statute as shield. FISA makes illegal intentional engage in electronic surveillance under appearance of an official act. It is surprise know that an Indian Information Technology act applies to extra territorial boundaries, means that criminals from outside from the nation also be convicted. These issues should be needed to understand broad perspective of both law and technology. The law Enforcing authority in India not well equipped to prevention and detection of cyber crimes. The progress in the law is slower than the progress in the Information Technology. To enforce Cyber Law especially all Judges, Judicial Officer and Investigating officers have to fully aware about Cyber crimes. Cyber Law has both technical and legal aspects to understand widely [8]. Technocrats and Counsels should be fully aware about law and communication technology respectively. Here I conclude that IT act motto is convict criminals in India and from abroad, tracing and catching of intruders(malicious hackers), is challenging task, where FISA motive to spy on targeted individual in countermeasure of terrorism, but such statute misusing by NSA. These technical and legal issues should be discussed in the International knowledge court to avoid misconceptions and misunderstandings. However Privacy was constitutional safeguard provided by supreme law to be protected as procedure established by law.

[η] An act, the Foreign Intelligence Surveillance Act of 1978 as amended FISA Amendment act 2008 to establish a procedure for authorizing certain acquisitions of foreign intelligence, and for other purposes.

VII. REFERENCES

[1]. Vijaita Singh, "Many Cybercrime Cases Not Investigated", The Hindu, New Delhi, November 30, 2017.

[2]. Kizza, Joseph Migga, Computer Network Security, 2005 Springer.pg.257.

[3]. Wenbo Mao, Modern Cryptography: Theory and Practice, Publisher: Prentice Hall PTR, 2003, pg.33.

[4]. Kizza, Joseph Migga, Computer Network Security, 2005, pg.77

[5]. William Stallings, Network Security Essentials: Applications and Standards 4th Edition, Prentice Hall, 2011pg 306.

[6]. Kizza, Joseph Migga, Computer Network Security, 2005, pg.78.

[7]. Rosenoer Jonathan., Cyber Law: the law of the Internet, 1997, pg.213.

[8]. Srinivas Katkuri, "Cyber Crimes and Penal Provisions in India", proceedings of National conference on ACPR2014.