# Cyber Crime And Security

**K.Ramya[1], G.Arunachalam[2], S.Kalpana[3], D.Lavanya[4]**
Department of MCA,ECE
[1,2] Assistant Professor, Gnanamani College Of Technology& Engineering, Pachal, Namakkal, Tamilnadu, India
[3,4] Student, Gnanamani College Of Technology& Engineering, Pachal, Namakkal, Tamilnadu, India

***Abstract-*** *Large-scale commercial, industrial and financial operations are becoming ever more interdependent, and ever more dependent on IT. At the same time, the rapidly growing interconnectivity of IT systems, and the convergence of their technology towards industry-standard hardware and software components and sub-systems, renders these IT systems increasingly vulnerable to malicious attack. This paper is aimed particularly at readers concerned with major systems employed in medium to large commercial or industrial enterprises. It examines the nature and significance of the various potential attacks, and surveys the defence options available. It concludes that IT owners need to think of the threat in more global terms, and to give a new focus and priority to their defence. Prompt action can ensure a major improvement in IT resilience at a modest marginal cost, both in terms of finance and in terms of normal IT operation.*

## I. INTRODUCTION

Industry, government and indeed society are becoming critically dependent on IT. This dependence is illustrated by the serious concerns which are now being caused by residual “Year 2000” bugs. The history of crime and crime prevention has been akin to the history of warfare: anoffense is developed, then a defense counters the offense, then a new offense counters the new defense. Machine guns led to the development of tanks which led to the development of rocket propelled grenades, etc. When commerce consisted of camel caravans, people in the Arabian Peninsula promoted banditry, ultimately forcing the commerce to go by sea. When merchants used the sea lanes through the Mediterranean, the people of the Maghreb promoted the Barbary pirates until they were ultimately countered by a punitive US military action. The purpose of this paper is Understanding Cybercrime: Phenomena, Challenges and Legal Response is to assist everyone in understanding the legal aspects of cyber security and to help harmonize legal frameworks. As such, it aims to help better understand the national and international implications of growing cyber threats, to assess the requirements of existing national, Regional and international instruments, and to assist in establishing a sound legal foundation.

### Cyber security and cyber crime

Cybercrime and cyber security are issues that can hardly be separated in an interconnected environment. The fact that the 2010 UN General Assembly resolution on cyber security addresses cybercrime as one Major challenge. Cyber security plays an important role in the ongoing development of information technology, as well as Internet services. 37 Enhancing cyber security and protecting critical information infrastructures are essential to each nation’s security and economic well-being. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy. Deterring cybercrime is an integral component of a national cyber security and critical information infrastructure protection strategy. In particular, this includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national prevention, preparation, response and recovery from incidents on the part of government authorities, the private sector and citizens.

### 1.The Present Situation

In commerce, industry and the public utilities there are now numerous systems of systems - which, **as regards their security features,**:

- are a haphazard collection of disparate, poorly-structured sub-systems.
- have evolved in an unplanned manner.
- and are often used and managed with little regard to their security.

## II. UNAUTHORISED INTERCEPTION

Interception of communications is normally undetectable and, in the absence of suitable countermeasures, offers a tempting target to attackers. In appropriate computer systems, unauthorised access to data-bases, etc., can be monitored and, where this has been done, it has produced ample evidence that probing attacks are indeed taking place on a substantial and increasing scale.

### Type of attack

- ❖ Random(finishing) attack on message or file content.

- “Space-Domain” analysis of organisational structure.
- “Time-Domain” trafficflow Analysis.
- systematic, system-wide message interceptionor data hacking.

**Comment**

- random attack on plain text is quick and easy
- countered by encryption.
- needs sustained effort, but attack is otherwise easy difficult to counter

**pre-requisite for the three forms of attack listed below.**

- needs sustained effort, but attack is otherwise easy
- a little harder still to counter
- must be countered by high-grade encryption
- needs substantial, sustained high-grade effort by
- attacker
- must be countered by high-grade encryption

**The principal defence options are listed briefly below:**

Defence against attack on decrypted redistribution nodes:

- traffic Bulk encryption. This can normally be implemented at relatively low cost, even retrospectively, and should be a standard feature in all networks carryingidentifiable critical.

Defence against attack on decrypted redistribution nodes:

1.Physical & personnel security. This should be - and mostly is - a “matter-ofcourse”for all significant facilities.

2.Routine end-to-end encryption of selected virtual links. This entails the creation of an appropriate key-distribution system - which may use “public-key cryptography” - but it can then superposed in a “transparent” manner on a network - including its encrypted trunk links (i.e. super-encryption) - for the duration of relevant connection session. It should be a standard facility for traffic or users of particular criticality or sensitivity. (The segregation of signalling in a separate channel facilitates this, but increases vulnerability to some other forms of attack.

**Protection of sensitive connection sessions:**

- End-to-end (super)-encryption. This is a variant of the preceding technique,applying it only to those connection sessions judged to warrant it

**1.Defence against Analysis of Organizational Structure:**

- Masking differences in traffic type or volume between different organisationalentities.
- Avoidance of distinctive emissions.
- Defence against traffic-flow analysis (see below).
- Using interface controllers to hide internal systems and network configurations It is frequently worth-while to make structure analysis harder for the attacker, but rarely practical to make it impossible.

**2.Defences against traffic-flow analysis:**

In some critical situations, in public or corporate governance, the mere existenceof a very non-standard pattern of traffic flow could give away sensitive information. If necessary, we may impede or prevent such analysis by:

- Dummy traffic.
- Dummy “post-box” addressees - interface controllers can sometimes alsosubsume this function.
- Filling non-busy links with “empty” key stream.
- Encryption of trunk signalling channels.

**3.Interference with Communications:**

Various forms of interference with communications may also be encountered, either ‘merely’ aiming to cause mayhem or for fraud or blackmail. All cause the receipt of incorrect messages or prevent the receipt of the correct messages (a form of "denial of service").Some of these attacks may be limited in scope, e.g. to a single communications link or a single local computer or a single type of transaction, or they may be limited inthe duration of their impact. On the other hand, attacks which immobilise network control or destroy confidence in the traffic carried would have a very grave pervasive impact, until countered, and so resilience against such attacks is of high importance. As far as we know, none of these active attacks have yet been deployed for criminal, political or terrorist purposes. However, all have been discussed in the literature, and the vulnerability of many important systems to such attacks has been proven by “tiger teams” emulating potential attackers. As shown below, most of these active attacks can be prevented by the appropriate use of crypto techniques, coupled with good, active security management

**4. Physical Attacks Against the Bearer Net:**

We also have to consider attacks against the physical bearer net. Terrestrial networks have at least the potential for a very high degree of redundancy in theircapacity and topology/cross-connectivity. The proper exploitation of this potential robustness requires:

1. Monitoring the availability and capacity of the various links,
2. Adaptive routing,
3. Prioritisation,
4. Possibly adaptation of operational procedures to tailor traffic load to the capacity available,
5. If necessary, restriction of access rights for lower-priority traffic.

**5. Attacks Against Crypto Systems:**

Crypto systems play a critical role in maintaining the security of IT systems against unauthorised reception and exploitation. Furthermore, they are also key components in:
- authentication,
- preventing various subtle attempts to pervert the communications process,
- security in data bases.

**6. Software Attacks on Computers:**

Much of the most vulnerable traffic flow is to, from or between computers. Computer systems generally comprise discrete hardware and software modules, Intercommunicating via “buses” or networks. Hence their defence has much in common with that of communications systems. However, even more than in Communications, most computer hardware and software is produced with no close control over its security features and, moreover, computers are vulnerable to selfpropagating “virus” or other infections.

**7. Insider Attacks:**

Within the bounds of a given, commercially- procured system, there can be little defence - other than personnel security - against insider attack at or below this insider's level of access rights. On the other hand, interface controllers can offer significant protection against insider attack spreading beyond the borders of this system segment, and in some system architectures, they could also play a role in preventing an insider going beyond his authorised user group, function or security level.

## III. CONCLUSIONS

The growing dependence of industry and society on IT, and the growing threat of cyber crime, require that serious effort be devoted to IT security.The risks of cyber crime are very real and too ominous to be ignored. Every franchisor and licensor, indeed every business owner, has to face up to their vulnerability and do somethingabout it.The cyber crime as a whole refers to Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)".

## REFERENCES

[1] Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

[2] Susan W. Brenner, Cybercrime: Criminal Threats from Cyberspace, ABC-CLIO, 2010. Also includes the statistics from the net search and many other sites.

[3] Benjamin, R. (1990) Security Considerations in Communications Systems andNetworks, Proc. IEE, 137, Pt 1, 2.

[4] G.Arunachalam, K.Ramya, M.Vimala, M.Shanmugapriya, C.Krishnaveni,”Future Principle of TCP High-Speed Network “International Journal for Research & Development in Technology.

[5] K.Ramya and K.Pavithradevi “Effective Wireless Communication,” International Journal of Advanced Research, volume4(12),pp. 1559-1562 Dec 2016.

[6] Blain, L. and Deswarte, Y. (1990) Intrusion-tolerant security servers for Delta-4. In Proceedings of the ESPRIT'90 Conference, Brussels, Kluver Academic Publishers, pp. 355-370.

[7] Cheswick, W. and Bellovin, S. (1994) Firewalls and Internet Security: Repelling the Wily Hacker, Addison-Wesley, Reading, Mass.

[8] Deswarte, Y., Blain, L. and Fabre, J.-C. (1991) Intrusion Tolerance in Distributed Computing Systems. In Proc. 1991 Symp. on Research in Security and Privacy,Oakland, California, IEEE Computer Society Press, pp. 110-121.