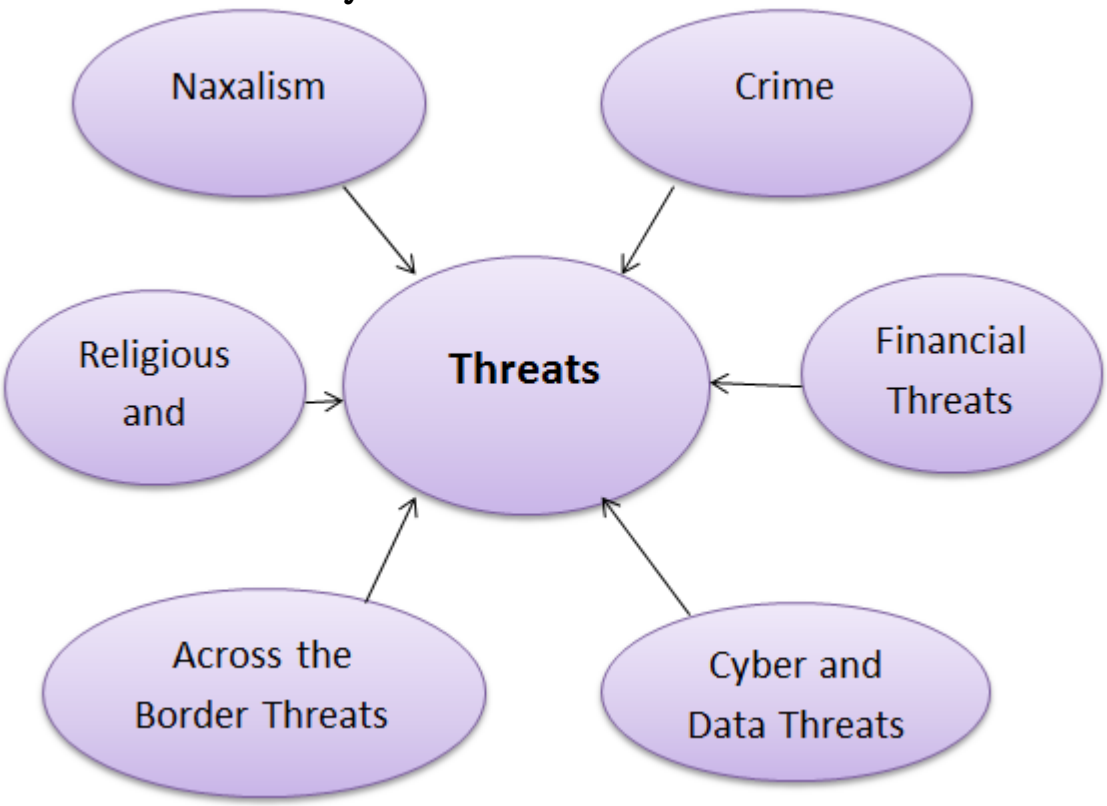
UNIT 32 – UPSC - Challenges to Internal Security through Communication Networks

In cutthroat competition and rapidly changing technical environment, there is more economic uncertainty and complexities that afflicting the nation. Currently, security has imperative role to protect data and relevant and secret information from growing internet attacks on computing and communication systems with the support of continuous innovative solutions. It is therefore necessary to provide a means for researchers in this domain to encourage quality publications of their work. Security is described by experts as ensuring protected communication among computing/communication systems and user applications across public and private networks, is essential for guaranteeing confidentiality, privacy and data/information protection.

It has been universally observed that there are large number of recent threats and incidents reported to CERT therefore security in networks and distributed systems has gradually become a global challenge. To deal with such debilitating issue, it is critical to design and develop security solutions from different viewpoints including that of end-to-end. Other than these threats, the growing need of wireless, ad-hoc and sensor networks also create hazards of a new dimension. Another significant technical feature that create risk is the communication speed in networks versus complex and time consuming cryptography/security mechanisms and protocols.

India's internal security threats



Earlier it was not major challenge in India with respect of an internal security viewpoint. The new types of the threats that India undergo need very active security governance. Internal security in India is considered as the national subjects that covers many multifaceted individual subjects, across the centre, state and local jurisdictions, defined by the borders of the homeland yet challenged by exceptional local conflicts of the country's huge and diverse landscape. In present condition, internal security is dealt by numerous executive bodies with intricate functional and reporting relationships. Law and order is a state subject and the state police are accountable for maintaining the internal security. The Ministry of Home Affairs has been charged for internal security, management of paramilitary forces, border management, centre-state relations, administration of union territories and disaster management.

For maintaining internal security, effectual communication networks has pivotal role. Communication networks described as an interconnection of communicating through electronic gadgets like computers, laptops, mobiles, telephones which enables executives to transmit important and secret information of all other sectors including voice, data, video, and internet networks. Communication network should not be understood with the computer networks such as LAN, WAN because they are just one type of the Communication networks. Various communication networks are the mainstay of much of the critical infrastructure in many sectors today such as civil aviation, shipping, railways, power, nuclear, oil and gas, finance, banking, IT, law enforcement, intelligence agencies, space, defence, and government networks. As such, communications systems serve in other key internal and external security and emergency readiness. Furthermore, the communication networks are mainly dependent on each other in complicated way. If there is a failure of one communication network, it can affect badly in other sectors.

In the Communication Networks, there may be serious security attacks such as data theft, fraud, and denial of service attacks, hacking, and cyber warfare, terrorist and antinational activities. A

cyber-attack which can control the infrastructure may harm the system and disrupt the communication network. The attacks can be through viruses, malware, Trojans, hacking, network scanning, probing, and phishing. Furthermore, the Social network attacks can be one of the major sources of attacks in future because it is used by huge number of users and they post their personal information on sites through these networks.

It has been explained in technical reports that Network security is a major part of a network that needs to be maintained because information is being passed between computers and is very susceptible to attack. Since last decade, experts that manage network security have seen a huge number of hackers and criminals that created malicious threats which disrupted the communication around the globe (ITSecurity, 2007)

There numerous network threats that can have adverse impact on communication network:

1. Viruses and Worms
2. Trojan Horses
3. SPAM
4. Phishing
5. Packet Sniffers
6. Maliciously Coded Websites
7. Password Attacks
8. Hardware Loss and Residual Data Fragments
9. Shared Computers
10. Zombie Computers and Botnets.

A Virus is a "program or piece of code that is loaded onto computer without user knowledge and runs against his wishes. Viruses can hugely damage to computers. With respect to a network, if a virus is downloaded then all the computers in the network would be affected because the virus would make copies of itself and spread itself across networks. A worm is similar to a virus but a worm can run itself whereas a virus needs a host program to run. To protect from worm, it is necessary to install a security suite, such as Kaspersky Total Protection, that protects the computer against threats such as viruses and worms.

A Trojan Horse is "a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on user's hard disk. In a network if a Trojan Horse is installed on a computer and interferes with the file allocation table it could cause enormous damage to all computers of that network. In order to get protected, security professionals must have Security suites, such as Norton Internet Security that will prevent from downloading Trojan Horses.

SPAM is "flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise pick to receive it. SPAM filters are an effective way to stop SPAM, these filters come with most of the e-mail providers online. Also you can buy a variety of SPAM filters that work efficiently.

Phishing is also a security threat that misuses user's valuable information. Phishing is explained as an e-mail fraud method in which the perpetrator sends out legitimate-looking emails in an attempt to gather personal and financial information from recipients. Phishing is one of the worst

security threats over a network because a lot of people that use computers linked up to a network are amateurs and would be very susceptible to giving out information that could cause situations such as theft of money or identity theft. It is recommended to use Phishing filters to filter out this unwanted mail and to prevent threat.

A packet sniffer is a device or program that allows snooping on traffic travelling between networked computers. The packet sniffer will capture data that is addressed to other machines, saving it for later analysis. In a network a packet sniffer can filter out personal information and this can lead to areas such as identity theft, so this is a major security threat to a network. When strong encryption is used, all packets are unreadable to any but not to the destination address. This makes packet sniffers ineffective. So to protect from it, it is important to obtain strong encryption.

Some websites across the net contain code that is malicious.

Malicious code is "Programming code that is capable of causing harm to availability, integrity of code or data, or confidentiality in a computer system. AVG report that "300,000 infected sites appear per day (PC Advisor, 2009). To protect the system, it is advised to use a security suite, such as AVG, can detect infected sites and try to prevent the user from entering the site.

Password attacks are attacks by hackers that are able to regulate passwords or find passwords to different protected electronic areas. Many systems on a network are password protected and hence it would be easy for a hacker to hack into the systems and steal data. This may be the easiest way to get private information because people are able to get software online that obtains the password. Currently, there is no software that prevents password attacks.

Hardware loss and residual data fragments are also major security threats for companies and governments. Suppose, if a number of laptops get stolen from a bank that have client details on them, this would enable the robber's to get personal information from clients and maybe steal the clients identities. This is an increasing concern and as of present the only solution is to keep data and hardware under strict surveillance.

Shared computers also pose threat. Shared computers involve sharing a computer with one or more people. There are number of suggestions when using shared computers that include:

- Do not check the "Remember my ID on this computer" box.
- Never leave a computer unattended while signed-in.
- Always sign out completely.
- Clear the browsers cache.
- Keep an eye out for "shoulder surfers".
- Avoid confidential transactions.
- Be wary of spyware.
- Never save passwords.
- Change password often

A zombie computer or "drone" is a computer that has been secretly compromised by hacking tools which allow a third party to control the computer and its resources remotely. A hacker could hack into a computer and control the computer and obtain data. The solution for this type of threat is that Antivirus software can help prevent zombie computers.

A botnet is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the internet. This is a major security threat on a network because the network, unknown to anyone, could be acting as a hub that forwards malicious files to other computers. To protect from this threat, Network Intrusion Prevention (NIP) systems must be installed.

Network Security is a wide arena and it is complicated task of Network Security manager. There are still threats such as password attacks that have no deterrence.

To summarize, internal security organisations in India and around the globe has to undergo unparalleled challenges such as the need to tackle crime, address the increasing challenge of Transnational criminal networks and the ongoing threat of international and domestic terrorism, cybercrime, money laundering, narcoterrorism and human trafficking. Since many years, India's internal security landscape has seen theatrical changes. The Ministry of Home Affairs has already taken effective measures to strengthen the national security apparatus and communication and information management systems. All internal security activities should be underpinned by vigorous information management to safeguard the effective use of resources and data assets. Nevertheless, security agencies face challenges at every stage of information management such as creation, collection, storage, and communication. To deal with such as challenges, security agencies must develop robust and automated information management and install various protective measures to protect from cyber threats.