International Journal of Engineering Technology and Applied Science
(ISSN: 2395 3853), Vol. 2 Issue 1 January 2016

Tempest and Echelon

Prof. Abhinav V. Deshpande

Assistant Professor, Department of Electronics & Telecommunication Engineering
Prof. Ram Meghe Institute of Technology & Research, Badnera, Amravati-444701, Maharashtra, India
avd.a.deshpande@gmail.com

ABSTRACT:- Tempest and Echelon are the method of spying in a sophisticated manner; both are developed by National Security Agency (NSA) for monitoring the people. These technologies are originally developed for pure military espionage, but hackers use them now for spying into other people activities. Tempest is the technology which reproduces what you are seeing in your monitor, what you are typing in your keyboard from a couple of kilometres away. It traces all electromagnetic radiation from the victim's monitor, keyboard, even PC memory and hard disk, and then it reproduces the signals. By using this technology it is possible to intrude only listening into a person's computer from a couple of kilometres away, even it is a computer which is not networked and enables the intruder to hack without any connection to the victim's computer. ECHELON is the spying on a large network by sniffing through the words. It is the ongoing secret project of NSA and its counterparts in UK, Canada, Australia and New Zealand. It can intercept as many as 2 million communications per hour through phone calls, faxes, emails, downloads, microwave, cellular, satellite communication etc. As quoted above it is developed for military purposes but it is now used for spying an organization, business and individuals etc.

KEYWORDS:- Tempest, Echelon, Monitor, PC, Communication, Interception, Emanations

1. Introduction

The notion of spying is a very sensitive topic after the September 11 attack of terrorists in New York. In the Novel 1984, George Orwell foretold a future where individuals had no expectation of privacy because the state monopolized the technology of spying. Now the National Security Agency (NSA) of USA developed a secret project to spy on people for keep tracking their messages to make technology enabled interception to find out the terrorist activities across the globe, named as ECHELON, leaving the technology ahead of any traditional method of interception. Its allies are tracing every single transmission even a single of keyboard. The allies of USA in this project are UK, Australia, New Zealand and Canada, ECHLON is developed with the highest computing power of computers connected through satellites all over the world. In this project, the NSA has left the wonderful method of Tempest and Carnivores behind.

ECHELON is the technology for sniffing through the messages sent over a network or any transmission media; even it is a wireless message. Tempest is the technology for intercepting the electromagnetic waves over the air. It simply sniffs through the electromagnetic waves propagated from any devices, even it is from the monitor of a computer screen. Tempest can capture the signals through the walls of computer screens and keystrokes of a keyboard even if the computer is not connected to a network. Thus, the traditional way of hacking has a little advantage in spying. For the common people, it is so hard to believe that their monitor can be reproduced from anywhere in one kilometre range without any transmission media in between the equipment and their computer. So we have to believe that the technology has enabled us to reproduce anything from the monitor of a computer to the hard disks including the memory (RAM) of a distant computer without any physical or visual contact. It is done with the help of electromagnetic waves which are propagated from that device. The main theory behind the Tempest (Transient Electromagnetic Pulse Emanation Standard) is that any electronic or electrical devices emit electromagnetic radiations of specific key when it is operated. For example, the picture tube of a computer monitor emits radiations when it is scanned up on a vertical or horizontal range beyond the screen. It will not cause any harm to a human and it is very small. But it has a specific frequency range. You can reproduce that electromagnetic wave by tracing with powerful equipment's and the powerful filtering methods to correct the errors while transmission from the equipment.

For the project named as Echelon, the NSA is using supercomputer for sniffing through the packets and messages through any transmission media. They are using the advantage of Distributed Computing for this purpose. Every packet is sniffed for spying for USA's NSA for security reasons. Interception of communication is a method for spying

commonly employed by intelligence services to spy for the secret services to provide the security to the government and the people so that they can use any method to ensure the security of the people including spying. It depends on the target we are aiming. To capture the terrorists before they can make any harm to the people, we must keep the technology ahead. We, the engineers are behind that project of NSA and so we have to become aware of that technology for enabling our country India also in this field. Because it is used mainly by the security agencies and spies all over the world even though there is a lack of equipment for this purpose. The equipments for the spying of Tempest are available in the USA and are prohibited for exporting from thee. There may be some smuggled equipments here. But we have to develop the systems for our military and Intelligence Agencies for ensuring the best security for our people.

While considering about the limitations of the surveillance systems, the issues depend in particular, upon the worldwide interception of satellite communication, although in the areas which are characterized by a high volume of communication only a very small proportion of those communications are transmitted by a satellite, whereas this means that the majority of communications cannot be intercepted by earth stations, but only by tapping cables and intercepting radio signals, something which is possible only to a limited extent, whereas the number of personnel required for the final analysis of intercepted communications imposes further restrictions. Therefore the USA and the UK states have access only to a very limited proportion of cable and radio communication and can analyse an even more limited proportion of those communications and whereas further, however extensive the resources and capabilities for the interception of communication may be, the extremely high volume of traffic makes exhaustive, detailed monitoring of all communication is possible in practice.

2. Tempest and Echelon

The interception of the communication is a method of spying commonly employed by the intelligence services, whereas there can now be no doubt that the purpose of the system is to intercept, at the very least, private and commercial communication and not the military communication, although the analysis which is carried out in the report has revealed that the technical capabilities of the system are probably not as extensive as some of the sections of the media had assumed.

2.1. The Need for an Interception System

The interception of the messages is the major work for the intelligence agencies all over the world, to keep track of the spies and the terrorists for preserving the security of the country from the leaking of sensitive documents and the terrorist attacks. By the work of intelligence agencies the government is ensuring the security of the state. For that we have to enable our intelligence agencies with modern technologies like USA. For that purpose, we must set up an interception system. While developing this strategy, we have to consider about the privacy of the common people and industrial organization. The targets for the ECHELON system which are developed by the NSA are apart from directing their ears towards the terrorists and the rogue states. The ECHELON is also being used for the purposes which are well outside its original mission. The other ECHELON targets the aero political spying and the industrial espionage. The existence and the expansion of the ECHELON is a foreboding omen regarding the future of our constitutional liberties. If a government agency can willingly violate the most basic components of the bill of rights without so much as congressional oversight and approval, we have reverted from a republican form of a government to tyranny. While considering about the political spying, we have to consider many legal issues. It consists of spying the other parties and the messages sent by them. Since the close of World War 2, the US Intelligence Agencies have developed a consistent record of trampling the rights and liberties of American people. Even after the investigations which are done in the domestic and political surveillance activities of the agencies that followed in the wake of the Watergate fiasco, the NSA continues to target the political activity of “unpopular” political groups and our duly elected representatives. While considering about the industrial espionage we have to discuss what we have to redefine the notion of National Security in order to include the economic, commercial and the corporate concerns. Many of the major companies which helped the NSA in order to develop the ECHELON system in order to tackle the mammoth task for setting up the largest computing power throughout the world. ECHELON is actually a vast network of electronic spy stations which are located around the world and maintained by five companies: the USA, England, Canada, Australia and New Zealand. These countries, bound together in a still secret agreement called as the UKUSA, spy on each other’s citizens by intercepting and gathering the electronic signals of almost every telephone call, fax transmission and email message which are transmitted around the world daily. These signals are fed through the massive supercomputers of the NSA to look for certain

keywords which are called as the ECHELON "dictionaries". For these above reasons, our country India must be enabled in order to cope with the new interception system. For that purpose, the engineers must perform the work otherwise our country will also become vulnerable to any attacks coming from the other states.

3. Inside a Tempest

Tempest is a short name referring to the investigations and the studies of compromising emanations (CE). The compromising emanations are defined as unintentional intelligence bearing signals which if intercepted and analyzed, disclose the national security information which is transmitted, received handled or otherwise processed by any information processing equipment. The compromising emanations consist of electrical or acoustic energy which is unintentionally emitted by any of the great number of sources within the equipments or systems which process the national security information. This energy may relate to the original message or information which is being processed in such a way that it can lead to the recovery of the plaintext. The laboratory and field tests have established that such CE can be propagated through space and along nearby conductors. The interception or the propagation ranges and the analysis of such emanations are affected by a variety of factors. For example, the functional design of the information processing equipment, system or the equipment installation and the environmental conditions which are related to the physical security and the ambient noise compromising emanations rather than radiation is used because the compromising signals can and do exist in different forms such as magnetic and or electric field radiations, line conduction, signal and power or acoustic emissions.

More specifically the emanations occur as:

1) The electromagnetic fields which are set free by the elements of the plaintext processing equipment or its associated conductors.
2) The text related signals are coupled to cipher, power, signal, control or the other black lines through:

    a) The common circuit elements such as the ground and power supplies or
    b) The Inductive and the Capacitive Coupling

3) The propagation of the sound waves from mechanical or electromechanical devices.
4) The Tempest problem is not the one which is confined to the cryptographic devices but it is a system problem and is of concern for all the equipment which process the plaintext national security data.

3.1. Sources of Tempest Signals

1) **Functional Sources:** The functional sources are those which are designed for the specific purpose of generating the electromagnetic energy. The examples are the switching transistors, oscillators, signal generators, synchronizers, line drivers and line relays.

2) **Incidental Sources:** The incidental sources are those which are not designed for the specific purpose of generating the electromagnetic energy. The examples are the electromechanical switches and brush-type motors.

3.1.1. Types of Tempest Signals

In practice, the more common types of CE (compromising emanations) are attenuated include the following:

1) RED Base band signals
2) Spurious carriers modulated by RED base band signals, and
3) Impulsive Emanations

3.1.1.1. RED Base Band Signals

The most easily recognized CE is the RED base band signal which is attenuated but otherwise in the unaltered form, since it is essentially identical to the RED base band signals itself. This emanation can be introduced into the electrical conductors which are connected to the circuits which are within EUT which have the impedance or a power source in common with the circuit processing RED base band signals. It can be introduced into an escape medium by the capacitive or inductive coupling and especially by the radiation with RED base band signals of higher frequencies or the data rates.

3.1.1.2. Modulated Spurious Carriers

This type of CE is generated as the modulation of a carrier by the RED data. The carrier may be a parasitic oscillation which is generated in the equipment, i.e., the chopper frequency of a power supply etc. The carrier is usually an amplitude or angle modulated by the basic RED data signal or a signal which is related to the basic RED data signal which is then radiated into the space or coupled into EUT external conductors.

3.1.1.3. Impulsive Emanations

The impulsive emanations are quite common in the equipment under the test processing the digital signal and are caused by the very fast mark-to-mark space and space-to-mark transitions of digital signals. The impulsive emanations can be radiated into the space or coupled into the equipment which is under test of the external conductors.

3.2. The technology behind the Tempest

The Tempest uses the electromagnetic waves which are propagated from the electronic devices intentionally or non-intentionally. For receiving the texts or the data at the other end we have to screw up to a specific frequency range and just listen or replicate the data at the other end. Tempest is the technology which can be reproduced what one can see in a monitor, what one can type in his keyboard from a couple of kilometres away. It traces all the electromagnetic radiation from the victim's monitor, keyboard and even a PC memory and the hard disk and then it reproduces the signals. By using this technology, it is possible to intrude in to a person's computer which is not networked and enables the intruder to hack without any connection to the victim's computer. The techniques that enable the software on a computer to control the electromagnetic radiation it transmits. This can be used for both attack and defence. In order to attack a system, the malicious code can encode the stolen information in the machine's RF emissions and optimize them for some combination of the reception stage, the receiver cost and covertness. In order to defend a system, a trusted screen driver can display the sensitive information by using the fonts which can minimize the energy which is emanated out by these emissions. When snooping in to a computer's VDU, similar periodic averaging and cross correlation techniques can be used if the signal is periodic or if its structure is understood. The output from the video display unit is in the form of a frame and it buffers the content periodically to a monitor and therefore a target, especially where the video signal is amplified to several hundred volts. The knowledge of the fonts which are used with the video display units and printers allows a maximum likelihood character recognition technique in order to give a better signal to noise ratio for the whole characters than is possible for the individual pixels.

4. Inside an Echelon

ECHELON stands for NSA's (National Security Agency of America) secret Global Surveillance System which is developed for the purpose of intercepting the messages all over the world. As said in the Media's NSA is no such agency but it is not the truth. This massive surveillance system apparently operates without the oversight of either congress or the courts. Shockingly, the NSA has failed to adequately disclose to the congress and the public the legal guidelines for the project. Without those legal guidelines and by using Echelon in order to spy on the Americans in the violation of the federal law. In April 2000, the house intelligence committee held a hearing in order to deal with the credible reports that suggest the Echelon is capturing the satellite, microwave, cellular and the fiber-optic communication worldwide. The house intelligence committee also intended the hearing in order to help in ensuring that the ECHELON does not circumvent any of the requirement in the federal law that the government obtains a warrant from a court before it eavesdrop on a conversation to, from or within the United States.

4.1. Espionage

The governments have a need for the systematic collection and the evaluation of information about certain situations in other states. This serves as a basis for the decisions concerning the armed forces, foreign policy and so on. They therefore maintain the foreign intelligence services, part of whose task is to systematically assess the information which is available from the public sources. The rapporteur has been informed that on an average this account for at least 80% of the work of the intelligence services. However, particularly significant information in the fields concerned is kept secret from the governments of businesses and is therefore not publicly accessible. Anyone who does not wish to obtain it has to steal it. Espionage is simply the organized theft of information.

4.1.1. Espionage targets

The classic targets of espionage are the military secrets and the other government secrets or the information concerning the stability of or posing as a danger to the government. These may for example comprise new weapon systems, military strategies or the information about the stationing of the troops. No less important is the information about the forthcoming decisions in the fields of foreign policy, monetary decisions or inside information about the tensions within a government. In addition, there is also an interest in economically significant information. This may include not only the information about the sectors of the economy but also the details of new technologies or the foreign transactions.

4.1.2. Espionage Methods

Espionage involves gaining access to the information which the holder would rather protect from being accessed by the outsiders. This means that the protection needs to be overcome and penetrated. This is the case with both the political and industrial espionage. Thus the same problem arises with the espionage in both the fields and the same techniques are accordingly used in both of them. Logically speaking, there is no difference; only the level of protection is generally lower in the economic sphere, which sometimes makes it easier in order to carry out the industrial espionage. In particular, the businessman tends to be less aware of the risks when using the imperceptible communication media than does the state when employing them in the fields where the security is a concern.

4.2. Processing of Electromagnetic Signals

The form of espionage by technical means with which the public are most familiar is that which uses the satellite photography. In addition, however, the electromagnetic signals of any kind are intercepted and analyzed. In the military field, certain electromagnetic signals, e.g., those emanating from the radar stations may provide valuable information about the organization of the enemy air defences. In addition, the electromagnetic radiations which could reveal the details of the position of troops, aircrafts, ships or submarines is a valuable source of information for an intelligence service. By monitoring other states, the spy satellites which take the photographs and perform the processes of recording and decoding the signals coming from such satellites can also prove to be beneficial. The signals are recorded by ground stations from low orbit satellites or from the quasi geostationary SIGINT satellites. This aspect of intelligence operations by using the electromagnetic waves means that by consuming a large part of services. Interception capacity, however, is not the only use made of the technology.

4.2.1. Processing of intercepted communication

The foreign intelligence services of many states intercept the military and diplomatic communications of other states. Many of these services also monitor the civil communication of the other states if they have access to them. In some states, the services are also authorized in order to monitor the incoming or outgoing communication in their own country. In the democracies, intelligence services, monitoring of the communication of the country's own citizens is subjected to certain triggering conditions and controls. However, the domestic law in general not only protects the citizens within the territory of their own country and other residents of the country concerned. The interception on the spot covers the following:

1) On the spot, any form of communication can be intercepted if the eavesdropper is prepared to break the law and the target does not take the protective measures.

2) The conversation in the room can be intercepted by means of planted microphones (bugs) or laser equipment which picks up vibrations in the window panes.

3) The screens emit radiations which can be picked up at a distance of up to 30 meters, revealing the information on the screen.

4) Telephone, fax and email messages can be intercepted if the eavesdropper taps into a cable by leaving the relevant building.

5) Although the infrastructure which is required is costly and complex communication from a mobile phone can be intercepted if the interception station is situated in the same radio cell (the diameter is 300 meters in the urban areas and 30 km in the countryside).

6) The closed circuit communication can be intercepted within the USW radio range.

4.2.2. The Worldwide Interception System

Nowadays various media are available for all forms of intercontinental communication (voice, fax and data). The scope for a worldwide interception system is restricted by two factors:

1) Restricted access to the communication medium.

2) The need to filter out the relevant communication from a huge mass of communication which is taking place at the same time.

4.3. Access to Communication Media

4.3.1. Cable Communication

All forms of communication (voice, fax, email and data) are transmitted by cable. The access to the cable is a prerequisite for the interception of communication of this kind. Access is certainly

possible if the terminal of a cable connection is situated on the territory of a state which allows the interception. In technical terms, therefore, within an individual state all the communication which is carried by the cable can be intercepted, provided this is permissible under the law. However, the foreign intelligence services generally have no legal access to cables which are situated on the territory of other states. At the best, they can gain illegal access to a specific cable, although the risk of detection is high. From the telegraph age onwards, the intercontinental cable connections have been achieved by means of underwater cables. Access to these cables is always possible at those points where they emerge from the water. The electric cables may also be tapped between the terminals of a connection by means of induction (i.e. electromagnetically by attaching a coil to the cable), without creating a direct conductive connection. The underwater electric cables can also be tapped in this way from submarines albeit at a very high cost. In the case of older generation fiber optic cables which are used today, inductive tapping is only possible at the regenerators. These regenerators transform the optical signal into an electrical signal, strengthen it and then transform it back into an optical signal. However, this raises the issue of how the enormous volumes of data carried on a cable of this kind can be transmitted from the point of interception to the point of evaluation without the layering of a separate fiber optic cable. The conditions apply to the communication which is transmitted over the internet via the cable. The situation can be summarized as follows:

1) The internet communication is carried out by using the data packets and different packets which are addressed to the same recipient may take different routes through the network.

2) In the internet communication, the routes which are followed by the individual data packets are completely unpredictable and arbitrary. At that time, the most important international connection was the “science backbone” between Europe and America.

3) The communication of the internet and the establishment of internet providers also resulted in the commercialization of the network. The internet providers operated or rented their own networks. They therefore made increasing efforts in order to keep the communication within their own network in order to avoid paying the user fees to other operators. Today, the route taken through the network by a data packet is therefore not solely determined by the capacity which is available on the network but also hinges on the cost considerations.

4.3.2. Radio Communication

The interceptibility of radio communication depends on the range of the electromagnetic waves employed. If the radio waves run along the surface of the earth their range is restricted and is determined by the topography of the earth’s surface, the degree to which it is built up and the amount of vegetation. If the radio waves are transmitted towards space two points a substantial distance apart can be linked by means of the reaction of the sky wave from the layers of the ionosphere. Multiple reactions substantially increase the range. The global communication interception system can only intercept the short wave radio transmissions. In the case of all other types of radio transmission, the interception station must be situated within a 100 km radius (e.g., on a ship, in an embassy. The practical implication for the interception with the terrestrial listening station is that they can intercept only a very limited proportion of radio communication.

4.4. Communication Transmitted by Geostationary Telecommunication Satellites

If a microwave radio link is set up by transmitting to a telecommunication satellite in a high, geostationary orbit and the satellite receives the microwave signals, converts them and transmits them back to the earth, large distances can be covered without the use of cables. The range of such a link is essentially restricted only by the fact that the satellite can receive and transmit only in a straight line. For that reason, several satellites are employed in order to provide a worldwide coverage which operates by listening the stations in the relevant regions of the earth in order to intercept all the telephone, fax and the data traffic which is transmitted via such satellites. The Echelon system which is developed by NSA and its allies uses this type of filtering of the messages by use of directories and keywords. Thus, the system filters the messages by using the modern technique for searching with the use of sophisticated searching algorithms. In this method, the NSA uses the sophisticated speech recognition software and the OCR software for searching or sniffing through the packets. The searching through the packets is done by the specific keyword and directories. These keywords and directories are the power of an Echelon system. It is told that an Echelon system can intercept about billions of messages every hour. This makes the Echelon system as the largest spying network of the world by using the largest computing power that the human kind ever

experienced. The power of the Echelon system is the dictionaries which are containing the keywords.

4.4.1. Keywords

When sniffing through the packets and sending the information to the destination of agencies , the computers which constitute a part of the Echelon system use some "Sensitive Words" in order to find out the messages which carry the sensitive information. These words are known as the Keywords. The computers automatically search through millions of intercepted messages for the ones which contain the pre-programmed keywords and then ship the selected messages off to the computers of the requesting agency. By processing millions of messages every hour, the ECHELON systems churn away 24 hours a day, 7 days a week looking for the targeted keyword series, phone and fax numbers and the specified voice prints. It is important to note that very few of these messages and phone calls are actually transcribed and recorded by the system. The vast majority are filtered out after they are read or listened to by these systems. Only those messages that produce the keyword "hits" are tagged for future analysis. Again, it is not just the ability to collect the electronic signals that gives ECHELON its power, it is the tools and the technology that are able to whittle down the messages to only those that are important to the intelligence agencies. The ECHELON system compares the intercepted messages with the keywords and when a "Hit" occurs then the system will forward the messages to the corresponding agencies.

4.4.2. The ECHELON Dictionaries

The extraordinary ability of ECHELON in order to intercept most of the communication traffic in the world is breath taking in terms of its scope and yet the power of ECHELON resides in its ability to decrypt, filter, examine and codify these messages into selective categories for further analysis by intelligence agents from various UK and USA agencies. As the electronic signals are brought into the station, they are fed through the computer systems such as Menwith Hill's SILKWORTH where voice recognition, optical character recognition (OCR) and the data information engines get to work on the messages. The database containing the keywords may be huge, this huge database is called as the Dictionaries. Each station maintains a list of keywords (the "Dictionary") designated by each of the participating intelligence agencies. A Dictionary manager from each of the respective agencies is responsible for adding, deleting or changing the keyword search criteria for their dictionaries at each of the stations. Each of these station dictionaries is given codeword, such as COWBOY for the Yakima facility and FLINTLOCK for the Waihopai facility. These code words play a crucial identification role for the analysts who eventually look at the intercepted messages. By the rise of post-modern warfare terrorism which gave the establishment of all the justification it needed in order to develop even greater ability to spy on our enemies. The satellites that fly thousands of miles overhead and yet can spy out the minutest details on the ground, the secret submarines that troll the ocean floors that are able to tap into undersea communication cables.

4.5. The Problem of ECHELON

Even the technology made us to access the sophisticated spying methods and prevention of terrorist activities up to certain extent. The ECHELON system has its drawbacks:

1) The ECHELON system will not provide any privacy for our own people in home and abroad. Everything is monitored by the Big-Brother. It will not provide any security of the data of the response firms. It will result in the complete destruction of the industries and it will lead to the 19th century colonialism. It will cause a threat to our modern culture.

2) Every military secret is public to NSA and its allies, even though if we are hiding that from their eyes. They will hear and see with sixth-sense eyes the computers. I will lead to the mass destruction of human kind. Even a single war can cause the complete destruction of the mankind.

3) As stated above, the ECHELON systems can be developed in order to protect us from the terrorist attacks, but we have to ensure that these systems are protected from intrusion and weather it occurs as the result will be hazardous. If the terrorists get the sensitive information about the military secrets and the intelligence secrets, the terrorists can cause a world war.

4.6. Cryptography as means of self-protection

Every time a message is transmitted, there is a risk of it falling into the hands of unauthorized people. In order to prevent outsiders accessing its content in such cases, the message must be made a secret so that it is impossible for them to read or intercept, i.e. encrypt the message. The invention of the electrical and electronic communication media such as the telephone, telegraph, radio, telex, fax

and the Internet has greatly simplified the transmission of intelligence communication and made them immeasurably quicker. The downside is that there is no technical protection against the interception or recording so that anyone with the right equipment could read the communication if he could gain access to the means of communication. If it is done professionally, the interception leaves a little or no trace. This imparts a new significance to encryption. It is the banking sector which first regularly used the encryption to protect the communication in the new area of electronic money transfers. The growing internationalism of the economy led to the communication in this field too for being at least partly protected by the cryptography. The widespread introduction of completely unprotected communication through the internet also increased the need for private individuals to protect their messages from interception. The use of computers made it possible to generate coded texts by using powerful encryption algorithms which offer practically no starting points for code breakers. The process of decryption now entails by trying all the possible keys. The longer the key, the more likely it is that this attempt will be thwarted, even by using very powerful computers by the time it would take. There are therefore usable methods which may be regarded as a secure at the present state of technology.

5. Conclusion and Future Scope

The interception of communication is the main function done by the Intelligence agencies all over the world. The intelligence agencies are searching for the sophisticated methods for surveillance and spying from its own people and from its enemies. Here the scientists in the NSA developed the modern techniques for finding the interception of the messages and they developed a network which is known as the Echelon system. It made them to leap ahead of the hackers in one step. The main topics which are discussed in this research paper are the Tempest and Echelon. Tempest is the technology for spying from electronic equipment's without any physical contact. It is the wonderful technology which people ever experienced. It enables us to replicate the data on electronic equipment from a couple of kilometres away. We can replicate the computer monitor and hard disk (or even the memory) of a computer system by this way. Echelon is the vast network which is formed by NSA and its allies all over the world to intercept the messages sent through any transmission media. It plays a major role in the intelligence related work of the NSA and its allies. It uses the search algorithms and sophisticated software like speech recognition system or OCR software. Even though we have discussed the advantages and disadvantages of the Echelon and Tempest there are some major disadvantages of these systems.

These systems are GOD-LIKE and nothing can be hidden from the Echelon system. But the Echelon system will not provide any secrecy for the common people. It will only preserve the state policies. This will cause the leaking of the sensitive data of the industries and it will cause harm to that company and again the Tempest equipment's are available in the USA and is prohibited of exporting from there, and thus if some terrorists got these Tempest equipment's then it will cause harm to our industries and society. But many of the corporate firms are protecting their companies from the Tempest attacks by use of software and equipments to prevent the Tempest attacks.

Now, discussing about the future scope of Tempest and Echelon, we can say that these can be used to empower our intelligence agencies to do their job better than before. Unfortunately, our India does not have a Tempest equipment developed yet. But we have to take care of the foreign intelligence agencies stealing our military data and the diplomatic data. We have to take the counter measures to protect our secret data from them. And we are not a part of Echelon network developed by NSA, so we have to develop one such for empowering our intelligence agencies and military agencies.

6. Acknowledgements

This research work was undertaken as a part of improvement and development of current technology which is used to monitor the activities of people particularly for the Defence and Military purposes. The concept of Tempest and Echelon was developed by National Security Agency (NSA) in the USA for preventing the intrusion by some third party in their country so that the secret data which is available in the communication devices of the country cannot be fallen into the intruder's hands. We are thankful to the Director and Chief of National Security Agency (NSA) for their great contribution in the field of Communication Engineering for implementing such a wonderful technique that can be useful for preventing the intrusion of an enemy in their country and successful prevention of fraudulently altering or manipulating the secret data which is useful for communication. The research project was undertaken at our institute to give a brief introduction to our students about the current techniques which are available in the field of Communication Engineering in order to prevent the manipulation or altering of secret data useful for defence and military purposes. I am thankful to our HOD, Department of Electronics and Telecommunication Engineering, Prof. Ram Meghe Institute of Technology & Research, Badnera,

Amravati-444701 and all the staff members and college authorities of our institute.

References

[1]. NSA Tempest Documents
[2]. Approved for release by NSA on 09-27-2007, FOIA Case #51633
[3]. http://jaisantonyk.wordpress.com/discuss/tempest-and-echelon
[4]. http://www.eskimo.com/~joelm/tempest.html
[5]. http://actionamerica.org/echelon/echelonwhat.html
[6]. http://cryptome.org/echelon2-arch.htm
[7]. http://actionamerica.org/echelon/echelonwork.html
[8]. http://www.akdart.com/carniv.html