ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 6, June 2014

Significances and Issues of Network Security

Dr. B V Ramana Murthy[1], Prof. Vuppu Padmakar[2], Ms. A. Vasavi[3]

Department of CSE Jyotishmathi College of Technology and Science, Shamirpet, Hyderabad, India[1,3]

Department of CSE, Chilkur Balaji Institute of Technology, Aziz nagar, Hyderabad, India[2]

Abstract: This is the age of universal electronic connectivity, where the activities like hacking, viruses, electronic fraud are very common. Unless security measures are taken, a network conversation or a distributed application can be compromised easily. Information security has been affected by two major developments over the last several decades. First one is introduction of computers into organizations and the second one being introduction of distributed systems and the use of networks and communication facilities for carrying data between users & computers. These two developments lead to ‘computer security’ and ‘network security’, where the computer security deals with collection of tools designed to protect data and to thwart hackers. Network security measures are needed to protect data during transmission. But keep in mind that, it is the information and our ability to access that information that we are really trying to protect and not the computers and networks.

Keywords: Security, Authentication, VPN, Firewalls, Antivirus

I. INTRODUCTION

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions.

Network security is becoming more and more important as people spend more and more time connected. Compromising network security is often much easier than compromising physical or local security, and is much more common.

- Increasing online transactions
- Personal and sensitive information shared over network
- Protect Network and related resources from unauthorized access
- Monitor and measure its activeness

1. SECURITY SERVICES

It is a processing or communication service that is provided by a system to give a specific kind of production to system resources. Security services implement security policies and are implemented by security mechanisms

1.1 CONFIDENTIALITY

Confidentiality is the protection of transmitted data from passive attacks. It is used to prevent the disclosure of information to unauthorized individuals or systems. It has been defined as “ensuring that information is accessible only to those authorized to have access”. The other aspect of confidentiality is the protection of traffic flow from analysis. **Ex:** A credit card number has to be secured during online transaction.

1.2 AUTHENTICATION

This service assures that a communication is authentic. For a single message transmission, its function is to assure the recipient that the message is from intended source. For an ongoing interaction two aspects are involved. First, during connection initiation the service assures the authenticity of both parties. Second, the connection between the two hosts is not interfered allowing a third party to masquerade as one of the two parties. Two specific authentication services defines in X.800 are

1.3 PEER ENTITY AUTHENTICATION

Verifies the identities of the peer entities involved in communication. Provides use at time of connection establishment and during data transmission. Provides confidence against a masquerade or a replay attack.

1.4 DATA ORIGIN AUTHENTICATION

Assumes the authenticity of source of data unit, but does not provide protection against duplication or modification of data units. Supports applications like electronic mail, where no prior interactions take place between communicating entities.

1.5 INTEGRITY

Integrity means that data cannot be modified without authorization. Like confidentiality, it can be applied to a stream of messages, a single message or selected fields within a message. Two types of integrity services are available. They are

1.6 CONNECTION – ORIENTED INTEGRITY

SERVICE**:** This service deals with a stream of messages, assures that messages are received as sent, with no duplication, insertion, modification, reordering or replays. Destruction of data is also covered here. Hence, it attends to both message stream modification and denial of service.

CONNECTIONLESS-ORIENTED INTEGRITY SERVICE**:** It deals with individual messages regardless of larger context, providing protection against message modification only. An integrity service can be applied with or without recovery. Because it is related to active attacks, major concern will be detection rather than prevention. If a violation is detected and the service reports it, either human intervention or automated recovery machines are required to recover.

NON-REPUDIATION**:** Non-repudiation prevents either sender or receiver from denying a transmitted message. This capability is crucial to e-commerce. Without it an individual or entity can deny that he, she or it is responsible for a transaction, therefore not financially liable.

ACCESS CONTROL: This refers to the ability to control the level of access that individuals or entities have to a network or system and how much information they can receive. It is the ability to limit and control the access to host systems and applications via communication links. For this, each entity trying to gain access must first be identified or authenticated, so that access rights can be tailored to the individuals.

AVAILABILITY: It is defined to be the property of a system or a system resource being accessible and usable upon demand by an authorized system entity. The availability can significantly be affected by a variety of attacks, some amenable to automated counter measures i.e authentication and encryption and others need some sort of physical action to prevent or recover from loss of availability of elements of a distributed system.

II. ISSUES IN NETWORK SECURITY

1. SECURITY MANAGEMENT

Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

2. HOMES AND SMALL BUSINESSES

Basic firewall or a unified threat_management system. For Windows users, basic Anti virus software. An anti-spyware program would also be a good idea. There are many other types of antivirus or anti-spyware programs available.

When using a wireless connection, use a robust password. Also one could try to use the strongest security supported by their wireless devices, such as WPA2 with AES. TKIP may be more widely supported by their devices and should only be considered in cases where they are NOT compliant with AES.

If using Wireless: Change the default SSID network name, also disable SSID Broadcast; as this function is unnecessary for home use. (Security experts consider this to be easily bypassed with modern technology and some knowledge of how wireless traffic is detected by software).

Enable MAC Address filtering to keep track of all home network MAC devices connecting to one's router. (This is not a security feature per se; However it can be used to limit and strictly monitor one's DHCP address pool for unwanted intruders if not just by exclusion, but by AP association.)

Assign STATIC IP addresses to network devices. (This is not a security feature per se; However it may be used, in conjunction with other features, to make one's AP less desirable to would-be intruders.)

Disable ICMP ping on router. Review router or firewall logs to help identify abnormal network connections or traffic to the Internet.

Use passwords for all accounts. For Windows users, Have multiple accounts per family member and use non-administrative accounts for day-to-day activities.

Raise awareness about information security to children.
Medium businesses: A fairly strong firewall or Unified Threat Management System Strong Antivirus software and Internet Security Software. For authentication, use strong passwords and change them on a bi-weekly/monthly basis. When using a wireless connection, use a robust password. Raise awareness about physical security to employees. Use an optional network analyzer or network monitor.

An enlightened administrator or manager: Use a VPN, or Virtual Private Network, to communicate between a main office and satellite offices using the Internet as a connectivity medium. A VPN offers a solution to the expense of leasing a data line while providing a secure network for the offices to communicate. A VPN provides the business with a way to communicate between two in a way mimics a private leased line. Although the Internet is used, it is private because the link is encrypted and convenient to use. A medium sized business needing a secure way to connect several offices will find this a good choice.

Clear employee guidelines should be implemented for using the Internet, including access to non-work related websites, sending and receiving information.

Individual accounts to log on and access company intranet and Internet with monitoring for accountability. Have a back-up policy to recover data in the event of a hardware failure or a security breach that changes, damages or deletes data.

Disable Messenger: Assign several employees to monitor a group like CERT which studies Internet security vulnerabilities and develops training to help improve security.

Large businesses: A strong firewall and proxy, or network Guard, to keep unwanted people out. A strong Antivirus software package and Internet Security Software package. For authentication, use strong passwords and change it on a weekly/bi-weekly basis.

When using a wireless connection, use a robust password. Exercise physical security precautions to employees. Prepare a network analyzer or network monitor and use it when needed. Implement physical security management like closed circuit television for entry areas and restricted zones. Security fencing to mark the company's perimeter. Fire extinguishers for fire-sensitive areas like server rooms and security rooms. Security guards can help to maximize physical security.

School: An adjustable firewall and proxy to allow authorized users access from the outside and inside. Strong Antivirus software and Internet Security Software packages. Wireless connections that lead to firewalls. Children's Internet Protection Act compliance. (Only schools in the USA) Supervision of network to guarantee updates and changes based on popular site usage.

Constant supervision by teachers, librarians, and administrators to guarantee protection against attacks by both internet and sneaker net sources. An enforceable and easy to understand acceptable use policy which differentiates between schools owned and personally owned devices FERPA compliance for institutes of higher education network.

Large government: A strong firewall and proxy to keep unwanted people out. Strong antivirus software and Internet Security Software suites. Strong encryption.

White list authorized wireless connection, block all else. All network hardware is in secure zones. All hosts should be on a private network that is invisible from the outside. Host web servers in a DMZ, or a firewall from the outside and from the inside. Security fencing to mark perimeter and set wireless range to this. Inventory controls of government owned mobile.

To port sweep is to scan multiple hosts for a specific listening port. The latter is typically used in searching for a specific service, for example, an SQL-based computer worm may port sweep looking for hosts listening on TCP port 1433

Idle scan is a TCP port scan method that consists of sending spoofed packets to a computer to find out what services are available. This is accomplished by impersonating another computer called a "zombie" (that is not transmitting or receiving information) and observing the behavior of the "zombie" system.

III. ACTIVE DENIAL-OF-SERVICE ATTACK

In computing, a **denial-of-service (DoS)** or **distributed denial-of-service (DDoS) attack** is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. As clarification, DDoS (Distributed Denial of Service) attacks are sent by two or more persons, or bots. (See botnet) DoS (Denial of Service) attacks are sent by one person or system.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. DoS threats are also common in business,[1] and are sometimes responsible for website attacks. This technique has now seen extensive use in certain games, used by server owners, or disgruntled competitors on games, such as server owners' popular Minecraft servers. Increasingly, DoS attacks have also been used as a form of resistance. Richard Stallman has stated that DoS is a form of 'Internet Street Protests' The term is generally used relating to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management.

One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources' that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Denial-of-service attacks are considered violations of the Internet Architecture Board's Internet proper use policy, and also violate the acceptable use policies of virtually all Internet service providers. They also commonly constitute violations of the laws of individual nations. Spoofing In computing

A denial-of-service (DoS) or **distributed denial-of-service (DDoS) attack** is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. As clarification, DDoS (Distributed Denial of Service) attacks are sent by two or more persons, or bots. (See botnet) DoS (Denial of Service) attacks are sent by one person or system.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. DoS threats are also common in business, and are sometimes responsible for website attacks. This technique has now seen extensive use in certain games, used by server owners, or disgruntled competitors on games, such as server owners' popular Mine craft servers. Increasingly, DoS attacks have also been used as a form of resistance. Richard Stallman has stated that DoS is a form of 'Internet Street Protests'. The term is generally used relating to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management.

One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Denial-of-service attacks are considered violations of the Internet Architecture Board's Internet proper use policy, and also violate the acceptable use policies of virtually all Internet service providers. They also commonly constitute violations of the laws of individual nations.

Man in the middle: In computing a denial-of-service (DoS) or distributed denial-of-service (DDoS) attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet. As clarification, DDoS (Distributed Denial of Service) attacks are sent by two or more persons, or bots. DoS (Denial of Service) attacks are sent by one person or system.

ARP poisoning: ARP spoofing is a technique whereby an attacker sends fake ("spoofed") Address Resolution Protocol (ARP) messages onto a Local Area Network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway), causing any traffic meant for that IP address to be sent to the attacker instead. ARP spoofing may allow an attacker to intercept data frames on a LAN, modify the traffic, or stop the traffic altogether. Often the attack is used as an opening for other attacks, such as denial of service, man in the middle, or session hijacking attacks. The attack can only be used on networks that make use of the Address Resolution Protocol (ARP), and are limited to local network segments.

Smurf attack: The Smurf Attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on. The name *Smurf* comes from the file "smurf.c", the source code of the attack program, which was released in 1997 by TFrea

Buffer overflow : The **Smurf Attack** is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on. The name *Smurf* comes from the file "smurf.c", the source code of the attack program, which was released in 1997 by TFrea

Heap overflow: The **Smurf Attack** is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on. The name *Smurf* comes from the file "smurf.c", the source code of the attack program, which was released in 1997 by TFrea

Format string attack : The Smurf Attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on. The name *Smurf* comes from the file "smurf.c", the source code of the attack program, which was released in 1997 by TFrea

SQL injection : The Smurf Attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on. The name *Smurf* comes from the file "smurf.c", the source code of the attack program, which was released in 1997 by TFrea

CVBER attack: The Smurf Attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on.

Cloud computing security: Cloud computing security or, more simply, cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Cloud security is not to be confused with security software offerings that are cloud-based such as security as a service.

Crime ware : Crime ware is a class of malware designed specifically to automate cybercrime. Crime ware (as distinct from spyware and adware) is designed to perpetrate identity theft through social engineering or technical stealth in order to access a computer user's online accounts at financial services companies and online retailers for the purpose of taking funds from those accounts or completing unauthorized transactions that enrich the thief controlling the crime ware. Crime ware also often has the intent to export confidential or sensitive information from a network for financial exploitation. Crime ware represents a growing problem in network security as many malicious code threats seek to pilfer confidential information.

Cyber security standards : Cyber security standards are security standards which enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks. These guides provide general outlines as well as specific techniques for implementing cyber security. For certain standards, cyber security certification by an accredited body can be obtained. There are many advantages to obtaining certification including the ability to get cyber security insurance. (Spelling of Cyber Security or Cyber security depends on the institution, and there have been discrepancies on older documents. However, since the U.S. Federal Executive Order (EO) 13636, “Improving Critical Infrastructure Cyber security”, most forums and media have embraced spelling "cybersecurity" as a single word.

Data Loss Prevention: Data loss/leak prevention solution is a system that is designed to detect potential data breach / data ex-filtration transmissions and prevent them by monitoring, detecting and blocking sensitive data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage). In data leakage incidents, sensitive data is disclosed to unauthorized personnel either by malicious intent or inadvertent mistake. Such sensitive data can come in the form of private or company information, intellectual property (IP), financial or patient information, credit-card data, and other information depending on the business and the industry.

The terms "data loss" and "data leak" are closely related and are often used interchangeably, though they are somewhat different Data loss incidents turn into data leak incidents in cases where media containing sensitive information is lost and subsequently acquired by unauthorized party. However, a data leak is possible without the data being lost in the originating side.

Greynet greynet (or Grayware) is an elusive networked computer application that is downloaded and installed on end user systems without express permission from network administrators and often without awareness or cognition that it is deeply embedded in the organization’s network fabric. These applications may be of some marginal use to the user, but inevitably consume system and network resources. In addition, greynet applications often open the door for end use systems to become compromised by additional applications, security risks and malware.

Information Leak Prevention: Data loss/leak prevention solution is a system that is designed to detect potential data breach / data ex-filtration transmissions and prevent them by monitoring, detecting and blocking sensitive data while **in-use** (endpoint actions), **in-motion** (network traffic), and **at-rest** (data storage). In data leakage incidents, sensitive data is disclosed to unauthorized personnel either by malicious intent or inadvertent mistake. Such sensitive data can come in the form of private or company information, intellectual property (IP), financial or patient information, credit-card data, and other information depending on the business and the industry.
The terms "data loss" and "data leak" are closely related and are often used interchangeably, though they are somewhat different. Data loss incidents turn into data leak incidents in cases where media containing sensitive information is lost and subsequently acquired by unauthorized party. However, a data leak is possible without the data being lost in the originating side.

Mobile security: Mobile security or mobile phone security has become increasingly important in mobile computing. It is of particular concern as it relates to the security of personal and business information now stored on smart phones. More and more users and businesses use smart phones as communication tools but also as a means of planning and organizing their work and private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks. Indeed, smart phones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company. According to ABI Research the Mobile Security Services market will total around $1.88 billion by the end of 2013.
All smart phones, as computers, are preferred targets of attacks. These attacks exploit weaknesses related to smart

phones that can come from means of communication like SMS, MMS, wifi networks, and GSM. There are also attacks that exploit software vulnerabilities from both the web browser and operating system. Finally, there are forms of malicious software that rely on the weak knowledge of average users.

Different security counter-measures are being developed and applied to smart phones, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps.

Network Security Toolkit: The Network Security Toolkit (NST) is a Linux-based Live CD that provides a set of open source computer security and networking tools to perform routine security and networking diagnostic and monitoring tasks. The distribution can be used as a network security analysis, validation and monitoring tool on servers hosting virtual machines. The majority of tools published in the article "Top 125 security tools" by Insecure.org are available in the toolkit. NST has package management capabilities similar to Fedora and maintains its own repository of additional packages.

TCP Gender Changer: TCP Gender Changer refers to a method of making an internal TCP/IP based network server accessible beyond their protective firewall. It consists of two nodes, one resides on the internal the local area network where it can access the desired server, and the other node runs outside of the local area network, where the client can access it. These nodes are respectively called CC (Connect-Connect) and LL (Listen-Listen). The reason behind naming the nodes is the fact that Connect-Connect node initiates two connections one to the Listen-Listen node and one to the actual server. The Listen-Listen node, however, passively listens on two TCP/IP ports, one to receive a connection from CC and the other one for an incoming connection from the client. The CC node, which runs inside the network, will establish a control connection to the LL, and waiting for LL's signal to open a connection to the internal server. Upon receiving a client connection LL will signal the CC node to connect the server, once done CC will let LL know of the result and if successful LL will keep the client connection and thus the client and server can communicate while CC and LL both relay the data back and forth.

TCP sequence prediction attack: A TCP sequence prediction attack is an attempt to predict the sequence number used to identify the packets in a TCP connection, which can be used to counterfeit packets. The attacker hopes to correctly guess the sequence number to be used by the sending host. If they can do this, they will be able to send counterfeit packets to the receiving host which will seem to originate from the sending host, even though the counterfeit packets may in fact originate from some third host controlled by the attacker. One possible way for this to occur is for the attacker to listen to the conversation occurring between the trusted hosts, and then to issue packets using the same source IP address. By monitoring the traffic before an attack is mounted, the malicious host can figure out the correct sequence number. After the IP address and the correct sequence number are known, it is basically a race between the attacker and the trusted host to get the correct packet sent. One common way for the attacker to send it first is to launch another attack on the trusted host, such as a Denial-of-Service attack. Once the attacker has control over the connection, it is able to send counterfeit packets without getting a response.

If an attacker can cause delivery of counterfeit packets of this sort, he or she may be able to cause various sorts of mischief, including the injection into an existing TCP connection of data of the attacker's choosing, and the premature closure of an existing TCP connection by the injection of counterfeit packets with the RST bit set. Theoretically, other information such as timing differences or information from lower protocol layers could allow the receiving host to distinguish authentic TCP packets from the sending host and counterfeit TCP packets with the correct sequence number sent by the attacker.

Another solution to this type of attack is to configure any router or firewall to not allow packets to come in from an external source but with an internal IP address. Although this does not fix the attack, it will prevent the potential attacks from reaching their targets. If such other information is available to the receiving host, if the attacker cannot also fake that other information, and if the receiving host gathers and uses the information correctly, then the receiving host may be fairly immune to TCP sequence prediction attacks. Usually this is not the case, so the TCP sequence number is the primary means of protection of TCP traffic against these types of attack.

Wireless LAN Security: Wireless security is the prevention of unauthorized access or damage to computers sing wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP is an old IEEE 802.11 standard from 1999 which was outdated in 2003 by WPA or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device which encrypts the network with a 256 bit key; the longer key length improves security over WEP.

Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to hack into wired networks. As a result, it is very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies. The risks to users of wireless technology have increased as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Hackers had not yet had time to latch on to the new technology and wireless was not commonly found in the work place. However, there are a great number of security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. Hacking methods have become much more sophisticated and innovative with wireless. Hacking has also become much easier and more accessible with easy-to-use Windows or Linux-based tools being made available on the web at no charge.

Some organizations that have no wireless access points installed do not feel that they need to address wireless security concerns. In-Stat MDR and META Group have estimated that 95% of all corporate laptop computers that were planned to be purchased in 2005 were equipped with wireless. Issues can arise in a supposedly non-wireless organization when a wireless laptop is plugged into the corporate network. A hacker could sit out in the parking lot and gather info from it through laptops and/or other devices as handhelds, or even break in through this wireless card-equipped laptop and gain access to the wired network.

Wireless security: Is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools.

WEP is an old IEEE 802.11 standard from 1999 which was outdated in 2003 by WPA or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device which encrypts the network with a 256 bit key; the longer key length improves security over WEP.

Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to hack into wired networks.

As a result, it is very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.

IV. CONCLUSION

The risks to users of wireless technology have increased as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Hackers had not yet had time to latch on to the new technology and wireless was not commonly found in the work place. However, there are a great number of security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level.

Hacking methods have become much more sophisticated and innovative with wireless. Hacking has also become much easier and more accessible with easy-to-use Windows or Linux-based tools being made available on the web at no charge. Some organizations that have no wireless access points installed do not feel that they need to address wireless security concerns. In-Stat MDR and META Group have estimated that 95% of all corporate laptop computers that were planned to be purchased in 2005 were equipped with wireless.

Issues can arise in a supposedly non-wireless organization when a wireless laptop is plugged into the corporate network. A hacker could sit out in the parking lot and gather info from it through laptops and/or other devices as handhelds, or even break in through this wireless card-equipped laptop and gain access to the wired network.

REFERENCES

[1] Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," Computer, vol.31, no.9, pp.24- 28, Sep 1998

[2] Kartalopoulos, S. V., "Differentiating Data Security and Network Security," Communications, 2008. ICC '08.

[3] IEEEInternationalConferenceon,pp.1469-1473,19-23May2008[3]"Securityverview,"www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/security-guide/ch-sgs-ov.html.

[4] Molva, R., Institut Eurecom,"Internet Security Architecture," in Computer Networks & ISDN Systems Journal, vol. 31, pp. 787-804, April 1999

[5] Sotillo, S., East Carolina University, "IPv6 security issues,"August 2006,

[6] www.infosecwriters.com/text_resources/pdf/IPv6_SSotillo.pdf.

[7] Andress J., "IPv6: the next internet protocol," April 2005, www.usenix.com/publications/login/2005-04/pdfs/andress0504.pdf.

[8] Warfield M., "Security Implications of IPv6," Internet Security Systems White Paper, documents.iss.net/whitepapers/IPv6.pdf

[9] Adeyinka, O., "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May 2008

[10] Marin, G.A., "Network security basics," Security & Privacy, IEEE , vol.3, no.6, pp. 68-72, Nov.-Dec. 2005

[11] Landwehr, C.E.; Goldschlag, D.M., "Security issues in networks with Internet access," Proceedings of the IEEE, vol.85, no.12, pp.2034-2051, Dec 1997

[12] "Intranet." Wikipedia, The Free Encyclopedia. 23 Jun 2008, 10:43 UTC. WikimediaFoundation,Inc.2Jul2008<http://en.wikipedia.org/w/index.php?title=Intranet&oldid=221174244>.

[13] "Virtual private network." Wikipedia, The Free Encyclopedia. 30 Jun 2008, 19:32 UTC. Wikimedia Foundation, Inc. 2 Jul 2008 <http://en.wikipedia.org/w/index.php?title=Virtual_private_network&oldid=222715612>.

[14] Tyson, J., "How Virtual private networks work,"http://www.howstuffworks.com/vpn.htm .

[15]] Al-Salqan, Y.Y., "Future trends in Internet security," Distributed Computing Systems, 1997., Proceedings of the Sixth IEEE Computer Society Workshop on Future Trends of , vol., no., pp.216-217, 29-31 Oct 1997

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

BIOGRAPHIES

Dr. B. V.Ramana Murthy has done his PhD from Osmania University, presently he working as Professor in Computer Science and Engineering, has 18 years of experience in Teaching and R&D. His primary area of interest is Software Engineering & Web Engineering.

Mr. V Padmakar is pursuing PhD in CSE and has done his M Tech (CSE) from JNTUH, presently working as Professor in Computer Science and Engineering has 17 years of experience in Teaching and Industry. His primary area of interests is Software Engineering, Network Security and Data mining

Mrs. A.Vasavi has done her M.Tech (CSE) from JNTUH, presently She is working as Associate Professor in Computer Science and Engineering department, has 10 years of experience in Teaching. Her area of interest is Network Security and Formal Languages.