Volume 5, Issue 12, December 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

The Wireless Security Survey of India

Ramesh Palanisamy
Research Scholar, AMET University,
Chennai, Tamilnadu, India

V. Mathivanan
Research Supervisor, AMET University,
Chennai, Tamilnadu, India

Abstract: ***Network security method is generally avoiding the losing data of the network infrastructure and, by increase protection of the information. The larger public network, the LAN network environment of the user is very vulnerable to DOS, phishing and other hacking attacks that can be devastating. In this paper, we examine the issues of wireless security from the perspective of the user and the local network. We look at all type of attacks by specialized sender and intercept receivers.***

Keywords: Security, Network, Attacks

I. INTRODUCTION

Wireless networking is used to connect personal desktop asstiance PDA and mobile users who travel from area to area and also mobile networks connected with satellite. A wireless transmission method is a frequently changing the locations to connect the lan segment. The following situations justify the use of wireless technology: Developers need to consider some parameters involving Wireless Raido Frequency technology for better developing wireless networks. Fig 1 shows the typical conntivity wireless vs wired LAN.

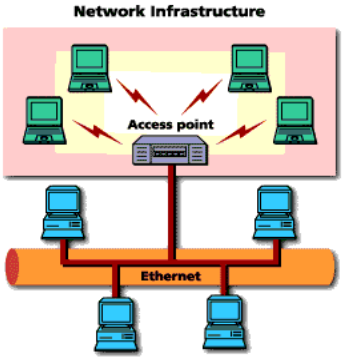

Fig 1: wired and wireless network

1.1 Advantage of wireless networking

- Cable Free Network is useful for organizations such as school, hotels, hospitals, and manufacturing units to implement easily and quickly.
- Mobility is useful for small and medium companies to relocate their premises according to their requirements .
- Connectivity: Its useful for Wireless user connect their network anywhere and anytime.
- Smart Device Connectivity: all type of wifi devices easily connect.

II. CELLULAR NETWORK

A cellular network or mobile network is a one type of wireless network distributed around the areas called cells, each cell served by one fixed transceiver, known as base station. In a cellular network, each cell associated with different set of radio frequencies, it can avoid cell interference. The transmission range of each cell provides radio coverage over a wide area (refer fig 2). This can support many number of mobile phones, pagers to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations.

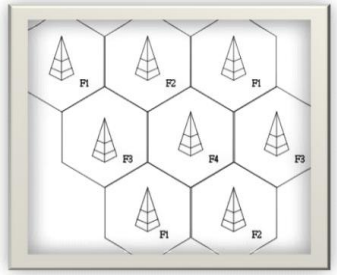

Fig 2: Cellular Network

2.1 Global System for Mobile Communications (GSM): The GSM network is allocated into three types of systems: the switching system, the base station system, and the operation and support system. GSM technology is mainly used for mobile phones.[7]

2.2 Personal Communications Service (PCS): PCS is a radio frequency that can be used by mobile phones in some areas.

2.3 D-AMPS: Digital Advanced Mobile Phone Service, an advanced version of AMPS, is being phased out due to advance technology. The newer Global System for Mobile Communications networks are replacing the older system.

2.4 Global area network: A global area network (GAN) is used for supporting mobile in number of wireless LANs and satellite coverage areas.

2.5 Space network: This network used for communication between spacecraft.

2.6 Cellular Networks in India: India's Cellular network is the one of the largest mobile network in the world based on the total number of telephone users (both fixed and mobile phone).India is using the lowest call tariffs for their mobile users. It has the one of the largest Internet users. According to the Internet and Mobile Association of India (IAMAI), the Internet user base in the country stood at 190 million at the end of June, 2013. Indian mobile communication industry, internet and television broadcasting. India mobile Industry in the country which is in an ongoing process of transforming into next generation network, wide system of modern network features such as

- digital telephone exchanges,
- mobile switching centers,
- media gateways
- signaling gateways

Interconnected by a wide variety of transmission systems using

- fiber-optics
- Microwave radio relay
- copper-pair,
- optic-fiber
- Wireless technologies.

*** Rank 1**

Operator name: Airtel, Technology using: GSM, EDGE,HSPA, TD- HYPERLINK "http://en.wikipedia.org/wiki/Time-Division_Long-Term_Evolution"LTE,Subscribers in crores: 19.84, Market share: 28.49%

*** Rank 2**

Operator name: Vodafone, Technology using: GSM, EDGE,HSDPA, Subscribers in crores: 16.04, Market share: 22.91%

*** Rank 3**

Operator name: Reliance Communications,
Technology,using:CDMA2000,EVDOREV.AGSM,EDGE,HSDPA,HSPA+,WiMAX Subscribers in crores: 15.41, Market share: Reliance ADAG (67%),Public (26%)22.91%.

*** Rank 4**

Operator name: Idea Cellular, Technology using: GSM,EDGE HSPA ,Subscribers in crores: 12.87, Ownership Aditya Birla(49.05%) Axi HYPERLINK "http://en.wikipedia.org/wiki/Axiata_Group_Berhad"t HYPERLINK "http://en.wikipedia.org/wiki/Axiata_Group_Berhad"ata HYPERLINK "http://en.wikipedia.org/wiki/Axiata_Group_Berhad" Group_HYPERLINK "http://en.wikipedia.org/wiki/Axiata_Group_Berhad"Berhad (19.96%) Market share: 18.74%.

*** Rank 5**

Operator name: BSNL, Technology using: GSM
EDGE,HSDPA,HSPA+,CDMA2000,EVDOREV,WiMAX,WiFi,,Subscribers in crores: 9.72, Ownership State-owned Market share: 14.31%.

*** Rank 6**

Operator name: Tata DoCoMo,Virgin Mobile India
Talk24/T24,Technology-using:CDMA2000,EVDO REV,GSM,EDGE,HSPA+,Subscribers in crores: 9.01,Ownership:Tata,Teleservices,(74%)NTT DoCoMo (26%) Market share: 14.31%

*** Rank 7**

Operator name: Aircel, Technology using: GSM
EDGE,HSDPA,TD-LTE,Subscribers in crores:6.69, Ownership: Maxis Communications (74%)
Apollo Hospital (26%) Market share: 9.32%

*** Rank 8**

Operator name: Uninor, Technology usingGSM
EDGE,Subscribers in crores: 0.32, Ownership Unitech Wireless(67.25%),Unitech Group (32.75%) Market share: 4.77%

*** Rank 9**

Operator name: MTS India, Technology using: CDMA2000,EVDO REV. B,Subscribers in crores: 1.4, Ownership Sistema (73.71%),Shyam Group (23.79%) Market share: N/A

*** Rank 10**

Operator name: Videocon, Technology using: GSM

GPRS,EDGE,Subscribers in crores: 0.40, Ownership Videocon Market share: 0.48%.

*** Rank 11**

Operator name: MTNL, Technology using: GSM

HSDPA,CDMA2000,Subscribers in crores: 0.35, Ownership State-owned Market share: 0.53%.

*** Rank 12**

Operator name: Loop Mobile, Technology using: GSM

EDGE,Subscribers in crores: 0.3, Ownership Khaitan HYPERLINK "http://en.wikipedia.org/w/index.php?title=Khaitan_Holding_Group&action=edit&redlink=1" Holding Group (100%) Market share: 0.45%

III. ACTIVE USER BASE OF TELECOM OPERATORS

The Active connection data represents peak VLR (Visitor Location Register) data for the month. Some stats:There were 731.44 million active connection in the month of June.- **Idea has 97.90% of its connections active** – the maximum among all the operators.- **Vodafone has the second highest active connection base** of 95.45%, followed by **Airtel** at 94.87%. In terms of the number of active connections, Airtel leads with 181.11 million connections followed by Vodafone at 147.97 million connections.

Indian Wireless Connections - June 2013						©MEDIANAMA
Telcos	May-13	Jun-13	Additions	Change	Active	
Bharti Airtel	189,649,322	190,912,421	1,263,099	0.67%	181,118,614	94.87%
RCOM	124,898,961	125,732,649	833,688	0.67%	109,198,806	86.85%
Vodafone	154,686,843	155,033,868	347,025	0.22%	147,979,827	95.45%
BSNL	98,066,315	97,990,720	-75,595	-0.08%	55,737,122	56.88%
Tata Teleservices	65,265,214	64,626,015	-639,199	-0.98%	43,919,840	67.96%
Idea Cellular	123,758,712	124,968,107	1,209,395	0.98%	122,343,777	97.90%
Aircel	60,358,016	60,969,974	611,958	1.01%	39,051,268	64.05%
MTNL	4,800,884	4,510,993	-289,891	-6.04%	2,131,895	47.26%
Loop Telecom	2,868,751	2,716,568	-152,183	-5.30%	1,341,170	49.37%
MTS	10,119,469	9,769,326	-350,143	-3.46%	5,373,129	55.00%
Uninor	31,999,931	32,295,872	295,941	0.92%	21,066,597	65.23%
HFCL	1,441,260	1,418,027	-23,233	-1.61%	818,060	57.69%
S Tel	0	0	0	0.00%	-	0.00%
Videocon	2,285,177	2,417,993	132,816	5.81%	1,383,576	57.22%
Etisalat+Allianz	0	0	0	0.00%	-	0.00%
All Operators	870,198,855	873,362,533	3,163,678	0.36%	731,441,121	83.75%

Fig 3: Active connection

IV. SECURITY ISSUES IN CELLULAR NETWORK

4.1 Problems

The GAO report came up with a list of mobile vulnerabilities it says are common to all mobile platforms and it offered a number of possible fixes for the weaknesses.

4.2 From the report:

1. Mobile devices often do not have passwords enabled. Mobile devices often lack passwords to authenticate users and control access to data stored on the devices. Many devices have the technical capability to support passwords, personal identification numbers (PIN), or pattern screen locks for authentication. Some mobile devices also include a biometric reader to scan a fingerprint for authentication. However, anecdotal information indicates that consumers seldom employ these mechanisms. Additionally, if users do use a password or PIN they often choose passwords or PINs that can be easily determined or bypassed, such as 1234 or 0000. Without passwords or PINs to lock the device, there is increased risk that stolen or lost phones' information could be accessed by unauthorized users who could view sensitive information and misuse mobile devices.

. Two-factor authentication is not always used when conducting sensitive transactions on mobile devices. According to studies, consumers generally use static passwords instead of two-factor authentication when conducting online sensitive transactions while using mobile devices. Using static passwords for authentication has security drawbacks: passwords can be guessed, forgotten, written down and stolen, or eavesdropped. Two-factor authentication generally provides a higher level of security than traditional passwords and PINs, and this higher level may be important for sensitive transactions. Two-factor refers to an authentication system in which users are required to authenticate using at least two different "factors" something you know, something you have, or something you are before being granted access. Mobile devices can be used as a second factor in some two-factor authentication schemes. The mobile device can generate pass codes, or the codes can be sent via a text message to the phone. Without two-factor authentication, increased risk exists that unauthorized users could gain access to sensitive information and misuse mobile devices.

3. Wireless transmissions are not always encrypted. Information such as e-mails sent by a mobile device is usually not encrypted while in transit. In addition, many applications do not encrypt the data they transmit and receive over the network, making it easy for the data to be intercepted. For example, if an application is transmitting data over an unencrypted WiFi network using http (rather than secure http), the data can be easily intercepted. When a wireless transmission is not encrypted, data can be easily intercepted.

4. Mobile devices may contain malware. Consumers may download applications that contain malware. Consumers download malware unknowingly because it can be disguised as a game, security patch, utility, or other useful application. It is difficult for users to tell the difference between a legitimate application and one containing malware. For example, an application could be repackaged with malware and a consumer could inadvertently download it onto a mobile device. the data can be easily intercepted. When a wireless transmission is not encrypted, data can be easily intercepted by eavesdroppers, who may gain unauthorized access to sensitive information.

5. Mobile devices often do not use security software. Many mobile devices do not come preinstalled with security software to protect against malicious applications, spyware, and malware-based attacks. Further, users do not always install security software, in part because mobile devices often do not come preloaded with such software. While such software may slow operations and affect battery life on some mobile devices, without it, the risk may be increased that an attacker could successfully distribute malware such as viruses, Trojans, spyware, and spam to lure users into revealing passwords or other confidential information.

6. Operating systems may be out-of-date. Security patches or fixes for mobile devices' operating systems are not always installed on mobile devices in a timely manner. It can take weeks to months before security updates are provided to consumers' devices. Depending on the nature of the vulnerability, the patching process may be complex and involve many parties. For example, Google develops updates to fix security vulnerabilities in the Android OS, but it is up to device manufacturers to produce a device-specific update incorporating the vulnerability fix, which can take time if there are proprietary modifications to the device's software. Once a manufacturer produces an update, it is up to each carrier to test it and transmit the updates to consumers' devices. However, carriers can be delayed in providing the updates because they need time to test whether they interfere with other aspects of the device or the software installed on it.

In addition, mobile devices that are older than two years may not receive security updates because manufacturers may no longer support these devices. Many manufacturers stop supporting smartphones as soon as 12 to 18 months after their release. Such devices may face increased risk if manufacturers do not develop patches for newly discovered vulnerabilities.

7. Software on mobile devices may be out-of-date. Security patches for third-party applications are not always developed and released in a timely manner. In addition, mobile third-party applications, including web browsers, do not always notify consumers when updates are available. Unlike traditional web browsers, mobile browsers rarely get updates. Using outdated software increases the risk that an attacker may exploit vulnerabilities associated with these devices.

8. Mobile devices often do not limit Internet connections. Many mobile devices do not have firewalls to limit connections. When the device is connected to a wide area network it uses communications ports to connect with other devices and the Internet. A hacker could access the mobile device through a port that is not secured. A firewall secures these ports and allows the user to choose what connections he wants to allow into the mobile device. Without a firewall, the mobile device may be open to intrusion through an unsecured communications port, and an intruder may be able to obtain sensitive information on the device and misuse it.

9. Mobile devices may have unauthorized modifications. The process of modifying a mobile device to remove its limitations so consumers can add features (known as "jailbreaking" or "rooting") changes how security for the device is managed and could increase security risks. Jailbreaking allows users to gain access to the operating system of a device so as to permit the installation of unauthorized software functions and applications and/or to not be tied to a particular wireless carrier. While some users may jailbreak or root their mobile devices specifically to install security enhancements such as firewalls, others may simply be looking for a less expensive or easier way to install desirable applications. In the latter case, users face increased security risks, because they are bypassing the application vetting process established by the manufacturer and thus have less protection against inadvertently installing malware. Further, jailbroken devices may not receive notifications of security updates from the manufacturer and may require extra effort from the user to maintain up-to-date software.

10. The GAO report went on to state that connecting to an unsecured WiFi network could let an attacker access personal information from a device, putting users at risk for data and identity theft. One type of attack that exploits the WiFi network is known as man-in-the-middle, where an attacker inserts himself in the middle of the communication stream and steals information.9. Communication channels may be poorly secured. Having communication channels, such as Bluetooth communications, "open" or in "discovery" mode (which allows the device to be seen by other Bluetooth-enabled devices so that connections can be made) could allow an attacker to install malware through that connection, or surreptitiously activate a microphone or camera to eavesdrop on the user. In addition, using unsecured public wireless Internet networks or WiFi spots could allow an attacker to connect to the device and view sensitive information.

V. SECURED CELLULAR NETWORKS

Enable user authentication: Devices can be configured to require passwords or PINs to gain access. In addition, the password field can be masked to prevent it from being observed, and the devices can activate idle-time screen locking to prevent unauthorized access.

Verify the authenticity of downloaded applications: Procedures can be implemented for assessing the digital signatures of downloaded applications to ensure that they have not been tampered with.Enable two-factor authentication for sensitive transactions: Two-factor authentication can be used when conducting sensitive transactions on mobile devices. Two-factor authentication provides a higher level of security than traditional passwords. Two-factor refers to an authentication system in which users are required to authenticate using at least two different "factors" something you know, something you have, or something you are before being granted access. Mobile devices themselves can be used as a second factor in

some two-factor authentication schemes used for remote access. The mobile device can generate pass codes, or the codes can be sent via a text message to the phone. Two-factor authentication may be important when sensitive transactions occur, such as for mobile banking or conducting financial transactions.

- Install antimalware capability: Antimalware protection can be installed to protect against malicious applications, viruses, spyware, infected secure digital cards,b and malware-based attacks. In addition, such capabilities can protect against unwanted (spam) voice messages, text messages, and e-mail attachments.
- Install a firewall: A personal firewall can protect against unauthorized connections by intercepting both incoming and outgoing connection attempts and blocking or permitting them based on a list of rules.
- Install security updates: Software updates can be automatically transferred from the manufacturer or carrier directly to a mobile device. Procedures can be implemented to ensure these updates are transmitted promptly.
- Remotely disable lost or stolen devices: Remote disabling is a feature for lost or stolen devices that either locks the device or completely erases its contents remotely. Locked devices can be unlocked subsequently by the user if they are recovered.
- Enable encryption for data stored on device or memory card: File encryption protects sensitive data stored on mobile devices and memory cards. Devices can have built-in encryption capabilities or use commercially available encryption tools.
- Enable whitelisting: Whitelisting is a software control that permits only known safe applications to execute commands.
- Establish a mobile device security policy: Security policies define the rules, principles, and practices that determine how an organization treats mobile devices, whether they are issued by the organization or owned by individuals. Policies should cover areas such as roles and responsibilities, infrastructure security, device security, and security assessments. By establishing policies that address these areas, agencies can create a framework for applying practices, tools, and training to help support the security of wireless networks.
- Provide mobile device security training: Training employees in an organization's mobile security policies can help to ensure that mobile devices are configured, operated, and used in a secure and appropriate manner.
- Establish a deployment plan: Following a well-designed deployment plan helps to ensure that security objectives are met.

5.1 Secure our wireless against these threats.

- Change the default system ID of your wireless access point or router.
- Change the default password for your system.
- Turn off identifier broadcasting.
- Encrypt wireless communications. (WPA-based encryption offers better protection than WEP-based encryption.)
- Use your router's built-in firewall to restrict access to your network.
- Keep your wireless system patched and up to date.
- Use a virtual private network (VPN) if possible.
- Avoid using passwords and providing personal information to web sites.
- Encrypt your files.Be aware of your surroundings.

VI. CONCLUSION

When we are using a telecommunication via a radio signal. Sometimes our secure this signal, strangers can piggyback on our data connection will hack our connection they can watch our network activity or they will access our files on our device. Today wireless networks are helping and definitely providing the opportunity to the colleges, hospitals and army, etc to cut costs, to increase security and the productivity and mobility. By following the above recommended security measures the normal work will in fact continue without any problem. The key to keep up and creating a security telecommunications network is on-going running all kind of people.

REFERENCE

[1] http://en.wikipedia.org/wiki/Wireless
[2] http://en.wikipedia.org/wiki/Wireless_network
[3] http://www.networkcomputing.com/netdesign/wlan2.html
[4] http://en.wikipedia.org/wiki/Wireless_network
[5] http://en.wikipedia.org/wiki/Mobile_network_operators_of_India
[6] http://www.ttplindia.com/wireless-networking.php
[7] http://searchdatacenter.techtarget.in/survey/Wireless-networks-in-demand-at-India-Inc-BYODs-aftermath
[8] http://chimera.labs.oreilly.com/books/1230000000545/ch05.html#REAL_WIRELESS_PERFORMANCE
[9] http://www.medianama.com/2013/09/223-june-2013-india-has-15-19m-broadband-731-44m-active-mobile-connections/
[10] HTTP://EN.WIKIPEDIA.ORG/WIKI/TELECOMMUNICATIONS_STATISTICS_IN_INDIA

