###

###  A Paper Presentation On

**INFORAMTION SECURITY ON WIRELESS NETWORKS**

**By**

ASHISH P. VISHROJWAR LALIT UMAP

 IV th year [IT] IV th year [CE]

ashishvishrojwar@gmail.com

### MADHUKARRAO PANDAV COLLEGE OF ENGG. BHANDARA

**2012-13**

### Guided by:

**Miss. Nita Maske Madam**

### CONTENTS

**1.ABSTRACT**

**2.INTRODUCTION**

**3.IMPORTANCE OF WIRELESS NETWORKS**

**4.IEEE 802.11**

**5.SECURITY CONCERNS MOUNT FOR WIRELESS NETWORKS**

**6.MOST POPULAR WIRELESS DEVICES**

1. **LAPTOPS**

# PHYSICAL PROBLEMS WITH LAPTOPS

* **SOLUTIONS TO PHYSICAL PROBLEMS**
* **SOFTWARE PROBLEMS WITH LAPTOPS**
* **SOLUTIONS TO SOFTWARE PROBLEMS**
1. **POCKET PC**

## PROBLEMS AND THEIR MEASURES

# PDA

* **SOLUTIONS TO PDA SECURITY**

**7.CONCLUSION**

**8.REFERENCES**

**ABSTRACT:**

Information security in the wireless network is a research hotspot. “Who cares for information security?”. This paper is asking "who cares" about information security-but may perhaps be better stated as "who should care”. It is likely that there is no simple answer to this question-and that responsibility for information security needs to be taken by several parties within the utility. The initial sections of this paper look at some of the different forms of attack an intruder may use to steal information from the sources(in particular in wireless networks), to cause device services to mal-function, or to deny the access to its own information.

Increasingly, companies and individuals are using wireless technology for important communications they want to keep private, so this paper in particular deals with **information security in wireless networks**.

Wireless network security based on the **IEEE 802.11** standard has received a lot of negative attention, since it is coupled with several design errors and security problems. This paper suggests the ways to lessen the security problems of IEEE 802.11. As wireless platforms mature, grow in popularity, and store valuable information, hackers are stepping up their attacks on these new targets. This is a peculiar problem because wireless devices, including **LAPTOPS, POCKET PCs and PDA (**Personal Digital Assistants), were not originally designed with security as a top priority. Now, however, wireless security is becoming an important area of product research and development. As in the wired world, wireless security boils down to protecting information and preventing unauthorized system access. However, it is challenging to implement security in small-footprint devices with low processing power and small memory capacities and that use unreliable, low bandwidth wireless networks.

INTRODUCTION:

## DEFINITION FOR INFORMATION:

A resource is something that has value to the organization. Defining **INFORMATION** resources at the appropriate level is a task that requires experience with the information. Data items that are always used together as a unit of information can be considered a single information resource. Information is the **summarization of data**. Technically, data are raw facts and figures that are processed into information, such as summaries and totals. But since information can also be the raw data for the next job or person, the two terms cannot be precisely defined, and both are used interchangeably. Information is becoming a crucial if not the most important resource of the economy and the society at large. This poses new challenges for the protection of this new resource and of intellectual property in general.

**NEED FOR INFORMATION SECURITY**: All of these resources have security requirements that vary depending upon the importance of the particular resource. However, before proper security measures can be applied, the company’s resources must be identified and their value and cost to the company should they be disclosed or destroyed, must be assigned.

Determining the value of information assets is pivotal to determining the appropriate level of security.

Classification is conceptually very easy. Determine the value and risks and assign an appropriate classification. However, information has varying degrees of importance and sensitivity, and a classification system must be used to ensure that the information receives an appropriate level of protection

The following factors should be considered when assigning a resource’s security classifications:

* **Sensitivityof the information**
* **Consequences of disclosure**
* **Information lifecycle**

**IMPORTANCE OF WIRELESS NETWORKS**:

Wireless technologies have become increasingly popular in our everyday business and personal lives. Cell phones offer users a freedom of movement unimaginable just over 10 years ago. Personal Digital Assistants (PDA) allow individuals to access calendars, e-mail, address and phone number lists, and the Internet. Some technologies even offer global positioning system (GPS) capabilities that can pinpoint the location of the device anywhere in the world. Wireless technologies promise to offer even more features and functions in the next few years

 Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections - without requiring network cabling. Wireless technologies use radio transmissions as the means for transmitting data, whereas wired technologies use cables. Wireless technologies range from complex systems, such as WLANs and cell phones, to simple devices such as wireless headphones, microphones, and other devices that do not process or store information. They also include infrared (IR) devices such as remote controls, some cordless computer keyboards and mice, all of which require a direct line of sight between the transmitter and the receiver to close the link. Historically, the number one application for wireless has been mobile voice communication with cellular technology, which has been around since the early 1980s.

 A WLAN connects computers and other components to the network using an access point device. An access point communicates with devices equipped with wireless network adaptors; it connects to a wired Ethernet LAN via an RJ-45 port. Access point devices typically have coverage areas of up to 300 feet (100 meters). This coverage area is called a cell or range.

WLANs offer four primary benefits to users:

**User Mobility, Rapid Installation, Flexibility and Scalability**

**IMPORTANCE OF SECURITY FOR WIRELESS LANS:**

 The benefits of wireless LANs (WLAN) are undeniable but the risks introduced by them are increasing exponentially. According to InStat MDR More than 75 million Wi-Fi devices have been deployed worldwide and another 4 million new WLAN devices are being shipped per month. Security is top-of-mind for businesses managing wireless networks, especially as they start adding new applications, such as voice over IP.

Wireless networks are frequently categorized into three groups based on their coverage range: **WWAN, WLAN, and WPAN** (Wireless Personal Area Network) and WLAN includes **802.11.**

### IEEE 802.11:

WLANs are based on the IEEE 802.11 standard, which the IEEE first developed in 1997. The IEEE designed 802.11 to support medium-range, higher data rate applications, such as Ethernet networks, and to address mobile and portable stations. Mobile stations access the LAN while in motion, while

portable stations are moved from location to location, but are only used while in a fixed physical location.

**ARCHIETECTURE OF IEEE 802.11:**

**802.11** is the original WLAN standard, designed for 1Mbps to 2Mbps wireless transmissions. It was followed in 1999 by **802.11a**, which established a high-speed WLAN standard for the 5GHz band and supported 54Mbps. Also completed in 1999 was the **802.11b** standard, which operates in the 2.4 - 2.48GHz band and supports 11Mbps. The 802.11b standard is currently the dominant standard for WLANs, providing sufficient speeds for most of today's application. Another standard, **802.11g**, still in draft, operates in the 2.4GHz waveband, where current WLAN products based on the 802.11b standard operate. Two other important and related standards for WLANs are **802.1x** and **802.11i.** The 802.1x, a port-level access control protocol, provides a security framework for IEEE networks, including Ethernet and wireless networks. The 802.11i standard, also still in draft, was created for wireless-specific security functions that operate with IEEE 802.1x.

### SECURITY FEATURES OF 802.11 WIRELESS LANS PER THE STANDARD

The three basic security services defined by IEEE for the WLAN environment are as follows:

* **Authentication**
* **Confidentiality**
* **Integrity**

**Security Concerns Mount For Wireless Networks**

The difficulties of securing the air: Security is top-of-mind for businesses managing wireless networks, especially as they start adding new applications, such as voice over IP.To understand the risk of wireless LANs, one must first understand the security vulnerabilities of all wireless LANs. Wireless LANs face all of the security challenges of any wired network. First the medium in which a wireless LAN **operates is the air,** an uncontrollable space. Additionally, wireless devices self deploy and have the capability to connect to strangers.

There are many ways in which WLANs can be compromised:

**More than rogue access points**: A rogue WLAN has traditionally been thought of as a physical access point unsanctioned by network administrators. Today rogue WLANs are further defined as laptops, handhelds with wireless cards, barcode scanners, printers, copiers or any wireless LAN device.

**Soft access points**: While hardware APs have been the focus of security issues to-date, wireless-enabled laptops are easily configured to function as access points with commonly available freeware such as HostAP or software from PCTel. Known as "Soft APs," these laptops are harder to detect than rogue access points.

**Accidental associations**: Accidental associations are created when a neighboring access point across the street or on adjacent floors of a building bleeds over into another organization's air space triggering its wireless devices to connect. Once those devices connect with the neighboring network, the neighbor has access back into the organization.

**To improve the security of your home wireless LAN:**

* Change Default Administrator Passwords (and Usernames)
* Turn on (Compatible) Encryption
* Enable MAC Address Filtering
* Assign Static IP Addresses to Devices
* Position the Router or Access Point Safely

**\**

**MOST POPULAR WIRELESS NETWORKS:**

**LAPTOPS:**

Laptop computers are increasingly being used by users to store and transport sensitive data. Laptops are a desirable tool due to their portability and ease of use; however, as computer technology becomes more advanced so do methods of compromising

 Vulnerabilities inherent in the laptop's configuration and existing security protocols.

If an unauthorized user has physical access to a laptop computer system, then gaining administrative access (i.e. the ability to run any program) to the laptop, and its sensitive data, is a simple process.

 Laptop security can be broken down into three phases**: physical security, access control/authentication and tracking/recovery**. But the biggest challenge may be changing users' attitudes and habits.

**Physical Problems with Laptops:**

Laptop computers are a prime target for theft from your office, your home, or at airports, hotels, railroad terminals and on trains while you are traveling. They are an extremely attractive target for all types of thieves, as they are small, can be carried away without attracting attention, and are easily sold for a good price.

**Solutions to Physical Problems:** Vendors have crafted a variety of **physical security devices** that diminish the threat of laptop thefts. Others manufacturers offer **alarms and sensors** for alerting users that someone is tampering with their notebook computers. Disguise your laptop. The distinctive size and shape of a laptop computer make it an easily spotted target for thieves

* Never let a laptop out of your sight in an airport or other public area
* Beware of power surges. Don't be connected to either power lines or a copper phone line during a storm with lightning.

**Software Problems in Laptops:** Most laptop computers were designed with basic access control features, including an **easily defeated BIOS password system**. But these password systems have limited effectiveness, since users will often choose **easily crackedPINs** and will not perform proper maintenance. On the other hand, organizations with **stringent security policies** are often burdened by the increased number of calls to their help desks by users who forgot their constantly changing and difficult-to-remember laptop passwords.

 The leap from compromised wireless laptop to the convention's wired network is possible, because most Wi-Fi notebooks **automatically connect to any access point within range**, even as they're on the wired network.

**Security Flaw expressed By a Self-Confessed Hacker: B**uilt-in wireless capabilities in Windows operating system searches for available wireless connections on start up, but when no wireless link is found then the software establishes an ad-hoc link to a local address can be established between the hacker’s and the victim’s machines, and the hacker can get full control of the compromised system.

**Solutions to Software Problems of Laptops:**

* Strong Authentication:
* **Encryption:**
* **Maintaining up-to-date anti-virus.**
* **Patching.**
* **Biometrics**
* **Access Point Configuration:** Network administrators need to configure APs in accordance with established security policies and requirements. Properly configuring administrative passwords, encryption settings, reset function, automatic network connection function, Ethernet Medium Access Control (MAC) Access Control Lists (ACL) agents will help eliminate many of the vulnerabilities inherent in a vendor's software default configuration.
* **Intrusion Detection System:** An IDS is an effective tool for determining whether unauthorized users are attempting to access, have already accessed, or have compromised the network. IDS for WLANs can either be host-based or network-based.
* **Firewalls:** A firewall is a hardware or software solution implemented within the network infrastructure to enforce an organization’s security policies by restricting access to specific network resources. The Cisco IOS Firewall provides integrated firewall and intrusion detection functionality for every perimeter of the network.

**POCKET PC:**

As the popularity of mobile devices increases, the security of the information and data on these devices becomes more important. The Pocket PC contains many features that reduce the risks that are associated with mobile devices

**Problems with Pocket PC and Their Measures:**

To reduce the possibility of data being stolen:

* Use the Power On password on your device
* Password protect your Compact Flash cards. The device must support this feature.
* Encrypting Your Data.
* Protecting Your Communication Links

**PDA (Personal Data Assistant):**

The personal data assistant (PDA) is a convenient, portable platform to assist the user in performing tasks in an efficient manner. However, because of its small size, it presents some risks to the user. The largest risk is **loss or theft of a device** containing sensitive information (e.g., protected health information (PHI)). Additional risks include **unauthorized physical access** to the device allowing access to the data contained within the device**, unauthorized electronic access** to the device allowing access to the data contained within the device and the **inability of authorized users** to access the system and/or data (known as denial of service).

**Solutions to PDA Security:**

* **Keep the PDA in your possession**.
* **Utilize physical restraints on PDA**
* **Disable IR Reception** The PDA device utilizing the infrared (IR) printing feature must transmit (or “beam”) information to the printer via IR. However, the device should not need to receive IR transmissions. The PDA should be configured to disable the reception of IR messages.
* **Use “Power-on” Passwords**.

# Password “lock” device when not in use

* **Remove applications and data from PDA when removed from service**
* **Use strong passwords**
* **Protect passwords**

**CONCLUSION:**

In this paper we already discussed about information security and importance of information security in wireless networks.As far as man are particular about their comforts there will be growth for wireless technologies. Because wireless devices unlike wired networks offers great comfort to the users and can be carried anywhere. As there is huge demand for wireless devices manufacturers are working towards the goal to provide a device capable of delivering multiple services. Next-generation mobile phones, already in the market, are quickly incorporating

PDA, IR, and wireless Internet, e-mail, and GPS capabilities. Future developments that will soon be in the market include GSM-based technologies such as General Packet Radio Service (GPRS), Enhanced Data GSM Environment (EDGE), and Universal Mobile Telecommunications Service (UMTS). These technologies will provide high data transmission rates and greater networking capabilities. However, **each new development will present its own security risks, and it is our own responsibility to address these risks to ensure that critical assets(information) remain protected**.

**REFERENCES:**

* Norton, P. and Stockman, M. *Peter Norton’s Information Security Fundamentals*. 2000.
* Arbaugh, W.A., Shankar, N., and Wan, Y.C., “Your 802.11 Wireless Networks Has No Clothes.”, March 30, 2001.

General Internet Resources:

* [www.networkworld.com](http://www.networkworld.com)
* [www.microsoft.com/technet](http://www.microsoft.com/technet)
* [www.about.com/computer](http://www.about.com/computer)