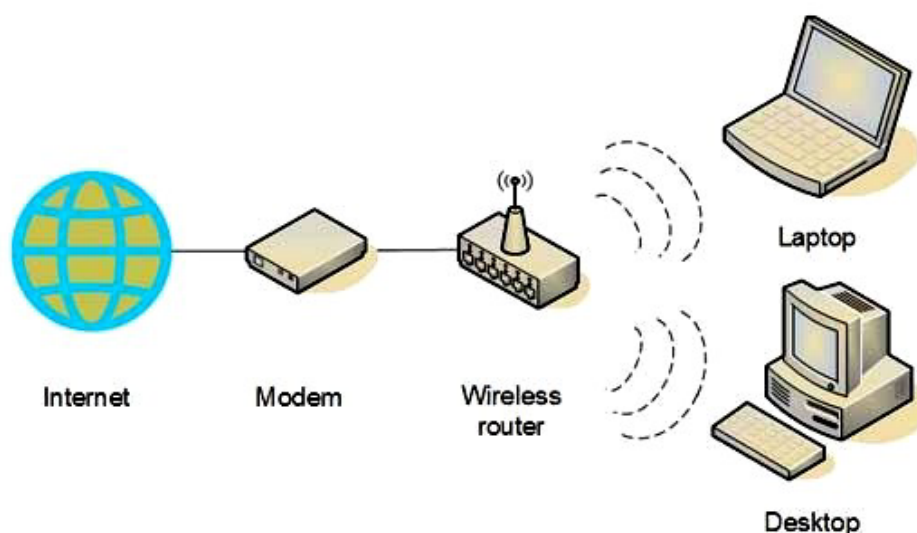


SECURING WI-FI NETWORK

(10 STEPS TO DIY SECURITY)



RAKESH M GOYAL

ANKUR GOYAL

Published by
Center for Research and Prevention of Computer Crimes

Sponsored by
Sysman Computers Private Limited
(www.sysman.in)

Supported by
Information Security Education And Awareness Project
(A project of Department of Information Technology, MoCIT, Govt. of India)

and
Data Security Council of India
(A Self Regulatory Organisation established by NASSCOM)
(www.dsci.in)

2008

CENTRE FOR RESEARCH AND PREVENTION OF COMPUTER CRIMES

Centre for Research and Prevention of Computer Crimes (CRPCC) is a registered society with R&D centre to study the multifarious dimensions of Computer Crimes and to define preventive methods. Policies of CRPCC are determined by its Governing Board and day-to-day management is supervised by its Director-General, Mr. Rakesh Goyal.

FUNCTIONS OF CRPCC:

1. To study the phenomena of Computer Crimes.
2. To study the human socio-economic factors underlying Computer Crimes.
3. To publish research paper on Computer Crimes.
4. To create awareness about Computer Crimes.
5. To co-ordinate with international agencies handling Computer Crimes.
6. To train individuals in prevention of Computer Crimes.
7. To find new ways & means of prevention of Computer Crimes.
8. To help the governments in drafting laws and rules on Computer Crimes.
9. To have distant learning programmes on Computer Crimes.
10. To test new technologies for their vulnerability to Computer Crimes.
11. To develop special software for monitoring and prevention of Computer Crimes.
12. To investigate computer crime incidents.
13. To provide consulting services on computer crime prevention.
14. To undertake market research studies on losses due to computer crimes.

PUBLICATIONS :

1. Book - **Computer Crimes- Concepts, Control & Prevention** by Rakesh M Goyal and Manohar S Pawar (1993).
2. Book - **Case Studies on Information Systems Security** edited by Dr. Sharad D. Varde (2002).
3. Book - **Digital Signature: All You Want To Know About It, But Do Not Know Whom To Ask** by Rakesh M Goyal (2004).
4. Book - **Demystifying Information Technology Act – 2000** by Rakesh M Goyal (2005).
5. eBook - **Sankat Mochan Yojana** – By Rakesh M Goyal (A Citizen's Initiative on local basis in each locality, till official aid moves in to provide immediate relief and assistance to effected co-citizens without any monetary assistance from any government / statutory body) (2005).
6. **12 research papers and over 50 articles** in international journals, local newspapers and magazines.
7. **IT Security e-Newsletter – 3 times a week.** Published on every Monday, Wednesday and Friday. Over 600 editions since June 2005. 75000+ direct subscribers as on October 2008. Details/Subscribe at <http://groups.google.co.in/group/control-computer-crimes?hl=en>

ACHIEVEMENTS :

1. Conducted awareness programmes for over 30,000 persons since 1991.
2. Investigated over 2000 incidents of Computer Crimes since 1991.
3. Provided assistance to various organisations on **Risk Analysis, IS Security Policies, IS Audit, Computer Crimes & Frauds, Prevention Strategy, Recovery Strategy and Plan, Data Transfer Strategy, Contingency Plans, Firewalls and Network Security.**

SECURING WI-FI NETWORK

SECURING WI-FI NETWORK

(10 STEPS TO DIY SECURITY)

RAKESH M GOYAL & ANKUR GOYAL

Center for Research and Prevention of Computer Crimes

Sponsored by

Sysman Computers Private Limited
(www.sysman.in)

2008

SECURING WI-FI NETWORK

(10 STEPS TO DIY SECURITY)

Authors : RAKESH M GOYAL & ANKUR GOYAL

Published in India by
Center for Research and Prevention of Computer Crimes
(<http://www.crpcc.in>)

SYSMAN COMPUTERS (P) LTD.
(<http://www.sysman.in>)
e-Mail: sysman@sysman.in

First Edition:
First Version (eBook) : Version 1.1 October 2008

Copyright and all rights reserved with
© RAKESH M GOYAL and
CENTRE FOR RESEARCH AND PREVENTION OF COMPUTER CRIMES

ISBN: 81-900385-6-7

Only usage rights of this publication are in PUBLIC DOMAIN for public usage. No one can claim any copyright except the author and publisher. Any part of this publication may be reproduced, printed and used for any type of public good with due credits to authors and publisher. For any type of reproduction, credits must be given to authors and publisher.

Index

1.	<u>Foreword</u>	7
2.	<u>Preface</u>	8
3.	<u>Acknowledgement</u>	9
4.	<u>Release Note and Disclaimer</u>	10
5.	<u>Unsecured Wi-fi</u>	11
6.	<u>What is Wi-fi</u>	14
7.	<u>Why WLAN (Wi-fi) are used</u>	16
8.	<u>Risks of using unsecured wi-fi network</u> (How wi-fi signal is detected)	17
9.	<u>How to secure wi-fi and protect ourselves</u>	19
	<u>Wireless network must be technically secured</u> (10 Steps to your security)	20
	<u>Necessary and indispensable Controls</u>	21
	<u>Desirable Controls</u>	28
	<u>User must be educated in security</u>	31
	<u>Security must be monitored for weaknesses and</u> <u>breaches</u>	33
10.	<u>Encryption</u>	34
11.	<u>Checklist to protect your wi-fi network</u>	35
12.	<u>How to implement these controls</u>	37
13.	<u>Some Indian Organisations, you must know</u>	38
14.	<u>Bibliography and useful web links</u>	39

DEDICATION

We dedicate this book to those enlightened and carefree people, who allowed themselves, to be made the victims of terrorist design, by allowing the terrorists to use their unsecured WI-FI connections.

**All it takes for evil to triumph is
for good people to do nothing.
(Edmund Burke)**

FOREWORD

Internet has left its imprint on the World stage – much in the manner of the Printing press and the Wheel. Internet has transformed the way work & business is done.

The benefits of Internet are manifold. In the same vein it needs to be emphasised that there is a flip side. As anonymity is the essence of Internet, it has led to a surge in undesirable activities termed as Cyber Crime. Security in the Internet is an issue that has gripped Policy Planners and Computer Professionals.

The Department of Information Technology, Government of India has a Project “Information Security Education & Awareness”. Shri Rakesh Goyal an authority in the field of Cyber Security is an integral part of the National Advisory Group guiding the Project.

It is heartening to note that Shri Rakesh Goyal has devoted his energies for the cause of prevention of Cyber Crime through his association with Institutions – Center for Research and Prevention of Computer Crimes and Sysman Computers Pvt Ltd.

I recommend his publication “Securing Wi-fi Network” for wide dissemination on the Net.

N. RAVI SHANKER
JOINT SECRETARY
DEPT. OF INFORMATION TECHNOLOGY
GOVT. OF INDIA

NEW DELHI
6.10.2008

Preface

Unsecured wi-fi network (genetically known as Wireless Local Area Network or WLAN) has become a national celebrity in vamp category due to it's misuse by terrorists, in the recent past.

Even otherwise, any open and unsecured node, especially wireless, is an extremely serious security hazard for any network, whether it is corporate, personal, home or small office user. The hacker (allow us to use the word - hacker for any unauthorized user or intruder or perpetrator or criminal or terrorist breaking into any network) get access not only to your internet bandwidth, but he (includes 'she' also, everywhere in this book) can send e-mails, download classified and/or confidential data/information, upload obscene material, hack into networks, initiate attack on other computers in the network or connected to internet, send malicious code to others, install a Trojan or botnet on the victim's computer to get long-term control of it through internet, etc. And this is not an exhaustive list but just a tip of the proverbial iceberg.

We strongly believe and also explained in this book that to help and protect any wireless network user, awareness is one of the utmost important key requirements. We felt a great need to create awareness to bridge the gap between secure WLAN, thus securing your IT critical assets on one side AND you become the victim of hackers and terror on the other side, using unsecured WLAN.

We are presenting this book to create user awareness by introducing wi-fi concepts and some basic guidance to make your wireless (wi-fi) connection / network reasonable secure. Most of these, a normal user can easily do himself with application of little common sense and investing his very minimal time and efforts.

We have attempted to achieve this limited objective in this book.

We are placing this book in Public Domain. The main reason to place the book in Public Domain is Corporate Social Responsibility (CSR). Please accept this book as our small contribution to fulfill our CSR.

Further, we discourage you to print this book in the interest of environment. In exceptional case, you may selectively print only – what is required. You may print "A quick guide to protect your wireless (wi-fi) network", at [page number 35](#), which may be used as your checklist and record of changes done in configuration.

Acknowledgement

I thank GOD to bestow the idea, perspective, direction, guidance, friends and strength to write this book.

I thank my parent, for their Aashirwad from their heavenly abode.

I specially thank Mr. N Ravi Shanker, IAS, Jt. Secretary, Department of Information Technology, Ministry of Communication and Information Technology, Government of India, for writing the forward of this book. I further thank him for including this Book as part of '*Information Security Education and Awareness Project*' of Department of Information Technology.

I thank Dr. K K Bajaj, CEO of Data Security Council of India, a self-regulatory organisation established by NASSCOM, to critically review the book and make it a part of DSCI security initiatives.

I thank Dr. Gulshan Rai, Director-General, CERT-In, Mr. B J Srinath, Director and Mr. Omveer Singh, Jt. Director of CERT-In for their critical review and suggestions.

I thank Mr. Arjen de Landgraaf of Co-Logic Security Ltd (New Zealand) to review the book critically. A researcher and active speaker at IT-Security conferences around the world, Arjen is based in the Netherlands. He was Joint Program Chair at FIRST 2007 Annual Conference in Seville and speaker at South Korea, Middle East, Brussels, the Dutch Government (GovCERT) and SurfNet.

I thank Mr. Rajan Subramaniam, a NJ, USA based Information Security researcher and my professional colleagues Mr. Shashin Lotlikar and Mr. Anjay Agarwal for their reviews.

I thank Mumbai Police Cyber Crime Investigation Cell Police Inspector I/c Mukund Pawar and Inspector Sachin Kadam to provide their inputs and encourage us to write this book for social good.

I thank some more friends, officials and professional colleagues, who have reviewed the book but we are forced to not to reveal their identities, due to their corporate / official protocol.

I thank Vinod Jha for providing logistical support. I thank Kamal Singh for reviewing the book from layperson angle.

I thank various people, especially Guruji Bal Dhupkar, Mr. Shantilal Jain, Mr. Nitin Shah, Mr. D C Nath, Mr. B G Deopujari, Mr. Chirag Gandhi, Dr. Rajesh Vishwanathan, Mr. P M Nayak, Mr. Vaibhav Banjan, Mr. S Sampat, Mr. Ajay Kaushal, Mr. Vishwanath Shetty and Mr. Vimal Jain for their motivation to keep this book in public domain, so that maximum users can improve their security.

I must also thanks those TERRORISTS, who have put this subject at the national center-stage by exposing the wi-fi security vulnerabilities and thus, resulted into the idea to write this book.

Final thanks to my wife Rekha and daughter Pallavi for reading the manuscript and provide support to both of us.

- Rakesh M Goyal

Release in Public Domain and Copyright

We release and place this book in public domain with copyright reserved with us. Anyone can download, print, circulate and use this book without changing the contents and format, as it is published. Any matter from the book can be reproduced with due credits. Reproduction of any matter without due credits may invite due legal action under Copyright Act and all other relevant acts.

Disclaimer

Each location, situation and IT installation is unique and may need some specific requirements. This book is a compilation of general guidelines and principles to keep your home / small-business wireless (wi-fi) network reasonably secure. For corporate / bigger / complex WLAN requirements, additional security layers will be required, which may need expert assistance.

Security is the physical manifestation of your mental state. Security is not a one-time activity but a constant vigilance process similar to your home security. Security needs (a) one time initial security policy / planning and execution/implementation; (b) then constant monitoring of existing security, new threats and risks; (c) periodic review/revise of implemented security policy / plan addressing the feedback and new challenges and; (d) implementation of revised policy / plan. Treat this book as the starting point of your WLAN security. In some cases, you may need more than the security requirements suggested in this book, which might need some expert advise and assistance.

- Rakesh M Goyal
- Ankur Goyal

Version – 1.0 completed on
this Dusshera day
dated 09 October 2008

For suggestions and feedback, please contact –

Rakesh M Goyal
Center for Research and Prevention of Computer Crimes
Sysman Computers Private Limited, Mumbai
e-mail – wifi-book01@sysman.in / rakesh@sysman.in
web-site- www.sysman.in and www.crpcc.in
(Response / Feedback / Suggestions strictly by e-mail only)

Unsecured Wi-Fi

**Open door tempts even the hermit.
(Chanakya)**

Wi-fi networks are in the news in the recent past due to effective misuse of these by terror organisations. They have been misused as these wireless (wi-fi) networks have been installed unsecured. With the misuse by terrorists, unsecured wi-fi misuse has become national celebrity in villain and vamp categories.

In the recent past, we saw a high drama about unsecured wi-fi connection subscribed at his residence by an American IT trainer Mr. Ken Haywoods in Navi Mumbai. Terrorists used the Internet connection, to send e-mail to authorities and news-channels about the serial bomb blasts in Ahmedabad, just 5 minutes before the blasts. This strengthen the hypothesis that some members of terrorist organisation were located near the unsecured wi-fi network connection, at least till 5 minutes before the bomb blasts at Ahmedabad.

Then on 23 August 2008 evening, the above was re-enacted at the prestigious "Khalsa College" in Matunga, Mumbai. In this incident too the terrorists used the unsecured wi-fi connection of Computer Center of the College, to connect to their Laptop or similar device; then created a gmail account used to send a 7 pages long mail with an attachment, all in a span of 6-7 minutes.

Again, the same story was repeated, just 5 minutes before Delhi Blasts on 13 September 2008 when the terrorists used an unsecured wi-fi connection of a company at Chembur in Mumbai.

Currently, terrorists are not limiting themselves to use traditional methods. They are keeping pace with the time and change in technology. They are taking full advantages of technological advancement and loopholes in technological development and/or implementation. They integrate technology with their other terror techniques with finesse and many times with flawless precision. These people keep themselves up-to-date in technology evolution alongwith it's vulnerabilities, bugs and legal / law-enforcement limitations. Further, they also take advantages of the social tendency of cost cutting by technology providers as-well-as users to sacrifice security at the cost of national / social / individual security.

These are all well reported incidents due to their association with terror activities. These incidents are not new or innovative. As these

have been performed by terrorists, it puts the wi-fi insecurity at the center stage of crime drama.

The unsecured wi-fi exploitation by hackers is well documented since 2002, though it may be used before that. The hackers used to drive in various cities in US with laptops loaded with wardrive software to locate unsecured corporate wi-fi networks to tap into them. Once they find an unsecured wi-fi network, they would publicly declare the same by making a graffiti at the location with chalk, which says – “*Hey look. Here is free Wi-Fi*”. This was termed as “*warchalking*”.

Using this technique, the hackers used to connect their laptops to corporate networks to become part of that specific corporate network. Once connected, they have easily stolen corporate data, IPR, customer / employee / supplier data, cost-sheets, credit cards number and other critical and confidential information. In some cases, the data was also deleted or altered or added.

A recent indictment of a hackers ring in Boston, San Diego and New York in USA has illustrated – how easy it is for hackers to break wi-fi network and steal corporate and critical information. These people had stolen data from TJX, OfficeMax, Barnes & Noble and other retailers. Hackers have stolen massive over 40 million credit card details from TJX by using wi-fi hacking on unsecured wi-fi networks.

As per the prosecution, these hackers penetrated into company networks through connecting to open unsecured wi-fi connections. After that they had installed network-sniffing software and then transferred huge amount of data, mostly credit card related information to their own computers. They had sold part of the stolen data and used the residual data to manufacture duplicate Credit/ATM cards of their use, by which they siphoned millions of dollars at ATMs.

Gradually, they have become professional criminals with professional-quality tools and technical knowledge. Once they found a hole, they used custom-built software to capture credit card information and a well-organized international network to sell them.

In USA, the hackers have broken into the network of BJ's Wholesale Club in 2003; OfficeMax network in 2004 and Marshalls department store network in 2005. In the last case, they penetrated into their mother server, i.e. Marshalls' corporate parent, TJX.

All these hacks had the same pattern. Hackers drive around to find unsecured wi-fi network signal and then connected into it.

Similarly, the hackers also broken into networks of Barnes & Noble, Sports Authority, Boston Market and other chains. Their total booty is conservatively estimated to be tens of millions of dollars.

Recently, in September 2008, it was reported that the hackers penetrated into open wi-fi network of luxury hotels owned by the Thompson Group in New York, Los Angeles and Washington DC and stole the private e-mails sent by guests. The hacker then attempted to extort money from the hotel chain by threatening to publish the emails.

All this happed in US, due to unsecured Wi-Fi access points. Terrorists adopted the same methodology related to Ahmedabad / Delhi blasts in July – September 2008.

What is Wi-Fi (as defined by Webopedia)

(http://www.webopedia.com/TERM/W/Wi_Fi.html)

Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. The Wi-Fi Alliance, the organization that owns the Wi-Fi (registered trademark) term specifically **defines Wi-Fi as any "wireless local area network (WLAN)** products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards."

Initially, Wi-Fi was used in place of the 2.4 GHz 802.11b standard only, however the Wi-Fi Alliance has expanded the generic use of the Wi-Fi term to include any type of network or WLAN product based on any of the 802.11 standards, including 802.11b, 802.11a, dual-band, and so on, in an attempt to stop confusion about wireless LAN interoperability.

Wi-Fi works with no physical wired connection between sender and receiver by using radio frequency (RF) technology, a frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through air or space. The cornerstone of any wireless network is an access point (AP). The primary job of an access point is to broadcast a wireless signal that computers can detect and "tune" into. In order to connect to an access point and join a wireless network, computers and devices must be equipped with wireless network adapters.

Wi-Fi is supported by many applications and devices including video game consoles, home networks, PDAs, mobile phones, major operating systems, and other types of consumer electronics. Any products that are tested and approved as "Wi-Fi Certified" (a registered trademark) by the Wi-Fi Alliance are certified as interoperable with each other, even if they are from different manufacturers. For example, a user with a Wi-Fi Certified product can use any brand of access point with any other brand of client hardware that also is also "Wi-Fi Certified". Products that pass this certification are required to carry an identifying seal on their packaging that states "Wi-Fi Certified" and indicates the radio frequency band used (2.4 GHz for 802.11b, 802.11g, or 802.11n, and 5GHz for 802.11a).

SECURING WI-FI NETWORK

A common misconception is that the term Wi-Fi is short for "wireless fidelity," however this is not the case. Wi-Fi is simply a trademarked term meaning IEEE 802.11x.

Why Wi-fi (WLAN) are used

New technology walks on the corpse of old technology.

WLAN and wi-fi are gradually becoming popular over cabled networks.

WLAN has numerous advantages over the wired LAN (Local Area Network). Some of these are –

1. WLAN can be set without using cabling under the floor, on the wall, etc. Thus, it is faster and cheaper. The aesthetics and appearance of the place is also neat.
2. User devices like Desktops, Laptops, PDAs, etc. can be used at any point in the office, home or building. You need not to go to the Computer desk. The computer can be used anywhere within the signal range. Laptops etc can be taken from office desk to conference room OR living room to bedroom without loosing network connectivity.
3. The devices can be used, where cable cannot reach like outdoors, gardens, airports, hotels, etc.
4. Wi-fi is a set of Global standards. Same wi-fi user can work in different locations, different countries without any compatibility issues.
5. Wi-Fi uses unlicensed radio spectrum. It does not require any regulatory approval for any individual user.
6. Wi-Fi products are easily available in the market. Different brands of access points and network interfaces are inter-operating at defined global standards.
7. A host of access points and network interfaces support good amount of encryption to protect them from hacking and interception.

Range Limitations –

Wi-Fi networks have limited range. A typical Wi-Fi home router using 802.11b or 802.11g with a stock antenna might have a range of upto 32 m (120 ft) indoors and 95 m (300 ft) outdoors. Range can also vary with frequency band. Wi-Fi in the 2.4 GHz frequency block has slightly better range than Wi-Fi in the 5 GHz frequency block. Outdoor range with directional antennas can go upto several kilometers or more with line-of-sight.

Risks of using unsecured wi-fi network

How wi-fi signal is detected

Nowadays, hackers use the devices called Wi-Fi detector. It is the device used to detect and analyze the presence of Wi-Fi networks (hotspots). A Wi-Fi detector can be a standalone handheld device that requires batteries to operate or a USB device that can be connected to any computer or laptop or PDA or even wi-fi enabled mobile-phones or communicator.

A typical Wi-Fi detector will show (a) the presence of a signal, (b) detect type of encryption (WEP or WPA), (c) wireless standard (802.11b or 802.11g) as well as the (d) relative signal strength. This information obtained about is usually shown on the device's built-in LCD display screen. This type of devices has many different names, usually based on the brand name of the product itself. Alternative names for a Wi-Fi detector include Wi-Fi scout, Wi-Fi finder, and hotspot detector.

Along with Wi-fi detectors, hackers also use Yagi antennae or wireless repeaters or expanders, which increases the effective range of signal without getting connected to the network or *Access Point* (AP) via cables. The device simply needs to be within the range of any AP signal and it will bounce the signal out to a remote wireless device.

This hacker does not leave a trail of footprints for the investigators to arrive a logical conclusion. The audit trail ends at wi-fi *Access Point* (AP). Anyone with wi-fi connectivity in his computer / laptop / mobile-communicator can connect to this unsecured AP. The criminal may be sitting pretty in a nearby building or nearby flat or even in a car/van, parked nearby, within the signal range of wi-fi AP.

Once the connection is established, the criminal can send mails, download classified / confidential stuff, upload obscene material, hack into network, initiate attack on other computer in the network or connected to internets, send malicious code to others, install a Trojan or botnet on the victim's computer to get long-term control on it through internet, etc.

All these criminal acts will naturally be associated with the legal user of wi-fi router / AP. It is up to the legal user to defend himself to prove that he has not been involved in this/these acts, which may be costly, time consuming with legal and law-enforcement tangles and most of the times unachievable too. How to prove innocence? In

some cases, the victim, whose unsecured wi-fi terrorists have used, have undergone Narco-test and/or brain-mapping tests.

It has been argued by many experts that even though the legal user has not done any of these acts, he can not be acquitted as he should be considered equal to assisting the hacker or criminal or terrorist as an accomplice or collaborator in the crime, as he has allowed the hacker or criminal or terrorist to use his facility at the cost of organizational or national interests. In other words, *ignorance is not bliss*.

In the Mumbai cases, i.e. (a) Haywood case and (b) Khalsa College case, where terrorists used unsecured wi-fi networks, the investigative agencies had questioned neighbors of Mr. Haywood; and all 55 people, who had authorised access at Khalsa College.

Using an unsecured wi-fi connection can be broadly equated to driving a car without reasonable security devices like brakes, headlights, horn, dashboard without meters, etc.

A very rudimentary test to verify your wireless network is completely unsecured –

In the MS Windows environment, drag your mouse over the wireless icon in the bottom right corner (this corner is called the “system tray”) of your computer screen. This will display the name of your wireless network. If it shows the default name of the wireless network, as provided by the manufacturer, you have high probability of having an unsecured network. In unsecured network, this may be the make or model of your wireless router and you may see something like, "Linksys" or "D-Link" or "Default (Unsecured)". [Linksys, 3Com, Netgear, D-Link, Microsoft Broadband are brand names of some wireless (wi-fi) routers]. This test is like a Thermometer test, which measures the body temperature only. Higher body temperature means some abnormality but cannot diagnose it. At the same time, normal temperature does not mean that all is normal.

Basic symptoms of wireless network being hacked if

1. the download or browsing speed is slow,
2. the connection breaks frequently,
3. the usage bill escalates, in case you use chargeable download,
4. there are Unusual log activities.

Please note that these symptoms may be due to some other reason like Virus, Malware, Computer / Router malfunction, glitch at ISP, etc. In case, you experience any/some of above, please investigate.

How to secure wi-fi and protect ourselves –

**Nothing is IMPOSSIBLE,
because IMPOSSIBLE itself says I M Possible**

The question arises – what a person must do to take care that the wireless network (wi-fi) is not misused by any anti-social, anti-national or criminal element or anyone else, may be insider, who is not authorised to access / use the network.

The question is: how to secure your wireless network or wi-fi network connection or access point (AP) –

There are three important aspects of wireless (or any) security –

- A. Wireless network must be technically reasonably secured.
- B. User must be educated in security.
- C. Security must be monitored for weaknesses and breaches.

Let us discuss these one by one.

PROTOCOL

Further in this Book, we have used following terminology, technology and geo-physical environment –

1. Wireless LAN or WLAN or Wireless network for wi-fi, as wi-fi is a sub-set of Wireless LAN or WLAN or Wireless network.
2. Router for both Access Point and Router.
3. We have given examples or setting information using mostly MSWindows-XP operating system, as it is most widely used OS, as we believe, thus cater to the largest user-group. This does not mean disrespect or disregard of other operating systems such as Linux or Unix or other flavours of Microsoft OS.
4. We have mostly quoted India-related examples, incidents, references, situations and solution. The main reason is that we are based in India and wi-fi security has become red-hot security topic in India. *The book is equally useful anywhere in the world, as in India. Technology does not have any nationality.* You can map your country's references, equivalent to Indian references, quoted by us. In this process of global assimilation, you also get introduced to Incredible India.

A. Wireless network must be technically secured

**Even if a snake is not poisonous,
it should pretend to be venomous.
(Chanakya)**

All easily available network security technology must be deployed to secure the network. The wireless router or wi-fi Access Point (AP) incorporates lot of security features, inbuilt into it. The job of the user or the person, who has installed it, is to use these security features as per the security policy or the minimum requirements of the situation.

We describe below '**10 steps to Wireless Security**', one should take to improve the security of the home wireless Network and Router / AP –

In the following 10 steps, you can secure your wireless (wi-fi) network, mostly by your self. We do not claim that your wireless network will be 100% secure but with proper implementation of these 10 steps, your wireless network will be reasonably highly secure, similar to you are securing your home, when you lock the door and close the windows and ventilators; and it will not easily be penetrated by hackers.

Necessary and indispensable Steps

**The biggest guru-mantra is:
Never share your secrets with anybody.
It will destroy you. (Chanakya)**

Step – 1 : Change Router administrator Usernames and Passwords

Issue : The Username and Password are required to allow your computer / device to connect to wireless router and get access to the network. All hardware manufacturers usually provide default Usernames and Password combination, when you buy / get and install their wireless (wi-fi) Router or AP. You, as an alert user, are required to change this Usernames and Password combination. It is normally seen that very few people change this Usernames and Password combination. Some studies find that over 90% users use their wireless router with Usernames and Password combination, as default set by the manufacturer.

Following are the Default Username and Password for some commonly used routers –

Router	IP Address	Username	Password
3Com	http://192.168.1.1	admin	admin
D-Link	http://192.168.0.1	admin	
Linksys	http://192.168.1.1	admin	admin
MS Broadband	http://192.168.2.1	admin	admin
Netgear	http://192.168.0.1	admin	password

Risk : The default Usernames and Password combination are available in public domain, as shown above, thus known to hackers. Further, these are easily available on the internet. Hackers can effortlessly break into your wi-fi network by just knowing the brand and model of your wi-fi router. Even beyond that hackers can change your Username and password and not only control your wireless connection but deny you the usage of the network itself.

Mitigating the Risk : You must change the Username and Password for your wireless router immediately after the installation and first login. Once you type the address, as given in above table in your browser window after installing wireless router, the browser will show a password screen. You need to enter the above stated default username and

password, till you change the same. This first login will be with default password, which is also defined in the instruction manual. After this, the setup process starts. In this setup process, you will find an option to change your Username and Password. Using this option, change the Username and Password and do not forget to save the new settings.

Further, please make sure that the Password must be difficult to guess. It should not be your name, spouse name, children name, date of birth date, car number, phone number or flat number, etc. which are the first guesses of hackers. Further, the Password should not be a simple English word like computer or password or airplane, etc. as hackers also use a technique called 'dictionary attack', which means hackers run a program that tries common English words as passwords. You must make sure that the password must be a combination of alphabets, special characters and numbers and should be minimum 8 characters long. For example a real difficult-to-break passwords can be Ahr34\$d92 or 7%rEc@bb, provided you could remember.

Step – 2 : Upgrading your Wi-Fi Encryption

Issue : Information flow between your wireless router and computer /device is encrypted.

The old encryption standard - called '*Wired Equivalent Privacy*' (WEP), is claimed to be broken within few seconds, even if you use a complex passphrase. WEP encryption is now so simple to hack that it is considered as slightly better than no encryption at all. A weak encryption means it can be easily broken within manageable time, i.e. few seconds or minutes.

'*Wi-Fi Protected Access-2*' (WPA2) encryption is highly difficult to break, even with the help of highly powerful computers. The usage of WEP encryption may be due to (a) either the user is unaware / not bothered of the problem or (b) feel technology to upgrade to WPA / WPA2 is complex.

Risk : Unfortunately, statistically a very large percentage of wi-fi users are still using default configured WEP encryption technology to encrypt their information, even though highly superior WPA and WPA2 encryption standards are easily available. If the encryption is weak, a hacker can easily break the encryption, tap into the network and monitor all data flow and your activities. When you enter confidential information such as bank or stock-trading information into a web page,

that hacker can steal that information alongwith your login Username and Password and thus he has stolen your identity.

Mitigating the Risk : The only solution, with the current technology, is to upgrade your Wireless encryption to WPA or better ideally to WPA2. (Even TKIP of WPA has been reported to be cracked recently).

For adding WPA2 encryption protection to your wireless network, you may be required to update the operating system and drivers in your computer. These are very minor tasks but provide enormous security. If you are using Windows XP, you may be required to download and install Microsoft's WPA2 hotfix.

For example MS-Windows XP WPA2 Hotfix update is KB893357 and is available at
<http://www.microsoft.com/downloads/details.aspx?FamilyId=662BB74D-E7C1-48D6-95EE-1459234F4483&amp;amp;amp;amp;amp;amp;displaylang=en&displaylang=en>

Or

<http://support.microsoft.com/kb/893357>

You may also need to update your wireless card driver (The driver is a software program, normally of small size). This driver either (1) may be available in Windows installation CD or (2) can be downloaded from the website of card manufacturer.

After downloading these updates, if required, these need to be installed.

Once your Operating system (we are discussing Windows XP here) and wireless card are up to date for WPA2, you need to log into your router's administration page through your web browser (this is the page, you logged in, to set up the wireless router for the first time with the address and password discussed in Step -1). Once logged in, you need to change the security settings to "WPA2 Personal" and select the algorithm "TKIP+AES". Then, you enter your password into the "Shared Key" field and save your changes.

Step – 3 : Disable Auto-Connect Feature to any open Wireless Networks

Issue : Most computers / devices provide a setting that will connect your computer automatically to any available open wireless network without notifying you. Normally, this isn't the default setting, but most users select this automatic connection setting as it enables connecting easier and faster when they travel or connecting at a friend's house. People commonly use 'connect automatically' feature to their own networks too. This is normally done for convenience, as most people do not want to manually enter the name of their wireless network and the password every time they log on.

Risk : If you connect your computer / device to every available wireless network automatically, you may get connected to some dummy wireless networks, which is designed specifically to catch unsuspecting users and hack their computers.

Similarly, if you connect automatically to your own wireless networks by not manually typing your network name and password, you are inviting hackers to hack your network. This is compounded as a large majority of users have not changed their default wireless name and password. Further, it is easy for a hacker to create a dummy network entitled "Linksys" or "Default", then enjoy the fun to watch about 90% of computers automatically connect to the network.

Risk Mitigation : Disable the feature 'connect to available wireless networks automatically' in your Network Connections window.

If you don't want to manually type the name and password of your wireless connection every time, you can use save option (for name and password) in the connect box.

Step – 4 : Enable and use firewall

Issue : Like national security, your IT security also has different layers of security. No single layer of security is enough to survive various types of attack. So, you need to add as much layers of security, as available and as easily possible. Adding layers of security will ensure that attacks by hackers, Trojans, spyware and malware are resisted and mostly defeated. You have two additional and important layers

of security at your command. These are the router firewall and your computer firewall.

Risk : Routers come with a built-in firewall. Mostly, it is seen that this firewall is either not used at all or disabled / turned off.

Risk Mitigation : Enable your router's firewall. Enable all related built-in security features in the firewall. These features include to block anonymous internet requests or pings; browsing unwanted websites; defining MAC addresses; protect from malware and spyware; etc. This additional layer of security will protect your wi-fi network not only from hackers and unwanted preying eyes but also from malicious software. Here you may need to define your security policies and then implement these policies in your firewall. You need to consult the firewall section of instruction manual of the router.

Step – 5 : Positioning of the Router or Access Point

Issue : Wireless signals do not obey physical boundaries, created by you and us. These signals don't understand where your house ends and where your neighbour's begins. Thus wireless signals go beyond the area and range of your control. All wireless routers have a signal range. Mostly, this range is about 100 feet radius. This can be visualized as a sphere or globe of this radius with wireless router or AP at the center. The whole inside of globe is within signal range. This means that the signal can be picked up in all directions (including up and down) up to 100 feet distance from the router. In certain routers, it can even be further. This wireless signal leakage gives hackers and neighbours the opportunity to find your wireless network and attempt to access it.

Risk : If the wi-fi router is placed near the window, the signal will definitely leak outside through the window and will invite hackers to hack into your network. Ideally, no signal should leak outside. But in small houses or offices, this may not be possible. A small amount of weak signal leakage outdoors may be acceptable, but it is utmost important to keep this leakage as minimum as possible. It is obvious that the further your signal reaches, the easier it is for hackers to detect and exploit.

Risk Mitigation : You need to plan carefully, where to install your wireless router. It should be installed in such a way that

the signal either does not leak outside or the leakage is minimum. You need to place the wi-fi router or AP in the center of the home rather than placing it near the windows or doors or ventilators. If you live in apartment block, you need to consider that the signal can leak through walls, floor and roof apart from doors and windows to adjoining or upper-floor or lower-floor apartments. If you live on top floor, placing near the roof will be better option. Similarly, for a ground floor apartment, placing router near floor will be better. Signal becomes weak depending upon (1) distance it travels and (b) material it passes through such as walls, metal, etc. Metal is one of the strong obstacles for wireless signal. You may consider to place the wireless router / AP in the metal closet or cupboard. This will reduce the signal strength. You can also use Aluminum foil at the windows or doors to reduce the strength of signal. However, you need to consider the aesthetics of the house.

Step – 6 : Turn the Router OFF, when not in use

Issue : Most of us keep the computer and router powered-on for 24 hours. In some cases, even if the computer is shutdown, the router is kept power-on. A power-on router keeps on emitting signals and any one can establish a connection with your network. It is also seen that when people go on vacations or go out for few days, the router is left powered-on.

Risk : A power-on router is an open invitation to hackers to connect to your wireless network. If the computer is also power-on, it is further bonus to hackers to enter into your computer and do whatever they like. If you are using your computer and network, and some one connects into your network, you may experience some degradation in speed or may face disconnection. This is one of the earliest and important symptoms. So, hackers avoid connecting, when the network is in use. But, when you are not using it and your router and/or computer is power-on, the hacker has a field day. Would you like the hacker to enter your personal and private space?

Risk Mitigation : The simplest, non-technical and only remedy for this risk is to shut the power of the router (and computer), when not in use. You may have a separate on/off power switch for your wireless router. Turn the power on, when you or any authorised person want to use the computer and network. Turn off the power switch, just after the usage.

You need to develop this habit in the interest of security. Developing this habit itself will make you reasonably secure.

Step – 7 : Use static IP addresses in the devices

Issue : Most of the devices use dynamic IP addresses, when get connected. Devices on any network are identified as per their IP address. In the current widely used protocol IPv4 protocol, the IP address looks like xxx.xxx.xxx.xxx (in dot-decimal notation format), in which xxx takes the value from 0 to 255 (example - address column in the table given in step-1. 192.168.1.1 is the IP address to access the router). This combination of four 0-255 numbers has to be unique for every device in any network.

Risk : It is very convenient to define dynamic IP address assignment in any network. At the same time, this will also work to the advantage of the hacker. The hacker's device will also be assigned a dynamic IP address and get connected.

Risk Mitigation : You must turn-off Dynamic IP Address or "Obtain IP Address automatically" or DHCP (Dynamic Host Configuration Protocol) in the configuration. You can define the private IP address for each device. These private IP addresses may be like 10.xxx.xxx.xxx or 172.16.xxx.xxx and provide these private IP addresses in the configuration of wireless router. This way, you will be able to block undefined IP address connection.

Desirable Steps

These steps do not add high value to wireless security but make the job of a not highly skilled hacker, a bit more difficult.

Step – 8 : Changing the Default System ID (SSID)

Issue : When you set-up your wireless router, it came with a default system identifier (ID) called the SSID (Service Set Identifier) or ESSID (Extended Service Set Identifier). This ID is also commonly known as the name of your Wi-fi network.

Risk : Similar to Username and Password. discussed in step-1, wireless router manufacturers assign same SSID to all their devices, and many studies says that 90% of Wi-fi users do not bother to change this default setting. This means that 90% of users have wireless systems titled, "Default" or "LinkSys" or <model-name> or whatever the router manufacturer sets as the default name.

Though knowing the SSID does not allow a hacker to break into your wi-fi network, it is usually considered by hackers that the person has not taken due precautions to protect their wireless network. Thus these wireless networks are the most common targets of hackers. These default settings provides a clear-cut message to hackers about unsecured status of your wireless network and your carelessness towards security. Hackers are on prowl to catch Wireless networks with default names. These default SSID are first target of hackers.

Mitigating the Risk : Change the default SSID as soon as you install your wireless router and configure into the WLAN. This will not offer any effective protection from a hacker, but changing your SSID to anything other than default like "<your-name> Wi-Fi Network", will separate you from normally unprotected networks, and your wi-fi network will not be first choice to be attacked.

Further additional advantage, as a bonus, of having a wireless network with a unique name is that neither you nor your family will make the mistake of connecting through a neighbour's wireless network, which may expose your computers through their unprotected wireless network.

Step - 9 : Disable Public Broadcasting of your SSID

Issue : One of the features of the wireless router is to broadcast your SSID at a regular interval. This is to enable the connecting device to know the network to get connected. This may be a necessary requirement in a corporate or hotspot environment, where anyone can get connected to the network. But, in a home or restricted environment, this feature helps the hackers and even curious neighbours to get some information about your wireless network set-up.

Risk : The regular broadcast of your SSID over air informs the hacker that your network exists. This is the first step in surveillance of your wireless network by hackers. Why broadcast to the world that your wireless connection exists? Why not protect the network from curious eyes by stealth? You already know to access it anyway.

Risk Mitigation : Just disable broadcasting your network SSID by the router. This can be done easily by checking in the disable radio-button or box – “Wireless SSID Broadcast” or similar feature.

This will mean that hacker will just do not know that your network exists. It does not make any difference to your own connection. This is good enough for your personal or home usage. For corporate or bigger wireless networks, policies and planning will be different, based on need-to-know and need-to-access.

Step – 10 : MAC Address Filtering

Issue : Every network device (in this case, your wireless network card) has a unique identifier number called MAC (Media Access Control) address. During connection, each device checks and keeps track of MAC address of connecting device at other end. Thus, the wireless router knows the MAC address of the wireless network card of the computer or any other device, it gets connected. This feature can be used to restrict the devices to be connected to the wireless network. The wireless router has the facility to define the list of MAC addresses, which may be allowed to be connected. Thus, no device other than with declared MAC could be connected.

Risk : Though, theoretically, the feature is very powerful but MAC address is easily hacked and spoofed. The hacker can define the MAC address of your wireless network card in his device configuration and thus fool the router in believing that his device is the genuine device. Even than it is advisable to define your device's MAC address with router configuration process than leave it open to be connected by any one.

Risk Mitigation : If you do not know your wireless device MAC address, you can get the same easily in MS Windows environment. Click at <Start> in task bar. Click at <Run>. In the box, type cmd. It will show a black box, which is called command box. Type at the cursor – ipconfig /all (after c: (directory-name)>) and press <Enter> key. You will see heading such as

Wireless adapter xxxxxx

Physical Address : nn-nn-nn-nn-nn-nn (n will be between 0 to 9 or A to F – these are called hexadecimal numbers or hexa). This 12 hexa is your MAC address.

In the router configuration, there is a facility to restrict the usage to specific MAC address. Enter this MAC address there.

Limitations : The MAC address filtering is not an effective control as it is easily hackable by reasonable expert hackers. Further, expert hackers know, how to spoof your MAC address. Even than, this is better than no MAC filtering.

B. User must be educated in security

**Education is the best friend.
An educated person is respected everywhere.
Education beats the beauty and the youth.
(Chanakya)**

The biggest protection to any asset, whether IT or non-IT, including wireless equipment or network is **user awareness and user education**. When, some hacker or thief wants to steal your IT assets or misuse your network, ignorance is not bliss. This will not only lead to losses like financial losses, credibility losses, etc but may also lead to legal troubles.

Once you know the basics of IT Security and you know the risks associated in using any of the technologies, you yourselves will be alert to risk mitigation and secure usage.

For example, in case of electrical installation - to mitigate the risks of electrical fire, electrocuting, theft of electricity, leakage of electricity, short circuit in any electrical appliance, burning of electric equipments, low or high voltage surges, etc, you make sure that the wiring is of required specifications to take the load of current with proper insulation; switches of defined rating with quality mark are used; circuit breakers are installed; earth wiring is proper; there is no loose connection etc. Then you take care of not touching the hot iron, not burn candle or any fire near the electrical wire, not opening the plug-pin, etc.

Similarly, in IT environment, you must know that due to existing risk

- ❖ your data/information can be stolen or deleted or corrupted;
- ❖ your data and application may not be available to you, when required, temporarily or permanently, due to computer or network or hard disk failure;
- ❖ your bandwidth is stolen or misused;
- ❖ your computer is infected with virus / worm / spyware / malware / etc.;
- ❖ you are being spied or watched;
- ❖ your computer can be remotely controlled;
- ❖ your e-mails are read / monitored;
- ❖ your username and password are hacked and then misused to your detriment;
- ❖ you are lured and cheated by 419/phishing scam;

- ❖ your computer becomes part of botnet to do many illegal things; etc.

(This is just an illustrative list and not exhaustive list of risks)

The probability of anyone and combination of some of above risks is very high, if you simply do not know about these risks. Even if, you are aware and do not know, how to mitigate or manage these risks, they exist.

The probability of risks becomes reasonably lower only when

- a. you know the risk;
- b. aware of mitigation methods and;
- c. are vigilant in implementing these methods.

You yourself may not know technical details of risk mitigation details or may not have time for that but just awareness can get the work done by some expert in the field, to your satisfaction with mental peace and less legal problems. You must know, how to monitor – whether risk mitigation methods are implemented and working. And this is not a complex job.

Security is the physical manifestation of your mental state of vigilance against risks and threats.

Security is not a one-time activity but a constant vigilance process similar to your home security.

Security needs

- a. one time initial security policy / planning and execution / implementation;
- b. constant monitoring of existing security, new threats and risks;
- c. periodic review/revise of implemented security policy / plan addressing the feedback and new challenges and;
- d. implementation of revised policy / plan.

We have tried to achieve this awareness about wireless LAN or wi-fi security by this book.

C. Security must be monitored for weaknesses and breaches

**Know your enemy alongwith
his strengths and weaknesses.
(Chanakya)**

As discussed above, security is not one time job. Security is constant vigilance against threats and attacks. We can not eliminate hackers, pirates, thieves, etc. from the face of the earth. It is part of human civilizations from time immemorial. Ramrajya* is not possible in this age.

Once, we accept this paradigm, the only option before us is to protect ourselves, be secured and save ourselves and our assets including IT assets.

At national (or macro) level, army, navy, air-force, para-military forces and police forces are doing the same to protect national assets. These forces are deterrent against any kind of invasion, terrorism, internal crimes, etc. At micro level, we employ security guards; install latches and use locks; periodically check weaknesses like cracks in the building structure and attacks by pests and insects; manage electrical, gas and water connections, close windows and ventilators, when we go out, etc.

Similarly, we need to create mechanisms in cyber systems, which will constantly monitor the weaknesses, intrusions and breaches in cyber system and take corrective action. At macro level, various agencies are engaged in this. At micro level, we all need to control and manage our own cyber security.

Security has to be implemented once and thereafter constant monitoring and vigilance is required against any attack and weakness. Do not get scared, as most of these do not required 24 hours constant human monitoring. Most of these are automatic processes, especially in small and non-critical installation. In some critical installations and networks, such as Banking or communication, even 24 hours human monitoring is also required to address the attacks, faults and weaknesses identified by automatic systems.

(for non-Indian constituents)

* **Ramrajya** – The ideal public governance model of Lord Ram, in which there was no crime.

Annexure – 1

Encryption: There are a lot of different encryption algorithms available, each with advantages and disadvantages.

Static WEP (Wired Equivalent Privacy) is the first that come along with wireless encryption. It's an old standard but has two big disadvantages. It requires every user and device to enter a long hexadecimal string to make connections and it has become easy to crack. It is an obsolete technology. Despite its pervasiveness in nearly all wireless equipment, static WEP has reached the end of its productive life. Don't use it.

Dynamic WEP has been better than static WEP because it eliminates most of the conditions that make static WEP unsafe. 802.1X+EAP combined with WPA is better than Static WEP.

Dynamic WEP with 802.1X+EAP is a combination of protocols that addresses some of the flaws in static WEP. Dynamic WEP uses a combination of the 802.1X and EAP protocols to authenticate user and, optionally, computer, create a unique WEP encryption key for each associated computer and rotate all keys at a specified time interval.

Next generation encryption

WPA (Wi-Fi Protected Access) is the next generation of wireless encryption technologies. It's far more secure and easier to configure than WEP. Almost all network devices support this. WPA replaces WEP with an improved encryption algorithm called Temporal Key Integrity Protocol (TKIP). TKIP supplies each client with a unique key and uses much longer keys that are rotated at a configurable interval. WPA also includes an encrypted message integrity check field in the packet to prevent denial-of-service and spoofing attacks, something that neither static nor dynamic WEP can do. WPA operates both with and without a RADIUS server.

WPA-Personal uses a pre-shared authentication key that is configured on each device.

WPA-Enterprise uses 802.1X+EAP for authentication, but replaces WEP with the more advanced TKIP encryption.

TKIP of WPA has been reported to be broken recently.

WPA2 is the latest thing on the scene. It uses Advanced Encryption Standard for security. It can be used in Personal or Enterprise modes and has so far proven difficult to attack.

It is recommended to use WPA or WPA2 encryption.

(You may print this page and use it as the checklist and to keep track of changes made in configuration. Backside of this page is also left blank for this purpose)

**Once you start working on something,
don't be afraid of failure and don't abandon it.
People who work sincerely are the happiest.
(Chanakya)**

Checklist to protect your wireless (wi-fi) network

Mandatory Controls -

1. Change Default Administrator Passwords and Usernames
2. Turn on (Compatible) WPA / WEP Encryption
3. Enable Firewalls On Each Computer and the Router
4. Disable Auto-connect feature
5. Position the Router or Access Point (AP) Safely
6. Turn Off the power switch of Router/AP, when not in use
7. Assign Static IP Addresses to Devices

Desirable Controls -

8. Change the Default SSID
9. Disable SSID Broadcast
10. Enable MAC Address Filtering

Notes -

NOTES

How to implement these controls

All these above do not require any special knowledge. This is not Rocket Science. Even Rocket Science is easily available now ☺.

We have tried to provide reasonable information on implementation of above controls / steps. Further, all these are available in your Routers / AP's User Manual. Please refer the user manual of the device.

You need the User Manual of your Router or AP. Most of the user manuals are supplied in the CD alongwith the AP or router.

Just read this manual and configure your Router / AP. You need to know the usage of a browser (Internet Explorer or Firefox or Chrome etc.), which you have been using for all web browsing, as the configuration is mostly browser based.

If you do not have the user manual, ask your hardware vendor not only for this important document but other manuals and CDs, which comes alongwith almost all peripherals.

You may ask your service provider to set-up wireless (wi-fi) security. Depending upon your service agreement, the expert assistance may be chargeable.

In case, you need expert assistance, it is recommended to choose a CERT-In empanelled IT Security Auditor to get the expert advise. **CERT-In (Indian Computer Emergency Response Team)** is part of Department of Information Technology, Ministry of Communication and Information Technology, Government of India. Visit CERT-In website as <http://www.cert-in.org.in/> to get more details about IT Security and panel of IT Security Auditing Organisations.

Some of the CERT-In empanelled IT Security Organisations are-

1. Sysman Computers Private Limited (www.sysman.in)
2. AAA Technologies Private Limited (www.aaatechnologies.co.in)
3. ISAAC - isaac1@vsnl.com

Some Indian organisations, you must know
(engaged in Information Security Policy, Planning, Research and Monitoring)

A friend in need is friend indeed.

1. CERT-In (Indian Computer Emergency Response Team), Department of Information Technology, Ministry of Communication and Information Technology, Government of India - <http://www.cert-in.org.in/>
2. ISEAP (Information Security Education and Awareness Project) is a project of Department of Information Technology, Ministry of Communication and Information Technology, Government of India. For more details at <http://www.isea.gov.in> and <http://infosecawareness.in/>.
3. DSCI (Data Security Council of India) – A Self Regulatory Organisation (SRO) has been established by NASSCOM as an industry initiative to promote best practices and standards for data protection. For more details on DSCI – visit www.dsci.in
4. e-secure-it.com – having with Action Response Centers in India (Kolkata), New Zealand, Europe and the USA, specialised in providing online IT-Security news and Business /Industry related risk intelligence alerts on a global 24x7 basis.
For more details visit <http://www.e-secure-it.com/>
5. IITs at Mumbai, Delhi, Kharagpur, Guwahati, Chennai, Kanpur, Roorkee and IISc at Bangalore.
6. CRPCC (Center for Research and Prevention of Computer Crimes) promoted by Sysman Computers Private Limited (www.sysman.in) at Mumbai.

In case of a cyber crime incident, police assistance in India is available at

(Visit their website now and keep their contacts handy)

1. Mumbai Police Cyber Crime Investigation Cell (CCIC)
2. Thane Police Cyber Crime Investigation Cell
3. Navi Mumbai Police Cyber Crime Investigation Cell
4. Pune Police Cyber Crime Investigation Cell
5. Bangalore Police Cyber Crime Investigation Cell
6. Delhi Police Cyber Crime Investigation Cell
7. Chennai Police Cyber Crime Investigation Cell
8. Kolkata Police Cyber Crime Investigation Cell
9. CBI Cyber Crime Investigation Cell

Bibliography and useful web links

We acknowledge obtaining some help from following websites –
(All these web links are valid, till these are available and online)

<http://www.microsoft.com/athome/moredone/wirelesssetup.msp>

<http://arstechnica.com/guides/tweaks/wireless-security.ars>

<http://compnetworking.about.com/od/wirelesssecurity/tp/wifisecurity.htm>

<http://www.dailywireless.com/features/secure-wireless-lan-021507/>

http://www.webopedia.com/TERM/W/Wi_Fi.html

Quotes by Acharya Chanakya, one of the greatest political thinker of all times (350-283 BC). See - <http://en.wikipedia.org/wiki/Chanakya>

Following websites may be useful for further reading –

About Routers and their settings

<http://resnet.uci.edu/routersetup.asp>

http://www.microsoft.com/windowsxp/using/networking/expert/bowman_03july28.mspx

http://www.firewallguide.com/wireless.htm#Wireless_Security

Linksys configuration

<http://www1.linksys.com/support/troubleshoot/wireless/index.html>

About routers access information

<http://www.governmentsecurity.org/articles/DefaultLoginsandPasswordsforNetworkedDevices.php>

RSA survey on wireless security

<http://www.rsa.com/node.aspx?id=3268>

Continuing education and updates

For regular updates on Cyber security, subscribe to IT Security newsletter at

<http://groups.google.co.in/group/control-computer-crimes?hl=en>

Or for 24x7 action response intelligent alerts – subscribe at e-secure-it.com

About Data Security Council of India (DSCI)

www.dsci.in

DSCI is a Self Regulatory Organisation (SRO) has been established by NASSCOM as an industry initiative to promote best practices and standards for data protection.

The Mission of DSCI is to create trustworthiness of Indian companies as global sourcing service providers, and to send out a message to clients worldwide that India is a secure destination for outsourcing where privacy and protection of customer data are enshrined in the global best practices followed by the industry.

To achieve it's mission, DSCI has created three Working Groups –

1. **Surveys** - To understand the current status of data security
2. **Education** - To organize events, hold training programs, promote certifications
3. **Guidelines for contracts** - To create a repository of different types of contractual agreements

About Information Security Education and Awareness Project (ISEAP)

<http://www.isea.gov.in>

ISEAP is a project of Department of Information Technology, Ministry of Communication and Information Technology, Government of India to develop Human Resources and create awareness in the area of Information Security.

SUBSCRIBE FREE - IT Security e-Newsletter

Published 3 times a week, on every Monday, Wednesday and Friday. Over 600 editions since June 2005. 75000+ direct subscribers as on October 2008.

Details/Subscribe at

<http://groups.google.co.in/group/control-computer-crimes?hl=en>

About CERT-In (Indian Computer Emergency Response Team)

<http://www.cert-in.org.in/>

The CERT-In operates under the auspices of, and with authority delegated by, the Department of Information Technology, Ministry of Communications & Information Technology, Government of India.

CERT-In ROLES & FUNCTIONS

Roles

Reactive

- Provide a single point of contact for reporting local problems.
- Assist the organisational constituency and general computing community in preventing and handling computer security incidents.
- Share information and lessons learned with CERT/CC, other CERTs, response teams, organisations and sites.
- Incident Response.
- Provide a 24 x 7 security service.
- Offer recovery procedures.
- Artifact analysis
- Incident tracing

Proactive

- Issue security guidelines, advisories and timely advise.
- Vulnerability analysis and response
- Risk Analysis
- Security Product evaluation
- Collaboration with vendors
- National Repository of, and a referral agency for, cyber-intrusions.
- Profiling attackers.
- Conduct training, research and development.
- Interact with vendors and others at large to investigate and provide solutions for incidents.

Functions

Reporting

- Central point for reporting incidents
- Database of incidents

Analysis

- Analysis of trends and patterns of intruder activity
- Develop preventive strategies for the whole constituency
- In-depth look at an incident report or an incident activity to determine the scope, priority and threat of the incident.

Response

- Incident response is a process devoted to restoring affected systems to operation
- Send out recommendations for recovery from, and containment of damage caused by the incidents.
- Help the System Administrators take follow up action to prevent recurrence of similar incidents

Keep your thoughts positive,
because your thoughts become your words.

Keep your words positive,
because your words become your actions.

Keep your actions positive,
because your actions become your habits.

Keep your habits positive,
because your habits become your lifestyle.

Keep your lifestyle positive,
because your lifestyle becomes your destiny

(Swami Vivekanand)

About Sysman Computers Private Limited

(www.sysman.in)

- ❖ Sysman Computers Private Limited is incorporated in 1985.
- ❖ Sysman is managed by professionals and has associates and offices in various cities in India and abroad.
- ❖ Sysman has with professionals qualified as Engineer, CA, MBA, Lawyers, CISA, CISSP, CISM, CFE, CCCI and ISO27001 Implementers.
- ❖ Sysman has completed over 2000 confidential assignments in IS Security and related areas for 150 Client Organizations covering Banks, Financial Institutions, Government bodies, Public Sector Undertakings and Private Companies since 1991.
- ❖ Sysman have published the first Indian book on '**Computer Crimes**'; sponsored first book on '**Digital Signature**'; first book on '**Information Technology Act-2000**' and '**Case Studies on Information Systems Security in Banks**'.
- ❖ Sysman is one of the **IS Security Auditors empanelled by CERT-In, Government of India**.
- ❖ SYSMAN is the first Mumbai-based '**Associate Consultant**' of BSI India (part of British Standards Institution, UK) for implementation of Information Security Management Systems as per **ISO27001**.
- ❖ Sysman has been one of the **IS Security Auditors empanelled** to audit Certifying Authorities under I.T. Act, 2000 since 2001 till 2007.
- ❖ Sysman provide following services -
 - ❖ IS Security Risk Assessment (Health Check of IT Infrastructure)
 - ❖ Computer / Systems / IS Audit of IT Infra-structure, Procedures & Controls
 - ❖ Compliance with relevant Cyber Laws and I. T. Acts
 - ❖ IS Security Training
 - ❖ Audit / Testing and Validation of Business Automation Software and Other Application Software Suites
 - ❖ Evolving Information Systems Security Policy
 - ❖ Preparing IS Security Guidelines / Norms / Standards / Manual
 - ❖ Disaster Recovery / Business Continuity Planning
 - ❖ Secure Data Centre Design, implementation and Validation
 - ❖ Assessment of Network Security and Network Administration
 - ❖ Internet / Intranet Vulnerability Check and Penetration Testing
 - ❖ Testing and Validation of Database for Integrity, Confidentiality & Availability
 - ❖ Assessment of Security & Controls of Operating Systems
 - ❖ Forensics: Clinical Investigation of Computer Crimes/Frauds
 - ❖ Implementing Information Security Management Systems in accordance ISO27001
 - ❖ IS Audit of Certifying Authorities and Local Registration Authorities
 - ❖ Turn Key Consultancy to become a Certifying Authority (CA) for Digital Signature certification under Public Key Infrastructure (PKI)
 - ❖ Preparing organizations to operate in PKI regime - business environment of tomorrow

Contact : send e-mail at sysman@sysman.in.

About the Book

The book provides basic Do-It-Yourself (DIY) methodology to any individual/home user on securing his/her home wi-fi network. The book gives basic introduction of wi-fi, how wi-fi can be attacked and how to secure your wireless (wi-fi) network / router / Access Point, mostly by yourself, in simple and understandable language.

The same principles are applicable on corporate or non-home user networks but these need more professional approach and expertise.

About the Authors

Rakesh M Goyal is a Gold Medalist in both - Engineering and PGDM (IIM-Bangalore). He is a Chartered Engineer, Certified Fraud Examiner, Certified Management Consultant, Certified Computer Crimes Investigator, Certified Information Systems Auditor and Certified Information Security Manager. He has 34 years of experience with 17 years in IS Security. He has done/supervised over 2000 IS Security Assignments. He had convened committees related to IT Act, 2000 and has done consulting and Audit of Certifying Authorities (Digital Certificate providers).

His first book titled **Computer Crimes** was published in 1994; second on **Bank Computerisation** in 1996; third on **Digital Signature** in 2004; fourth **Demystifying Information Technology Act – 2000** in 2005; fifth book **Sankat Mochan Yojana** in 2006. He is the Director-General of Center for Research and Prevention of Computer Crimes and Managing Director of Sysman Computers P Ltd., India. He was awarded the "Young Consultants Award" in 1990 by CDC, Govt. of India. He has 6 patents and copyrights. He also has a black belt in Karate.

He publishes the IT Security Newsletter, which has over 75,000 subscribers as on this Dusshera day 2008. This e-newsletter is published three times a week, i.e. Mondays, Wednesdays and Fridays.

Ankur Goyal is an MBA from BC Canada after BMS from Mumbai University.

He is member of Executive Council of CRPCC. He is a computer user from the age of 3 years. He has over 3 years of active IT Security experience. He is a regular contributor to IT Security Newsletter. He is a Black Belt in Karate.