

Navi Mumbai Wireless Security Survey

Wireless Network Security Landscape of Navi Mumbai

Foreword

Wireless Networks are growing rapidly especially among home users and SME segment. However the limited awareness related to security concerns and information regarding securing them has exposed users to potential misuse of the unsecured Wireless Networks

With the ever increasing use of wireless technology, there have been growing concerns over the security aspects of wireless networks. There have been many media reports on potential misuse of unprotected wireless networks. The security risks have arisen due to lack of user awareness, inappropriate configuration or inherent limitation of technology used.

After successfully conducting the Wireless Security Survey in Mumbai, the Enterprise Risk Services division ('ERS') of Deloitte Touche Tohmatsu India Private Limited ('Deloitte India') has extended its survey to Navi Mumbai. It was carried out using WarDriving technique described in the methodology documented in Annexure I. We eventually plan to cover few more major cities in India and release an all India Survey. This Wireless Security Survey aims to increase wireless security awareness of the general public. We have included Wireless Network Security Good Practices in Annexure II. This survey should be read in conjunction with the disclaimer available on the last page of this document.

Deloitte India thanks Vijay Mukhi for his valuable inputs for carrying out the survey.

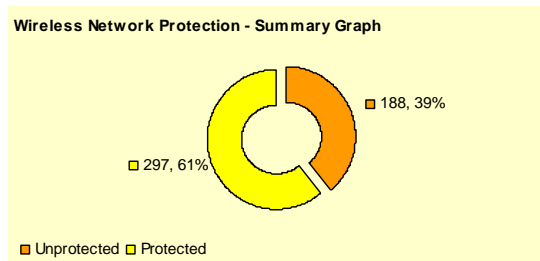
Executive Summary

A large number of wireless networks exist in Navi Mumbai with either limited or no protection that can be easily compromised. Basic configuration errors like using default manufacturer device names, device names that reveal company details, no or weak encryption mechanisms and default passwords, expose risk of access of such networks through these default settings using publicly available information.

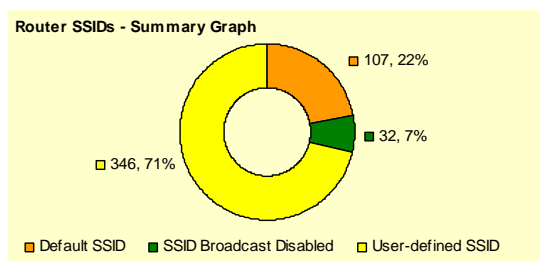
We could see over 450 wireless networks without any efforts with the help of wireless card features available in Windows™ Operating System (*Windows referred here in and after is a registered trademark of Microsoft Corporation*) which might include business as well as residential networks.

There was scope for enhancing the security of many of the wireless networks observed during the survey.

Of the total networks sampled, around 39% appeared to be unprotected i.e. not having any encryption on them.



Around 22% of wireless networks were broadcasting default manufacturer Service Set Identifiers ('SSID') as their wireless network names.

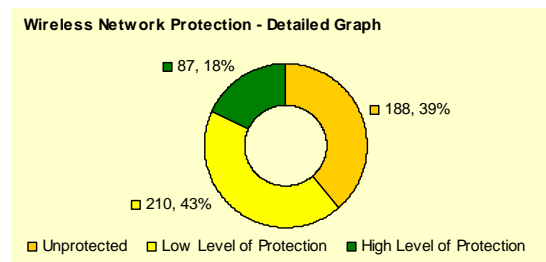


While we did not check whether default device passwords were in use, it is possible that default manufacturer passwords might also be left unchanged on some of these networks making them more vulnerable.

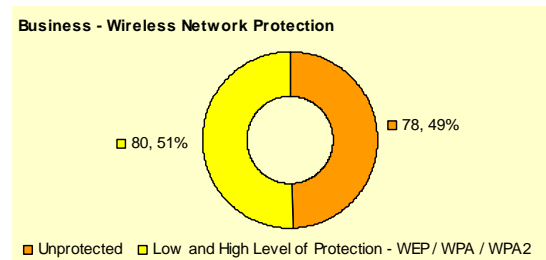
Survey Observations

Of the 485 wireless networks seen, 39% appeared to be unprotected i.e. without any encryption. 43% were using low level of protection i.e. Wired Equivalent Privacy ('WEP') encryption. Balance 18% networks were using the more secure Wi-Fi Protected Access ('WPA') or WPA2.

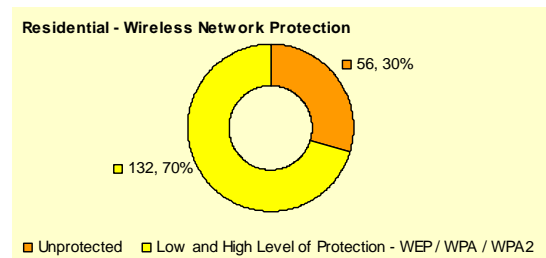
This makes 82% of the observed wireless networks being relatively easy to compromise.



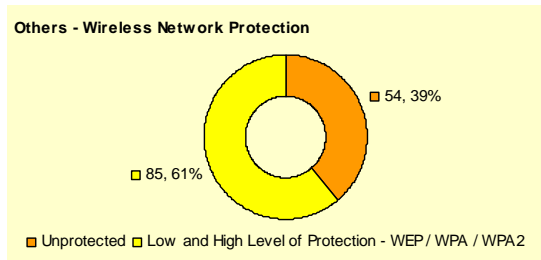
From nomenclature of the SSID broadcast, 158 appeared to be business wireless networks. Of these, 49% appeared to have no encryption at all.



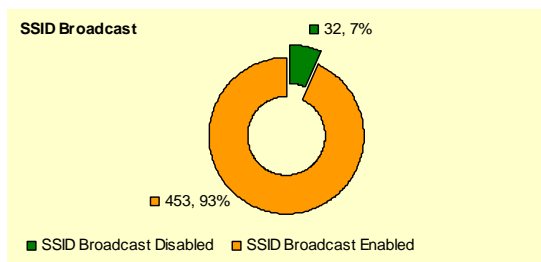
Another 188 appeared to be residential wireless networks based on nomenclature of the SSID broadcast. Of these, 30% appeared to have no encryption.



139 networks either had no SSID broadcast or could not be classified, based on the SSID nomenclature displayed, as being either business or residential. 39% of such networks appeared to be unprotected i.e. without any encryption.



Over 93% of the networks had SSID broadcast enabled. This might lead to easier compromise of the networks by guessing default information related to device password etc.



We noticed from SSID nomenclature, that the devices used to create wireless networks might be from different manufacturers.

The differing configuration interfaces of such devices and limited awareness on configuring such devices may be one of the reasons for limited or low level of protection and uniform implementation of security over these networks.

Our survey indicated that three makes had 96% of market share.

This also indicates that publicly available exploits or use of default settings of these devices would make the networks more vulnerable.

Conclusion

The rapid growth in wireless networks without commensurate increase in wireless network security awareness, both at homes and businesses, is indeed a growing concern. At the same time, there is significant scope for enhancing security over unsecure networks.

The major risks that one might be exposed to include:

- Unauthorized users might visit objectionable or banned sites, post objectionable material on websites, send threatening emails etc.
- The abuser may not be at risk because all this might be done from the owner's unsecured network. If there is subsequent criminal investigation, logs will indicate that the owner's IP was used to commit the illegal activity.
- Unauthorized users may sniff the bank account details, passwords, online transaction passwords, etc. of other users of the unsecured networks. This may cause monetary loss to the owner of such networks.
- Unauthorized users may gain access to unsecured network and surf the Internet free of charge. This will not only clog the network but also consume upload and download limits.

In keeping with our overall objective to increase the security of wireless networks deployed in Navi Mumbai, we have included Wireless Network Security Good Practices in **Annexure II**.

Annexure I – Methodology

The Wireless Security Survey was conducted using the methodology depicted below:



- **Area Selection**

Our effort was to obtain a representative sample of wireless networks deployed across Navi Mumbai. Key areas in Navi Mumbai were short listed on our understanding of Internet usage in the city. These included both business and residential areas.

- **Observation**

In this phase, we adopted the widely known “**WarDriving**” technique and we drove around selected areas using standard laptops having a wireless card which automatically provides information about wireless networks in the vicinity. No special hardware was used in this activity. The laptops had standard Microsoft Windows Operating Systems, manufacturer provided wireless card utilities and open source wireless network identification utility.

- **Data Analysis**

During this phase, we analysed and segregated data observed during WarDriving using appropriate data analysis tools. The wireless networks information was analysed for the overall city based on the following parameters:

- Encryption mechanisms that might have been implemented
- Classification into business and residential networks based on nomenclature of SSID
- SSID broadcast setting status
- Make of wireless devices used

- **Survey Results**

In this phase, we interpreted the data to the best of our ability / knowledge and keeping all information found confidential to understand the overall state of wireless network security in Navi Mumbai. The results of our survey are generalized and no individually identifiable information is presented in this document. The entire purpose of this survey and presentation of findings is to increase public awareness and enhance wireless networks security.

Some of the inherent limitations of a WarDriving survey are as follows:

- Networks 500 feet away from the car will not be detected i.e. typically above 6th floor
- Access points that are deployed behind thick walls may not be found

Some important precautions taken during this exercise include:

- No intentional attempts were made to connect to any wireless networks found.
- We have taken reasonable measures to keep information obtained during this survey confidential. All persons involved in the survey have signed non-disclosure agreements.

Annexure II – Wireless Network Security Good Practices

Most wireless access points by default have all the security options turned off. This means that anyone may use your wireless network without your knowledge and permission. The first thing that you must and have to do is turn lots of security options on in your wireless access point. People in a radius of 500 feet in all directions may also be held responsible, thus it is in your best interest to make sure that there are no unsecured wireless networks in your surroundings.

The following guidelines are recommended and provide suggestions to secure wireless connectivity for users who have installed a wireless network. You are strongly advised to protect your wireless network from unauthorized use and attempts to gather confidential information from your network devices.

- Ensure that your wireless access point has the latest firmware installed so that you can take advantage of more secure encryption mechanisms like WPA or WPA2
- Ensure that the SSID of wireless access point is changed from the default manufacturer set SSID so that no one can identify the type of access point that you are using and hence exploit any known vulnerabilities. Also ensure that your SSID does not reveal any information about you or your business
- Ensure that your wireless access point does not broadcast its SSID
- Ensure that the default administrator account password is changed so that no one can compromise your wireless access point
- Enable WPA2 on your access point with a passphrase having alphanumeric characters and special characters. This will make it difficult for anyone to crack the passphrase. If your wireless access point does not support WPA2, you must enable WPA or WEP
- Always activate MAC Address Filtering to provide a “trusted” communication channel to your wireless network
- Ensure that your wireless network is switched off when not in use
- Place the router in a physically secure place

Note: The above guidelines are general wireless network security good practices. Deloitte India is not responsible for comprehensiveness or accuracy of the above. You are strongly recommended to seek assistance from an IT Security Specialist or your IT service provider for expert advice. Also, kindly refer to your wireless device manufacturers’ instructions for implementing security.

For more information on the Navi Mumbai Wireless Security Survey, please contact us on ersindia@deloitte.com

Disclaimer

This document / publication contains general information only, and none of Deloitte Touche Tohmatsu, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

Survey users should be aware that Deloitte India has made no attempt to verify the reliability of such information. Additionally, the survey results are limited in nature, and do not comprehend all matters relating to wireless security that might be pertinent to your organization or residence. The information is provided as is, and Deloitte India makes no express or implied representations or warranties regarding the information. Without limiting the foregoing, Deloitte India does not warrant that the information will be error-free or will meet any particular criteria of performance or quality. Deloitte India expressly disclaims all implied warranties, including, without limitation, warranties of merchantability, title, fitness for a particular purpose, non-infringement, compatibility, security, and accuracy.

Your use of the information is at your own risk and you assume full responsibility and risk of loss resulting from the use thereof. Deloitte will not be liable for any direct, indirect, special, incidental, consequential, or punitive damages or any other damages whatsoever, whether in an action of contract, statute, tort (including, without limitation, negligence), or otherwise, relating to the use of the information.

If any of the foregoing is not fully enforceable for any reason, the remainder shall nonetheless continue to apply.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in 140 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's 165,000 professionals are committed to becoming the standard of excellence.

Deloitte's professionals are unified by a collaborative culture that fosters integrity, outstanding value to markets and clients, commitment to each other, and strength from cultural diversity. They enjoy an environment of continuous learning, challenging experiences, and enriching career opportunities. Deloitte's professionals are dedicated to strengthening corporate responsibility, building public trust, and making a positive impact in their communities.