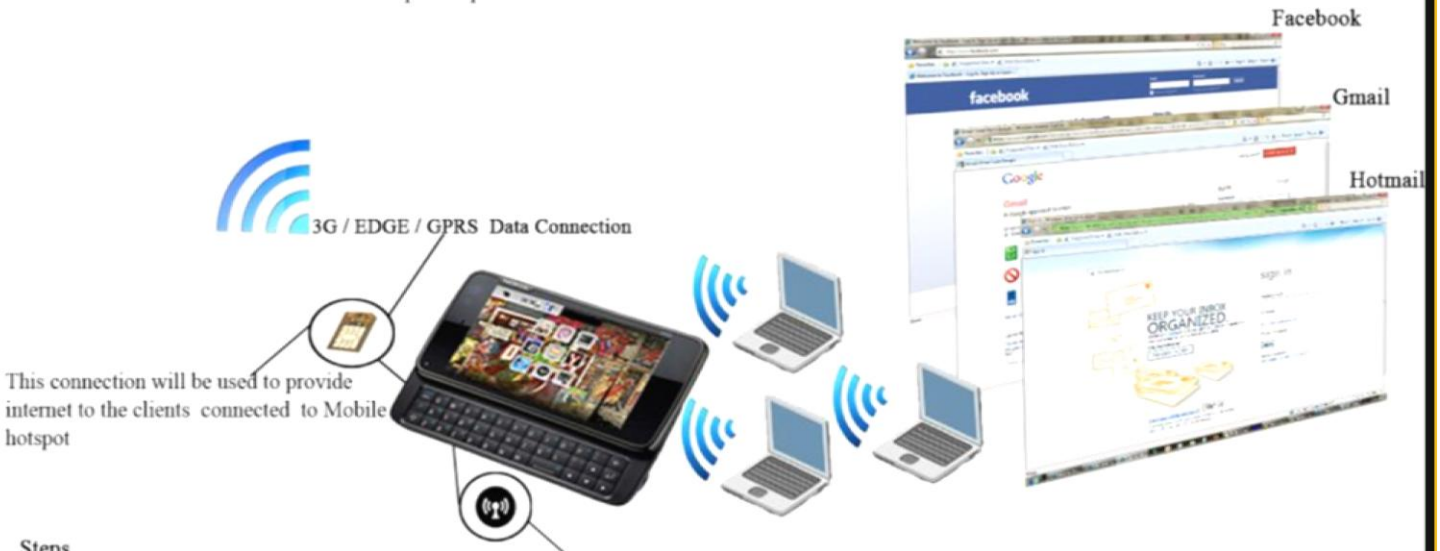
# Mobile Based MiTM Attack

A simple but powerful mobile based wireless network MiTM attack illustration




**Steps**

1) Spoof wlan0 mac using macchanger
2) Start mobile hotspot application
3) Start MiTM Script.
4) MiTM script will automatically save credentials in text file.

maemo **YAMAS MITM Script** Qt Mobile Hotspot

Bilal Bokhari
27 / OCT / 2011

## Introduction

If we look at the history of computer development, the computer developers/engineers just 10 years back did not have any clue as to how this industry is going to be, the way this industry we have today. The Computers and its applications nowadays are more powerful and much smarter than ever before. Computer applications are used in every industry like engineering, designing, music programming, web development etc which enables their users to come up with amazing products every day.

So far so good the story of the computer development sounds amazing but there is a problem with its development. When computer applications are developed, they are not particularly a complete perfect solution. They contain some flaws or bugs which can be exploited by computer hackers.

Normally when a computer "Exploit" or "Flaw" is discovered, it is either fixed quickly by its developers or it is exploited by the computer hacker. The computer exploits which are discovered by computer hackers before the applications developers are "zero day vulnerability" and if they are exploited then they are called the "Zero Day Attacks". It is just one explanation of how computer users can be affected, but there are other different types of computer based attacks that can disrupt computer communication flow. They can either be user information disclosures, DDOS attacks, Website defacements, Botnets, Trojans, Spywares, Email spam and etc. All these mentioned attacks utilize some applications, operating system and procedures which act as a platform in order to make them happen and to affect a targeted user. So it is clear that a platform and a target are required in order to launch a successful computer based attack.

Like computers, mobile phones of today have also redefined the way of communication. They are more like a personal computer rather than being just a simple two-way communication device. You no longer need to sit in front of a monitor screen just to check your facebook comments, emails, news, forums, blogs etc because all can be done right from your handheld device. Everyday more and more developments are made to make the user experience on mobile phone more pleasant than ever before. Mobile phones of today are more like the re-invention of the computer itself. They are small in size and are powerful enough to carry out tasks which earlier required a chair, table and a pc.

Just visualize for a moment, what if the same computer based platforms are provided in small handheld devices then what? Well, only the computer's history of development will be repeated but in a smarter way. The same pros and cons will be inherited. It also means that the same computer attacks will be executed right from the attacker's handheld device.

By now this mobile based computer attacks is not at all a new concept. There are a lot of platforms, applications and procedures available and developed for mobile devices to launch the same computer based attacks with the same amount of damage.

## Selecting a platform

In this article I will try to demonstrate a very simple mobile based MITM Attack which has very high impact on its targeted victims.

The platform I have selected is the Nokia's N900 which will be used to carry out this. The reason of selecting this handheld device is that it has almost the good amount of capacity, power and an excellent operating system i.e. none other than the Linux.

Only two applications I have used in order to make this work which is the "QT Mobile Hotspot" & "YAMAS". Both these applications are easily available from the maemo repository. I have also made sure that I have a primary internet connection from the 3G connection of my mobile SIM.

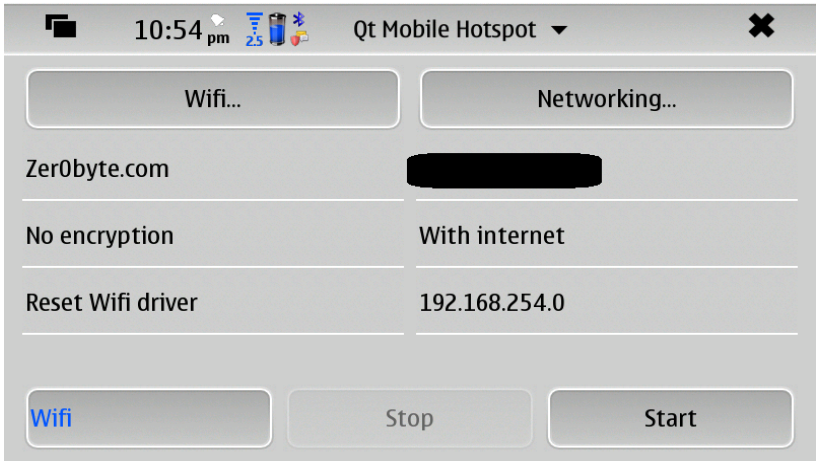
If you don't own an N900 mobile phone even then you can carry out this type of attack by using a very nice tool by the name "ANTI" (Android Network Toolkit) developed for Android devices from zimperium.com. This tool was also declared as a tool of the year on www.thehackersnews.com

## Launching the Attack

This mobile based MITM attack can be launched simply in 2 steps. Like I mentioned earlier, this very simple network attack but it has a very high impact on its victims.

Following are the steps.

1) To begin with, you have to start the "QT Mobile Hotspot" application. This will create a hotspot using 3G internet connection from your Mobile SIM.




There is something I would like to bring to your notice is that the internet connection will be shared from the mobile's internal WLAN card, by using this application you can also attach an external USB WLAN card as well which will also extend the possibilities.

2) The second and the last Step, just run the "YAMAS" (Yet Another Man in the Middle Attack Script). This is a very beautiful script designed originally by "**comax**" for backtrack and now it is available for devices running "Maemo" and "Android". This uses sslstrip to strip ssl off the traffic so that the credentials are transmitted as clear text and are saved in Text File.

3) That's all, Now Just wait for your victims to join your network and enjoy the show.

## Conclusion

I hope you enjoyed this simple mobile based demonstration of WLAN attack. The coolest thing about these types of attack is that they are very hard to notice. Just imagine you that you're getting credentials just out of thin air.

If you really liked my article please do visit my website @ www.zer0byte.com

## Useful Links

1) www.zer0byte.com (Bilal Bokhari's Website)
2) http://zer0byte.com/wp-content/uploads/2011/10/Mobile-Based-MiTM-Attack-Graphic-illustration-By-Bilal-bokhari.jpg ( Article's cover high resolution image )
3) http://comax.fr/yamas.php ( Download Link for YAMAS)
4) http://maemo.org/packages/view/qtmobilehotspot/ ( QT Mobile Hotspot Homepage)