60-564 Security and Privacy on the Internet
Dr. A. K. Aggarwal

Wireless Network Security featuring NoCat

NoCat is an Authentication and Gateway system serves wireless LANs

Student name: Aniss Zakaria
101131490

Wednesday, October 06, 2004

- **Introduction:**

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs. Wireless local area network (WLAN) devices, for instance, allow users to move their laptops from place to place within their offices without the need for wires and without losing network connectivity. Less wiring means greater flexibility, increased efficiency, and reduced wiring costs. Ad hoc networks, such as those enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices. Bluetooth functionality also eliminates cables for printer and other peripheral device connections. Handheld devices such as personal digital assistants (PDA) and cell phones allow remote users to synchronize personal databases and provide access to network services such as wireless e-mail, Web browsing, and Internet access. Moreover, these technologies can offer dramatic cost savings and new capabilities to diverse applications ranging from retail settings to manufacturing shop floors to first responders.

However, risks are inherent in any wireless technology. Some of these risks are similar to those of wired networks; some are exacerbated by wireless connectivity; some are new. Perhaps the most significant source of risks in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders, making it the logical equivalent of an Ethernet port in the parking lot.

Unlike wired networks, wireless networks use radio signals to communicate. Because radio signals travel outside your network, other wireless devices can pick up unprotected signals and either connect to your network (uninvited) or capture information being sent across it. For example, a network set up in your home might be accessible by your next-door neighbor.

Figure (1) [1]

Since this paper is not intended to discuss Wireless Network Security in great details I will mention briefly some tips, which can help securing any wireless network, I'll provide as well a tool, which can break it if available.

---

[1] Figure taken from
http://www.microsoft.com/hardware/broadbandnetworking/10_concept_wireless_security.mspx

- **Securing Wireless networks:**

These are general steps and tips to secure wireless network:

- **Change the System ID**: Wireless devices (Access Points) come with a default system ID called the SSID (Service Set Identifier) or ESSID (Extended Service Set Identifier). It is easy for a hacker to find out what the default identifier is for each manufacturer of wireless equipment so you need to change this to something else. Use something unique- not your name or something easily guessed.

  Tools used to discover SSIDs are NetStumber [2] (http://www.netstumbler.com) and SSID Sniff (http://www.bastard.net/~kos/wifi).

- **Disable Identifier Broadcasting**: Announcing that you have a wireless connection to the world is an invitation for hackers. You already know you have one so you don't need to broadcast it. Check the manual for your hardware and figure out how to disable broadcasting.

- **Enable Encryption:** WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) encrypt your data so that only the intended recipient is supposed to be able to read it. WEP has many holes and is easily cracked. 128-bit keys impact performance slightly without a significant increase in security so 40-bit (or 64-bit on some equipment) encryption is just as well. As with all security measures there are ways around it, but by using encryption you will keep the casual hackers out of your systems. If possible, you should use WPA encryption (most older equipment can be upgraded to be WPA compatible). WPA fixes the security flaws in WEP but it is still subject to DOS (denial-of-service) attacks.

  Tools used to crack WEP encryption are WEPCrack (http://wepcrack.sourceforge.net) and AirSnort (http://airsnort.shmoo.com).

- **Use MAC address based Access**: many routers and Access Points have the ability to control the clients that can use them. MAC addresses are tied to physical network adapters, so using this method requires a little coordination and maybe a little inconvenience for LAN users. And MAC addresses can be "spoofed" or imitated/copied, so it's not a guarantee of security. But it adds another hurdle for potential intruders to jump.

  Most of current NICs (Network Interface Cards) provide a feature where you can change your own MAC address without any third-part software, but in case your own NIC does not provide this feature, use SMAC (http://www.klcconsulting.net/smac), which allow MAC Spoofing.

Beside previously mentioned wireless specific security measures, its always recommended to use normal security techniques like firewalls, VPNs, strong passwords, change default passwords and patch/update your systems.

---

[2] NetStumbler consider one of the best wireless hacking tool, its not just SSID finder it can as well display wireless access points, channels, whether WEP encryption is enabled and signal strength. NetStumbler can connect with GPS technology to accurately log the precise location of access points

- **NoCat:**

As discussed earlier, the built-in wireless security mechanism, WEP (Wired Equivalent Privacy) has shown its weaknesses, problems and its disability to provide authentication and data integrity checks, more and more third-party tools where developed in order to bolster wireless networks security.

One of these tools is the open source program – NoCatAuth. Herein, a glimpse at NoCatAuth system as a tool for enhancing wireless networks security is given.

Captive portals became very popular among wireless community and hotspot operator, since they provide user authentication and resource management solutions. The authentication is usually done via a central authentication server and any connections beyond that server are prohibited.

A captive portal operates in two modes when dealing with wireless infrastructure: a closed captive portal and an open captive portal.

In closed operation mode, a user must supply authentication credentials before an access is granted. In open operation mode, the user must accept the terms of use before an access is granted – this mode is usually deployed in public wireless networks.

NoCatAuth is an open source captive portal, which operates in both modes and designed to provide high-level authentication system for gateways. It's written in Perl and designed to run under Linux. NoCatAuth is comprised of two major components: a gateway service and an authentication service.

The NoCatAuth authentication service component is responsible for presenting a login prompt and as a middle service between the gateway service and the user. If the supplied credentials match the user database, the authentication service sends a PGP singed message to the gateway service, which can now verify the authenticity of the message. To keep user privacy, the authentication credentials are supplied using an SSL web page.

The gateway service is responsible for blocking any data-flow (except the authentication service) until the user is authenticated. Once the authentication process is completed, data-flow is granted.

NoCatAuth becomes the credential backbone in wireless-based communities and networks. That's not surprising, due to its minimal requirements and its independence of any specific wireless technology. [3]

The NoCatAuth system is composed of a gateway server(s), authentication server, and an access point(s). A gateway server is a Linux router that is connected to an access point and issues IP addresses, throttles bandwidth, permits access to other networks, and times out old logins. An Authentication server is a Linux server that acts as a central authority by looking up a user's credentials in a MySQL database, notifying the gateway server of a user's status, and authorizing further access. It is the combination of the gateway and authentication servers that make NoCatAuth so user friendly yet secure and manageable.

---

[3] http://hosteddocs.ittoolbox.com/NoCatWireless.pdf

When a user attempts access on a Web page, a captive portal redirects them to a page that instructs them to enter a login and password. After correctly identifying themselves, a user is allowed access for a leased amount of time.

Installation and Testing

First of all, you have to create a gateway server, this can be either a separate machine other than NoCat Authentication or on the same machine, which I prefer, and I will use one machine to install both Gateway and Authentication servers.

Hardware Requirements

1. Any PC or Server with a 486 processor or better
2. Two network interface cards (NICs); one for connecting to the AP, the other to connect to your outside network.
3. A hard disk with at least 10GB
4. At least 256K of RAM

Software Requirements

1) RedHat 9.x Linux distribution with kernel version 2.4.x with iptables running. You need iptables running so that your two NICs can communicate with each other.
2) A Copy of NoCatAuth. (obtained from http://nocat.net/download/NoCatAuth) download a nightly build of NoCatAuth which is usually the latest (but unstable) version.
3) The following programs should be installed and configured correctly too:
    (a) Apache (http://www.apache.org)
    (b) MySQL (http://www.mysql.com)
    (c) Perl(http://www.perl.com) usually PERL comes already installed with any RedHat distribution.
4) You need to have DHCP (Dynamic Host Control Protocol) server daemon running on your machine. Sometimes DHCP can be served from your access point or another server.
5) If you plan on setting bandwidth limits on a per user basis, you will need to have 'tc' installed on your sever.
6) Optionally, you can install a local caching DNS (domain name service) server. There are instructions on how to install this online (http://www.linux.org/docs/ldp/howto/DNS-HOWTO.html). You should have the option to install it when you install RedHat 9.x from scratch.

Going through the steps of installing NoCat gateway and Authentication server may take several pages, so I'm going to direct the reader to some site which give great details on how to do so:

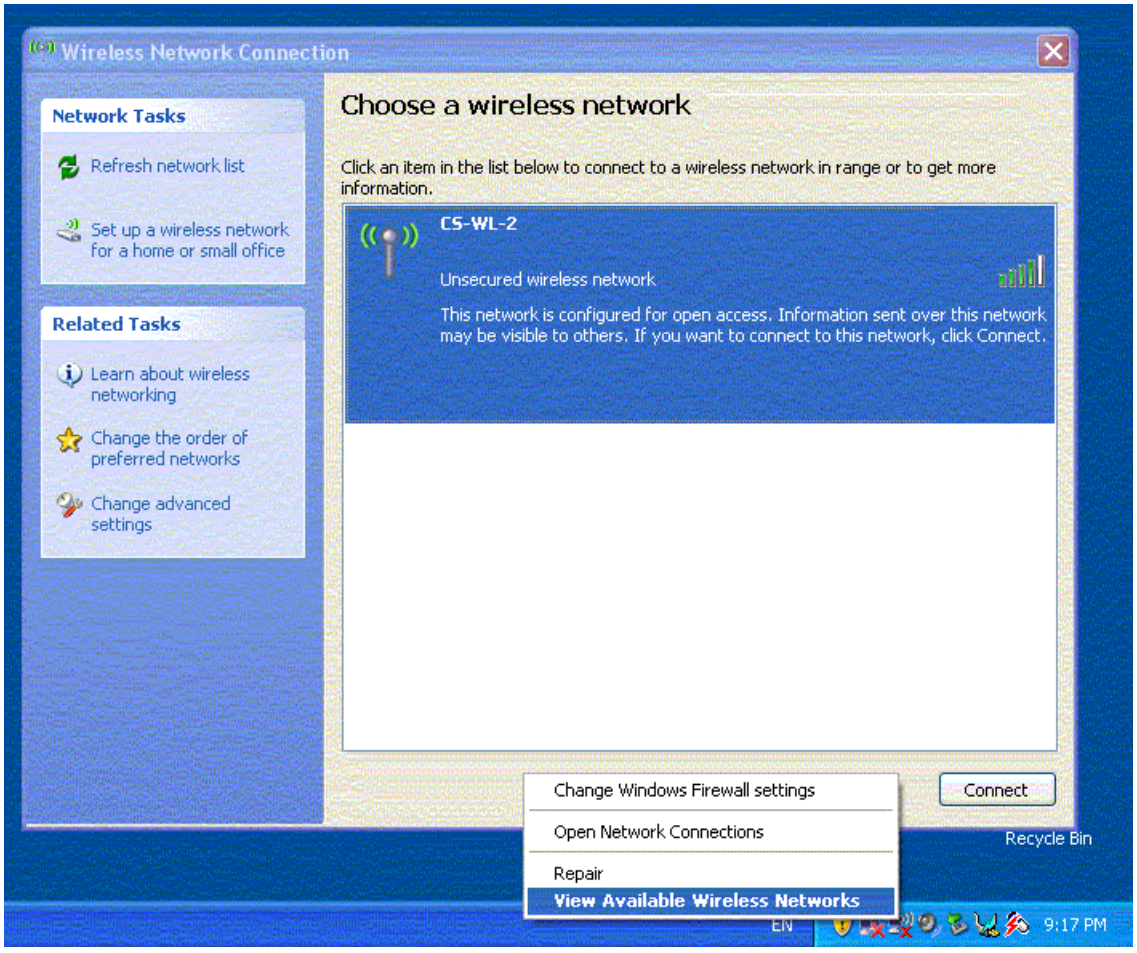
i) http://www.nocat.net (read through the mailing list, it's the best resource)
ii) http://nocat.net/moin/NoCatAuthInstallationGuide
iii) http://www.wi-fiplanet.com/tutorials/article.php/3111111
iv) http://www.wi-fiplanet.com/tutorials/article.php/3286631

Testing

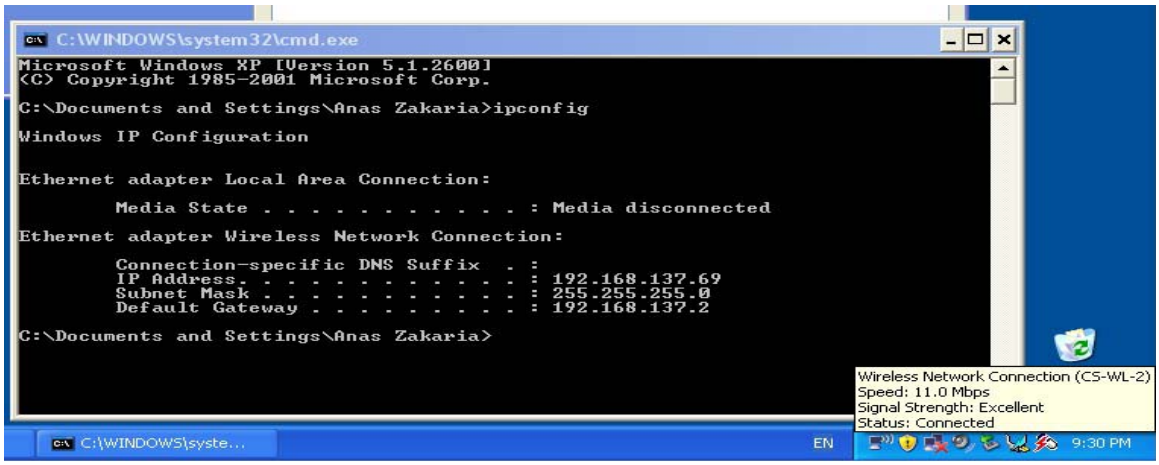
Once the server is up, now you can test it. Get any machine with wireless network interface, PC or laptop, place it in local wireless coverage area; if you have MS Windows XP you don't need to install any third party software to access wireless network, as it has full wireless capabilities build-in as well as the latest distributions of Linux. but incase you have earlier version of MS Windows, you need to install the software which usually comes with the wireless Interface card you bought.

I will explain how to connect using MS Windows XP with SP2 as an example.

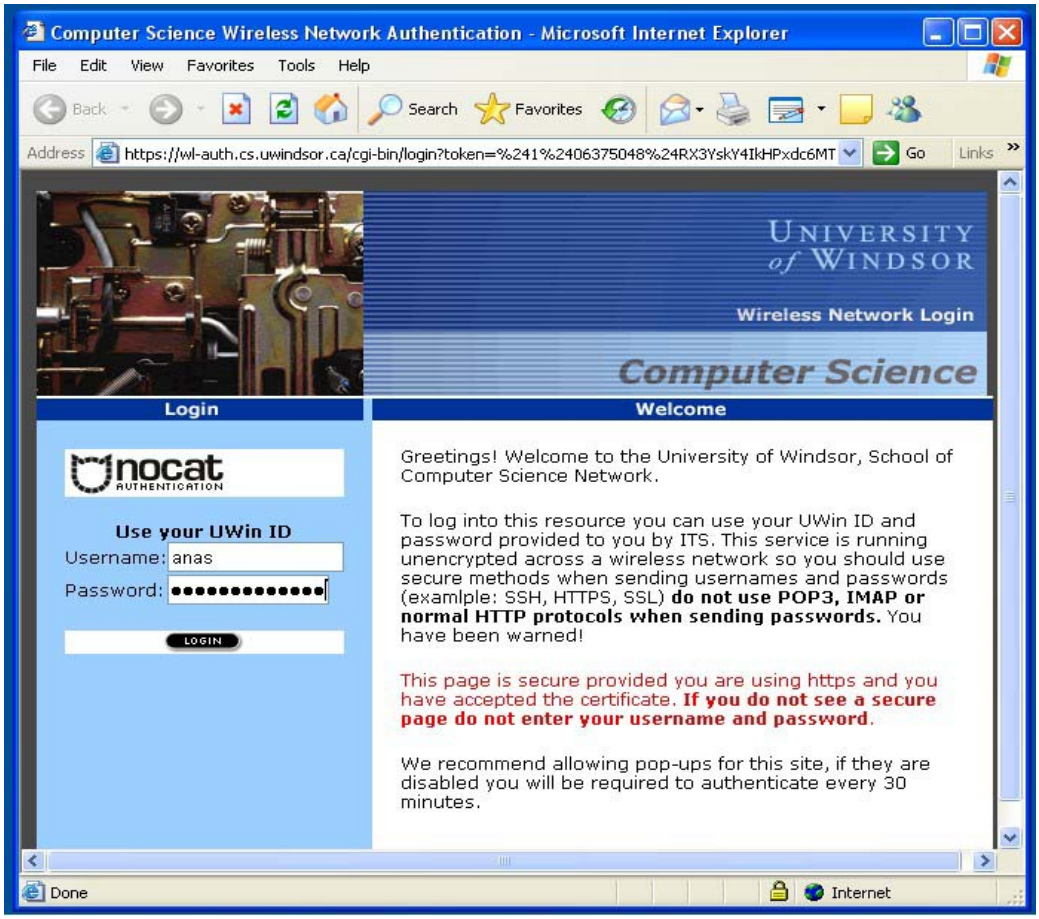
On the notification bar, right click on your wireless network interface icon and click on **View Available Wireless Network**, a windows will popup showing all available wireless networks in your domain. In our case, at school of Computer Science, we have one available network, which is **CS-WL-2**, click on it and then click on **Connect** button. It may warn you that this connection is insecure, just ignore it and click **Ok**, Windows will consider this connection insecure because the WEP encryption is not enabled.



By now, your computer should contact the DHCP server (which we created within the NoCatAuth server) and the client should get an IP, in our case the server will release a non-routable IPs from network 192.168.137/24.



Now, open your favorite browser, like Internet Explorer, it will direct you to the main page of NoCat Authentication page, where it asks for user name and password, in School of Computer Science, we have linked NoCatAuth Server with ITS main LDAP server, so Faculty, Staff and students can use their own UWINID to maintain consistency of passwords all over campus.

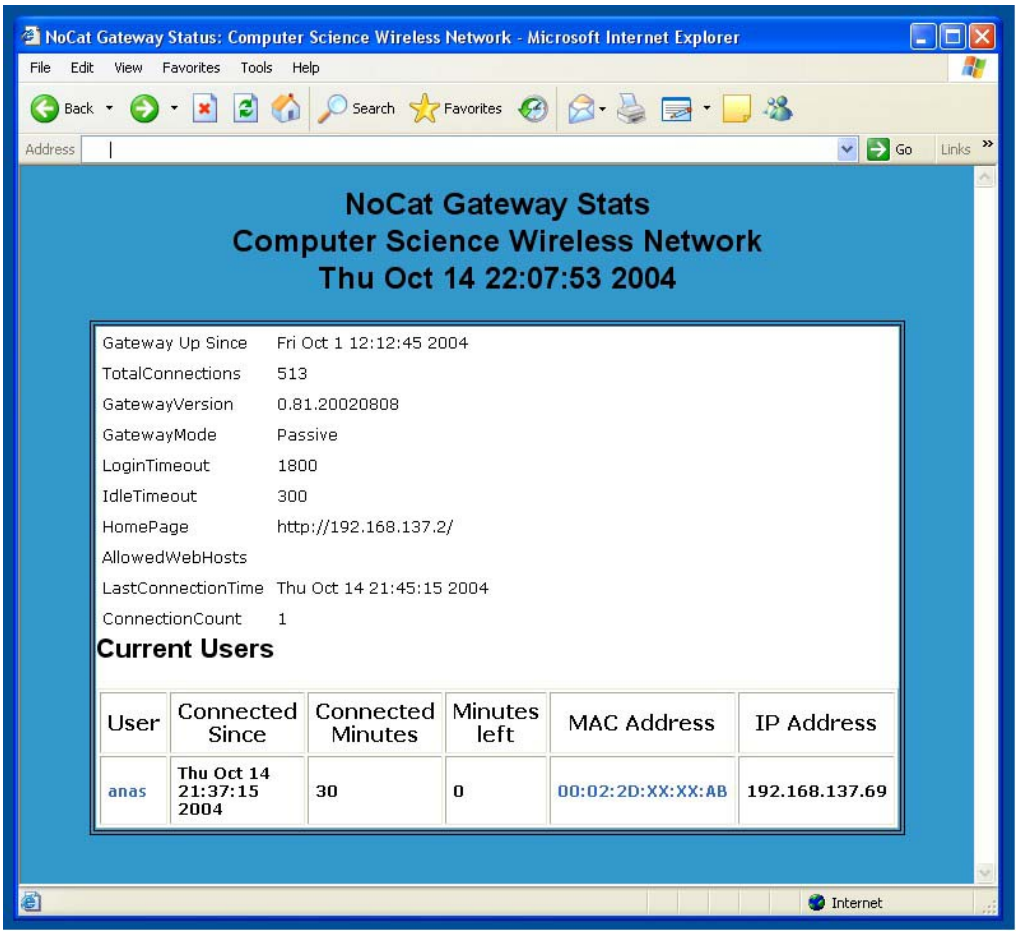


Please notice the yellow lock at the right bottom of Internet Explorer, as indication that this page is secure and your password will be encrypted before sending it over the network to the Authentication server, which will make it very hard (kind of impossible) for intruder to read your private information.

After providing username and password correctly, a welcome page to the NoCat network will greet you, this page will stay for 5 seconds, and then will direct you to default homepage.

- **Conclusion:**

Although NoCat will not prevent intruders from sniffing or snooping into your wireless network, but it will give the feelings that your network is under control, as no one can access it without authentication and it provide a status page where you can monitor all users connected currently to your wireless network with some extra useful information.



So, I believe, NoCat consider an important tool until they discover a very strong Wireless security mechanism which include stronger encryption algorithm other than WEP which has proven to be a breakable, insecure algorithm.

- **Reference:**

1. The Official website of NoCatAuth , http://www.nocat.net
2. NIST, Wireless Network Security, http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf
3. WiFi Planet, two articles about Installing and configuring NoCat gateway and Authentication server
    a. http://www.wi-fiplanet.com/tutorials/article.php/3286631
    b. http://www.wi-fiplanet.com/tutorials/article.php/3111111
4. Free Wireless Security tools from about.com, http://netsecurity.about.com/cs/hackertools/a/aafreewifi.htm
5. Wireless Network Security, Microsoft, http://www.microsoft.com/hardware/broadbandnetworking/10_concept_wireless_security.mspx
6. Wireless LAN Security FAQ, http://www.iss.net/wireless/WLAN_FAQ.php
7. Wi-Fi Protected Access, http://www.wi-fi.org
8. WPA Security Enhancements, Jim Geier, http://www.wi-fiplanet.com/tutorials/article.php/2148721