What is Bluesocket, NoCat Auth and Chillispot

What is **Bluesocket**, **NoCat Auth** and **Chillispot** ?

In short, those devices work by providing authentication services to wireless users to ensure they can access those services they're allowed to. For example, when a user is authenticated, he/she can begin to access the internet, check mail from his/her wireless computer.

You may have heard of the term "hotspot" and "splash screen". Say when you sit down at Starbucks Cafe, you can surf the net by login with an ID an password. Those devices mentioned above allow you to setup similar services.

At UCLA (in some areas), when you open your browser on the laptop computer, you may see the browser automatically redirected to a login screen. Once you entered your BOL ID and password and completed the authentication, you can begin to access the internet.

NOTE: authentication only checks your identity but it offers no encryption. If you are using a public wireless service, what you are transmitting over the air (packets) can be captured and reassembled to reveal the content. If you are paranoid then use encryption (VPN – virtual private networking). VPN is available on BOL website.

How it (hotspot / splash screen) works is beyond the scope of this discussion, more information can be found at:

- http://www.bluesocket.com/
- http://www.nocat.net/
- http://www.chillispot.info/ (also, Wikipedia)

Bluesocket is available commercially and can be very expensive. Some areas on campus use BlueSocket behind the scenes.

NoCAT and **chillispot** are opensource which means you can download the software and install it on a suitable PC. DD-WRT has a chillispot implementation option:

- http://www.dd-wrt.com/wiki/index.php/Chillispot
- Many additional technical descriptions by searching

Revision #2
Created Wed, May 24, 2006 8:18 AM by Tran, Daniel

Updated Fri, Nov 4, 2011 1:02 PM by Postovoit, Philip