

## **Basic Security for Your Wireless Network**

### **August 2008**

---

Lots of people run wireless networks within their business or home. It's easy and simple and as far as many people are concerned their network is available for them and only them. It is a fact however that the signal from a wireless Access Point (AP) may be detected and used from many metres away. This means the house down the street, or the business next door may be using your wireless network and if they wished, looking at your data as it passes over the airwaves.

There are a few simple things that you can do to protect your privacy.

#### **Change Your SSID**

A SSID is the public name of your wireless network. SSID stands for Service Set Identifier. Many people leave this set to the factory default, which may be LINKSYS or 3COM or similar. Change the SSID to something that describes your own network, this will at least ensure that people do not accidentally connect to your network instead of their own.

#### **Turn off the Access Point Beacon**

When you have setup your wireless network there is no further need for your AP to transmit it's beacon that basically says 'I AM LINKSYS. I AM HERE'. So within the administration software or web-page that you use to administer your AP, turn off the beacon. This will make your wireless network invisible to somebody who is just scouting around. If they know you have a network already or if they know the SSID they can still see and/or connect to you.

#### **Restrict Access to specific MAC Addresses.**

Each network card within a computer contains a Mac Address that is (to all intents and purposes) unique. With some AP's you can restrict access to your wireless network to computers of a known MAC Address. The procedures differ for each AP and some do not even support this, but if your AP does support this it is worth pursuing. This assumes that you do not regularly have new computers needing to connect to your network. Also be aware that valid MAC Addresses can be sniffed from your network and the attacker can spoof his MAC Address so that it looks like yours ...

#### **Change the Admin Password on your Access Point**

This one goes without saying. If you haven't already, do this. Do it now.

#### **Run Encryption**

Turn on the encryption option on your wireless network. If you don't I can load a program such as E\*\*\*\*\* and see the logon and passwords you are using, the letters you are typing and your secret cookie recipe. With software such as E\*\*\*\*\* I can see every image you load on every website you visit. It's that easy. If you only have access to WEP encryption then use it. Otherwise use WPA or WPA2 if possible. WEP encryption can be broken by a skilled attacker in under 4 minutes. If offered a choice of how many 'bits' do you want for your encryption, go for the highest. Always.

**Steve Cholerton**  
**Arten Science**