Introduction to Wireless Security

Introduction

As WLAN networks continue to increase and gain momentum newer technologies and software packages are introduced to further develop the wide varieties of uses currently available. Companies that benefit from the technologies continue to push the envelope improving overall systems performance and real time tracking of orders from receive to despatch.

One of the biggest issues in WLAN technology is security, and how to administer it. Currently most access points have up to date security features but these are not been utilised and or set to default settings making it easy for anyone to break in and take what they want. Typically users attempt to implement a security measure cannot get it operational, get frustrated and turn it off.

How much security do you need??

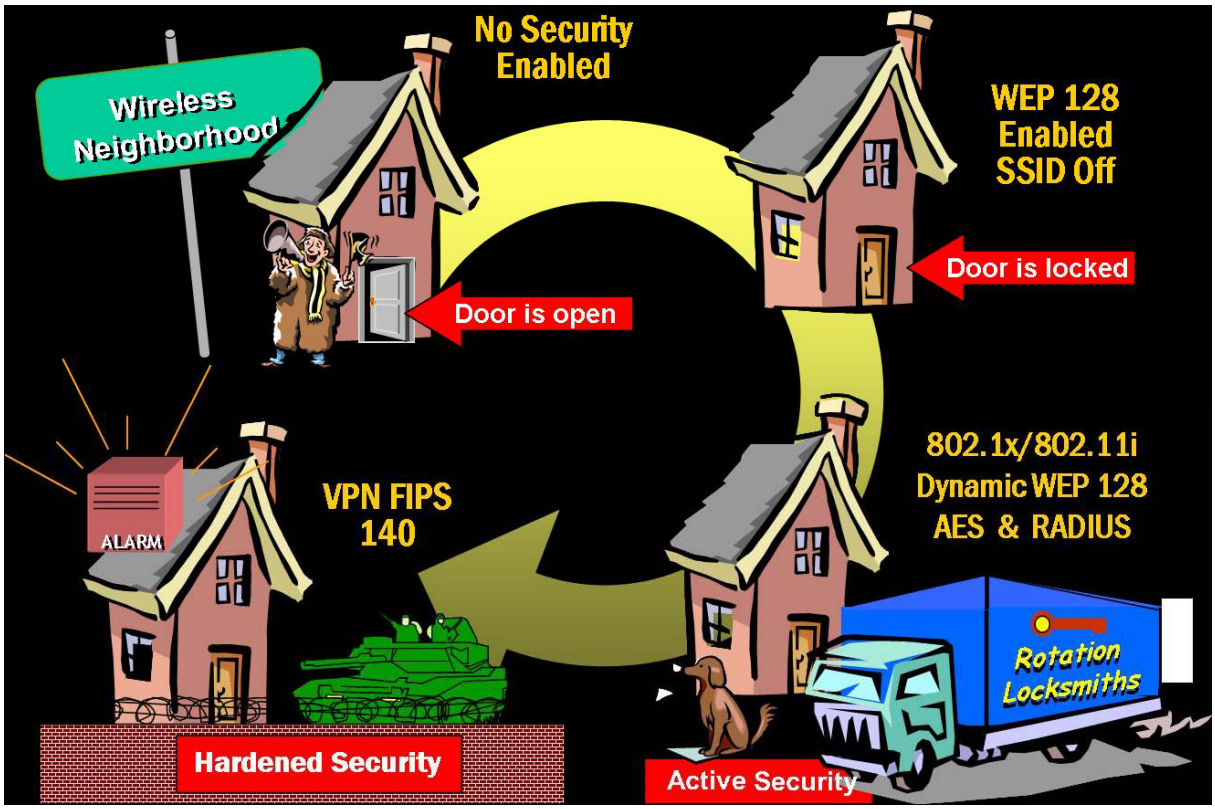
On a wireless LAN Ethernet adapters are replaced with radio access points and a radio card in the end device. Since there is no physical connection (hard wired) anyone with a radio enabled card can receive WLAN signals (sniffing) manipulate the information and present themselves as a valid user to gain access to the network. Once this occurs they have essentially connected to your network and have the ability to penetrate your corporate LAN taking control of all data and administrative access.

Depending on your situation analysing these areas will assist you in determining the type of security required for your site.

On of the important factors to think about is the data. What type of information does your company manage??

In the case of sensitive information credit card details and or personal health records stringent security measures will be required as that data will need to be protected at all costs.

Brief types of Security available



- **No Security Enabled**

Encompasses an open door approach where no security is active at any stage.

- **WEP 64 / 128 Bit Encryption**

A secret shared encryption key is used amongst devices to avoid eavesdroppers. Any device requesting authentication to the network will require this key to pass data through the access point.

- **802.1x Dynamic WEP key rotation**

Improved data encryption through the rotation of the WEP 128 keys, Uses a radius server in conjunction with a two data communication protocols EAP (extensible authentication protocol) and TLS (transport layer security).

- **FIPS 1.40 and VPN**

This hardened security subset uses point to point security for wireless communications and complies with FIPS 1.40 (federal information protection standard 1.40). These include software offerings such as Air-fortress and IPSec VPN's.

Wireless security is a complex issue, but can be tackled easily through UMD's Technologh Integration Division. We offer a wide spectrum of security solutions and can provide a level of network security based upon your specific situation.