Published on *Jisc community* (https://community-stg.jisc.ac.uk)

Rogue wireless suppression

A number of wireless LAN management systems have recently introduced functions that attempt to suppress rogue access points. Organisations considering using these should ensure that they are covered by their agreements with their users and their neighbours, otherwise their actions are likely to be highly unpopular and possibly even illegal.

The Problem

Wireless networking deployments are limited to a very small number of channels and an organisation with a WLAN of any size is likely to need all the frequencies available to provide adequate coverage. Any additional APs (Access Points) installed by others within range are therefore likely to cause radio interference and reduce the performance of the network. APs installed carelessly or maliciously (sometimes known as rogue APs) may present additional security threats, either by allowing unauthorised users to connect directly to the organisation's internal network – bypassing perimeter or internal firewalls – or by making authorised users think that they are connected to the organisation's own encrypted network and therefore safe to transmit passwords or other sensitive data. (APs intentionally performing this deception are known as 'evil twins' since they present an interface that duplicates the legitimate service in order to harvest credentials.)

What is Rogue Suppression?

Rogue suppression is a technique implemented in some WLAN controller appliances that uses their ability to monitor and manage their constituent APs to respond and intervene when they detect a potential security risk. A rogue suppression system will typically monitor all wireless transmissions in the vicinity, looking for traffic patterns characteristic of a client computer connecting to an AP (or, with some products, any ad hoc wireless network) that is not on a list of the official network infrastructure. The suppression system will then instruct the APs of the legitimate WLAN to transmit a series of packets instructing the client and/ or the unknown AP to terminate the connection. The aim is to prevent any client computers from connecting to the rogue AP so they have no opportunity to send or receive any sensitive information. In this way, the potential security threat is minimised by temporarily disabling the AP until a member of the organisation's IT staff is able physically to investigate and/or remove it. However, until this is done, the continuing flood of 'disconnect' packets is likely to add to the existing radio interference and further degrade the service offered by legitimate APs in the area.

What's the Problem With Rogue Suppression?

Rogue suppression systems work by assuming that any AP they do not recognise is hostile. Unfortunately nearly all organisations will have neighbours whose own APs or users are within radio range. In these cases great care will be needed to avoid disconnecting legitimate users of these neighbouring WLANs. An organisation that attempts to disable all other wireless networks in the surrounding area is likely to be very unpopular.

Such an organisation may even break the law under amendments to the *Computer Misuse Act 1990* introduced by sections 35-38 of the *Police and Justice Act 2006*. These make it an offence under section 3 of the Computer Misuse Act to intentionally or recklessly impair the function of a computer without authorisation. Disabling an AP or client computer certainly impairs its function, so is likely to be a crime unless the action is authorised. Prior agreement with all those likely to be affected will be essential for rogue suppression systems to be used lawfully. This will entail maintaining an up-to-date register of all legitimate APs at all neighbouring sites in radio range, an activity unlikely to be scaleable or sustainable in an urban environment.

Can Rogue Suppression Be Used At All?

Any organisation considering using rogue suppression must balance the protection of users' privacy against availability of their own wireless network and the possibly serious consequences if the system disconnects legitimate users of other wireless networks. Measures that should help to reduce those consequences include:

- Agreeing conditions for use of the system with any neighbours who may have their own wireless APs. Making these known to the rogue suppression system should prevent it from disconnecting their users, but requires continuous effort to keep the list up-to-date.
- Ensuring that any incident that activates the suppression system is investigated immediately, whenever it occurs. Even if the system has correctly identified and disabled a malicious rogue, wireless interference around the rogue and the flood of disconnect packets will still be disrupting the network service. If the system is acting to shut down a legitimate service then it is essential to stop this behaviour as soon as possible.
- Consider deploying technologies such as IEE 802.1X that allow a client to identify a rogue access point before transmitting a username and password. This reduces the risk of theft of credentials by such access points, though the confidentiality and radio interference problems still need to be dealt with by monitoring and speedy removal.

It is also possible that an active suppression mechanism might itself be exploited to cause a denial of service. A malicious user could inject traffic simulating a number of rogue APs and thus induce the production WLAN to switch to suppression mode, limiting its availability to legitimate users.

Source URL: https://community-stg.jisc.ac.uk/library/advisory-services/rogue-wireless-suppression