

Drawbacks of Wireside-Only Rogue Detection

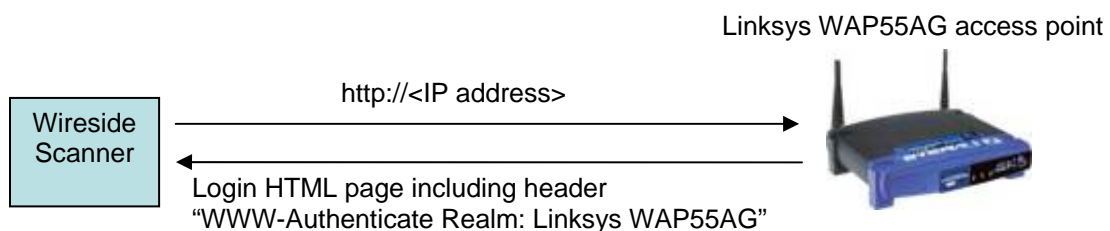
Hemant Chaskar and K. N. Gopinath
AirTight Networks

August 26, 2009

Rogue access point on enterprise network poses serious security threat. It is now well established that wired–wireless traffic correlation is the only robust way for comprehensive rogue access point detection. Nonetheless wireside-only scanning is sometimes touted as a low cost alternative for detecting rogue access points on network. It is important to note that the wireside only scanning is not robust enough to provide assured rogue access point detection. This paper deliberates on this point.

How wireside-only scanning works?

Wireside scanner attempts to fingerprint devices connected to the network by issuing different types of queries and examining responses to infer if the responding device is access point. Commonly used queries are SNMP, HTTP etc. An example of wireside only fingerprinting using HTTP is shown below:



So if HTTP query to an IP address fetches HTML page including the header “WWW-Authenticate Realm: Linksys WAP55AG”, the scanner infers that the device at that IP address is Linksys access point.

Sometimes MAC fingerprinting is also be used in the wireside-only scanning technique. In MAC fingerprinting, the scanner infers vendor of the device from the OUI (3 most significant bytes) of the wireside MAC addresses of the device. The scanner needs to access wired MAC addresses by some means such switch CAM table lookup. For example, the OUI assigned to Linksys Group is 00:04:5A. So if wireside MAC is found starting with 00:04:5A, the scanner infers that it is most likely Linksys access point.

OS and IP stack fingerprinting can also be used in principle to detect rogue access points.

Drawbacks of wireside-only scanning for rogue detection

Wireside-only scanning is basically signature based identification. It requires extensive set of signatures such as known responses of access points to HTTP/SNMP queries, MAC OUI-vendor mapping, and other OS and IP stack fingerprints of access points.

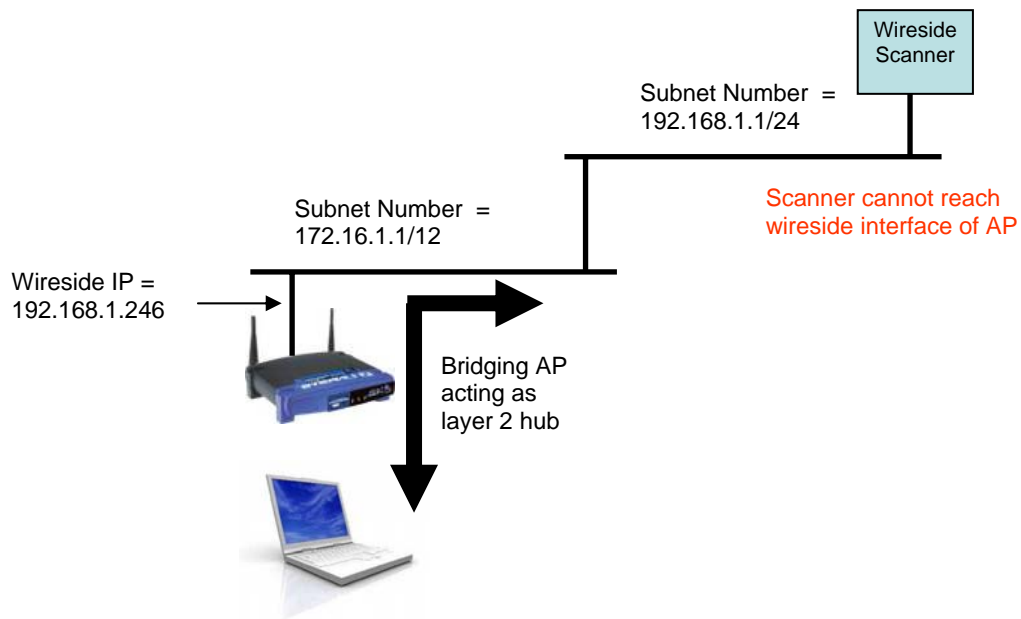
There is continuous overhead of keeping signatures up to date with new hardware and firmware releases of access points. Moreover, it is to be noted that many of the signatures are false alarm prone, for example, OUI assigned to DLink can be found not only in wireside MAC addresses of WiFi access points, but also in MAC addresses of many other networking devices provided by DLink.

Even if one assumes perfect signature database, still several rogue access points are fundamentally undetectable with wireside-only scanning. Here are some examples:

Scenario (i): Bridging Access point whose wireside IP is inconsistent with subnet range where it is connected.

This occurs if a bridging access point is connected in its default configuration or with a static IP address to a network. Taking example of the above Linksys AP, it has IP address of 192.168.1.246 on its wired interface by default. Now suppose that this AP is connected in default configuration (which by the way also uses OPEN wireless link in default configuration) into a network jack which is on 172.16.1.1/12 subnet. This AP being bridging device, it is still fully operational on such network to forward packets between wired and wireless sides, notwithstanding the IP mismatch. But now scanner cannot reach wired side interface of this access point as it is not possible to route packets to 192.168.1.246 address sitting on 172.16.0.0/12 subnet. So in general HTTP, SNMP, and OS fingerprinting is of no use.

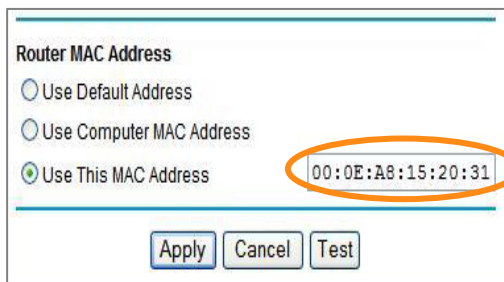
It is also important to note that MAC address of the wired interface of this rogue access point does not appear anywhere in the wired infrastructure (e.g., switch ports or DHCP server) as it is not used for any forwarding or addressing functions. So MAC OUI analysis is also not going to work.



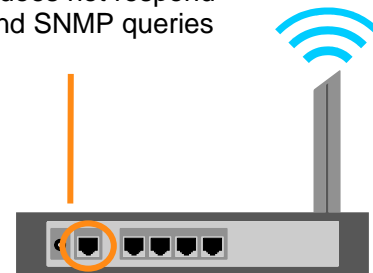
The only way to fingerprint this AP from wireside is for the scanner to be also present on 172.16.1.1/12 subnet, which is not what commercial scanners are able to do today. Even then not only does the scanner will have to do some low level non-standard tricks to detect presence of such device on the network (such as ARPing for 192.168 addresses even if the scanner is on 172.16 subnet), but it will also have to brute force its way through all possible IP addresses. This is because it is possible to set static IP on wired interface of this rogue access point to any value, not even necessarily in the private IP address range. Such brute forcing will take significant time, and will also generate lots of traffic on the subnet.

Scenario (ii): Wireless Router with cloned MAC addresses.

MAC cloning makes OUI based fingerprinting impossible



WAN Port does not respond to HTTP and SNMP queries



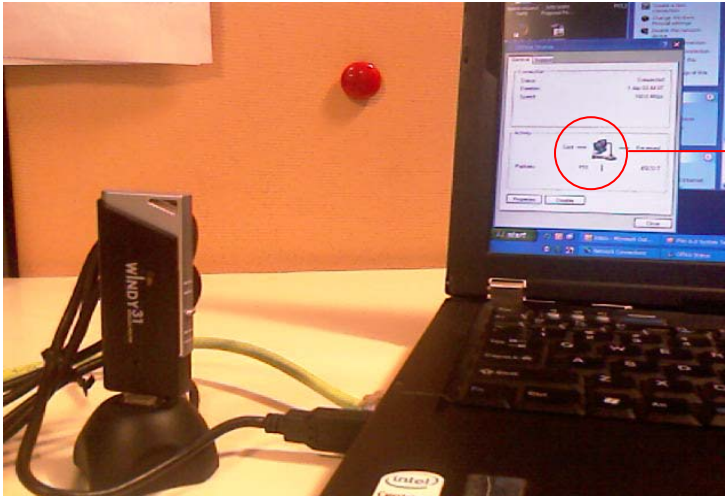
Wireless Router

Many wireless routers do not respond to HTTP, SNMP queries and even Ping on their WAN interface. This behavior is consistent with their intended use in which the WAN interface plugs into modem facing the Internet cloud and the LAN interfaces are for local connectivity. It is not necessary to enable HTTP, SNMP or Ping on WAN interface; in fact it is a good security practice to not enable them on WAN port. So HTTP and SNMP based fingerprinting will not work on WAN port.

In addition, many wireless routers will have their WAN side MAC addressed cloned. Cloned MAC address makes OUI based identification also impossible. Finally, many wireless routers use standard IP stacks available in market and hence OS based fingerprinting may not work as well.

Scenario (iii): Wireless Router piggybacked on enterprise laptop.

Several wireless USB and PCMCIA devices are available in the market which can be connected to laptop to turn it into an access point. For example, Windy31 is such popular device. Windy31 is a USB stick including WiFi radio which plugs into laptop's USB port. It automatically configures the laptop to perform routing between laptop's wired interface and the USB port.



Internet
Connection
Sharing

Now what wireside-only scanner sees is the wired interface of the legitimate laptop and completely misses the fact that it has rogue access point piggybacked on it.

Key Takeaways

Wireside-only scanning technique for detection of rogues on enterprise network at first sight. However as we discussed it has several drawbacks as follows:

- i) Wireside-only rogue detection requires extensive signature set which needs to be regularly updated for new hardware and firmware versions. In practice, the signature set will mostly be incomplete. Also signatures are often prone to false positives.
- ii) Even if perfect signature database is assumed, wireside-only rogue detection misses many types of common rogue scenarios.
- iii) Wired-wireless correlation is the only robust way to comprehensively detect rogue access points on network.
- iv) Even the compliance bodies such as PCI have made wireless side scanning mandatory to keep enterprise networks free from wireless vulnerabilities such as rogue APs. Wireless-only scanning not only violates PCI DSS 1.2 in letter as it does not use wireless scanners, but it also violates it in spirit as it fails to detect many common types of rogues on wired network.