WLAN Testing Reports

"Debunking the Myth of SSID Hiding"

by Robert Moskowitz
Senior Technical Director
ICSA Labs, a division of TruSecure Corporation

December 1, 2003

In IEEE 802.11 networks, the SSID (Service Set Identifier) is viewed by some security professionals as an unneeded advertisement of the wireless network to attackers and these professionals assert that all measures should be taken to 'hide' the SSID. But this advertisement is the essential role that SSIDs are designed to play. The broadcast of the SSID improves the performance of a wireless network and the SSID cannot be hidden without degrading proper WLAN operations. Efforts to hide the SSID are at best half-measures which lead to a false sense of security and to a degradation of wireless network performance, particularly in a roaming situation.

The SSID is a 1 to 32 byte value that functions in wireless networks much the way that NETBIOS Scope functioned in the old bridged networks: to segment the airwaves for usage. If two wireless networks are physically close, the SSIDs label the respective networks, and allow the components of one network to ignore those of the other. SSIDs can also be mapped to VLANs; thus many APs support multiple SSIDs. The SSID is present in the following 802.11 management messages:

- BEACONs
- PROBE Requests
- PROBE Responses
- ASSOCIATION Requests
- REASSOCIATION Requests

This presence in management messages, or frames, is an oft-overlooked detail of the IEEE 802.11 specification that is critical to debunking the myth of SSID hiding. Management messages are always sent in the clear, even when link encryption (WEP or WPA) is used, so the SSID is visible to anyone who can intercept these frames.

SSIDs in AP BEACONs

The SSID is normally carried in every BEACON sent by the APs (5 to 20 times per second). The BEACON also contains the time, capabilities, supported data rates, and physical layer parameter sets that regulate the smooth operation of a wireless network. The SSID in the BEACON is the network advertisement that appears to those not fully versed in the low-level workings of IEEE 802.11 networks to be the risk exposure. It is possible to use the Broadcast SSID (an SSID of length zero) instead of the configured SSID and still include the other network information in the BEACON. This would seem to 'hide' the wireless network, as in this configuration, the only evidence of a wireless network is the MAC address of the AP.

SSIDs in Station Messages

It is not only the BEACONing behavior of the APs that exposes the SSID, but also the management message behavior of the stations. Every time a station connects to an AP, it sends either an ASSOCIATION or REASSOCIATION message. These messages always contain an SSID. If the SSID is not the same as that configured in the AP, the association fails. This behavior has led some to think of the SSID as a password sent in the clear. If this were the case, it would surely be a security flaw. Again, this is a misunderstanding of the role of the SSID in the ASSOCIATION message. Since an AP can host multiple SSIDs, the station includes the SSID in the ASSOCIATE message to inform the AP which network the station is trying to join. The Station must either learn the SSID from BEACONs or be manually configured. Through the action of the PROBE messages (or BEACONs that contain the SSID), a properly functioning station should never present the wrong SSID to an AP.

When an AP includes the SSID in the BEACONs, the stations learn of the appropriate APs to use for association through passive scanning of the wireless channels. This operation is done at times when the

station's radio is not scheduled for transmission or reception (a wireless device can only operate on one channel at a time). When the BEACONs lack the SSID, the stations have to use active scanning. They have to stop transmitting or receiving normal data traffic and work through all the channels sending PROBE Requests containing the SSID of the network they wish to join and listening for PROBE Responses containing the same SSID.

The Role of SSIDs in supporting Roaming

BEACONs are frequent events and it might seem that the other management messages rarely occur. In fact they may occur very frequently and can be forced to occur on demand through a simple active attack. Although the SSID can be omitted from, or 'hidden' in the BEACON, it is always present in the other messages.

In order for a station to roam, it must discover APs and choose one. Roaming is not just for stations on the move, but can happen any time that the station determines that it has a weak signal from its current AP. The method of this determination and the definition of "weak" is very vendor specific. In general, this determination is made when the station's view of its Radio Frequency environment changes. This change could be triggered by physical motion, either of the station, the access point, or of other objects in the vicinity, by changes in interference caused by other stations, by antenna blockage, by microwave oven leakage, or other factors.

A station preparing to roam in a WLAN whose BEACONs do not carry the SSID must actively scan to discover APs. The station sends out PROBE Requests sequentially on all channels with its SSID and listens for PROBE Responses. The station may do this channel scanning every 50 msec (20 times a second!) as it attempts to discover a stronger signal. In some office configurations, stations have been observed to 'bounce' between APs, spending only minutes on one AP and then switching to another based on signal strength. Thus a WLAN that has stations with weak signals from the APs will readily expose the SSID in all the PROBE Requests and ASSOCIATION frames.

A network that has only one AP is still faced with roaming behavior and active scanning if SSIDs are hidden. The same events mentioned above still can occur even if there is only one AP. Even with only one AP and even if it is configured to use channel 1, the station will still scan all channels checking for other APs. In the end, the station will ASSOCIATE with its original AP, exposing the SSID.

The excessive PROBE Requests and Responses in this configuration have the potential to negatively impact on WLAN performance, particularly when there are many stations roaming. And again, roaming does NOT require the station to physically move. A station with a weak signal (including one whose reception is weakened due to local interference) or one located between two APs will attempt to roam. Further, this increased active probe traffic may actually INCREASE the number of frames in the air which contain the SSID of the network, thus making it easier for a passive observer to capture the SSID, and having the exact opposite of the intended effect of "masking" the SSID.

Attacking 'hidden' WLANs to expose the SSID

Since a station always includes the SSID in the ASSOCIATE message, it can be forced to expose a hidden WLAN through a simple active attack. To do this, an attacker simply sends a forged DISASSOCIATE message to an active station, seemingly coming from the AP. Within seconds (at most 30), the station will REASSOCIATE, exposing the SSID. This simple attack means that the only WLAN that can be successfully hidden is one that is not being used.

SUMMARY

Contrary to a common belief that the SSID is a WLAN security feature and its exposure a security risk, the SSID is nothing more than a wireless-space group label. It cannot be successfully hidden. Attempts to hide it will not only fail, but will negatively impact WLAN performance, and may result in additional exposure of the SSID to passive scanning. The performance impact of this misguided effort will be felt in multiple WLAN scenarios, including simple operations like joining a WLAN, and in significantly longer roaming times.

Trying to hide the SSID does not strengthen security in WLANs. The scarce resources of today's WLAN administrator are better spent tuning WLAN performance and operations with full SSID usage, and enhancing WLAN security by deploying modern security technology, such as link-layer encryption, and IEEE 802.1X authentication.

Author Biography

Robert Moskowitz has been a member of the Internet Architecture Board, the IETF Application Area Directorate, and co-chair of the IETF IPSec Workgroup. In these areas, he was been heavily involved in security work. He is now active in IEEE 802 working on security solutions for 802.11 and all the other 802 Medias (Ethernet, wireless broadband, UWB, etc.).

Moskowitz is a contributing editor for Network Computing Magazine and writes The Security Watch column. He is a Senior Technical Director at ICSA Labs, a division of TruSecure Corporation and supports the IPsec and WLAN certification programs.

Robert Moskowitz
Senior Technical Director
ICSA Labs, a division of TruSecure Corp.
(248) 968-9809
Fax: (248) 968-2824
Email: rgm@icsalabs.com
Website: www.icsalabs.com