IEEE P802.11
Wireless LANs

|  |
| --- |
| Privacy Enhanced Wireless |
| Date: 2017-03-20 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HP Enterprise | 3333 Scott boulevard, Santa Clara, CA | +1 408 227 4500 |  |
|  |  |  |  |  |

Abstract

While a station attempts to discover services on a network pre-association, it may inadvertently expose privacy sensitive data to passive monitors. Pervasive monitoring of traffic of STAs in this state allows networks of activity and relationships to be built up based on mobility, location, and associations of data gleaned from 802.11 frames. This information can be used to help identify and track an individual.

This submission proposes using randomized MAC addresses, and the randomization and resetting of other data contained in 802.11 frames to limit the effectiveness that passive monitoring has in tracking. It also recommends a behavior on STAs for which privacy considerations are important.

***Instruct editor to insert new section:***

**4.5.4.10 Privacy Enhancements**

When a STA searches for, and connects to, an infrastructure BSS or IBSS or attempts to discover services on a network pre-association, it defines the addressing of its MAC layer for the particular connection. If the STA uses a fixed MAC address it is trivial to track the STA. An MSDU transmitted by a STA is assigned a sequence number that, if never reset, can also be used to track a device irrespective of the MAC address. If OFDM is used, the PHY DATA scrambler used can enable tracking of a device irrespective of the MAC address if it is not reseeded. The dynamic nature of BSS membership combined with this tracking information allows for construction of a network of connections, locations, and behavior. This network can be used to glean private and sensitive information regarding the individual behind the device.

Furthermore, even without establishing a connection, a mobile or portable STA that gratuitously probes for favored infrastructure BSS networks, or announces the existence of IBSS networks, can reveal potentially sensitive information about its location and location history.

To mitigate this sort of traffic analysis mobile and portable STAs can support the ability to periodically and randomly change their MAC addresses and reset counters and seeds prior to association. Post-association, these devices use a unique random MAC addresses with a single sequence number space and seeded data scrambler for an established network connection. While discovering networks, STAs can refrain from gratuitously probing for favoured BSS networks.

***Instruct the editor to modify section 10.3.2.11.2 as indicated:***

**10.3.2.11.2 Transmitter requirements**

A STA maintains one or more sequence number spaces that are used when transmitting a frame to determine the sequence number for the frame. When multiple sequence number spaces are supported, the appropriate sequence number space is determined by information from the MAC control fields of the frame to be transmitted. Except as noted below, each sequence number space is represented by a modulo 4096 counter, starting at 0 and incrementing by 1, for each MSDU or MMPDU transmitted using that sequence number space. If dot11PrivacyActivated is true, the counter in each sequence number space shall be set to a random value modulo 4096 when the STA’s MAC address is changed.

***Instruct the editor to modify section 11.1.4.3 as indicated:***

**11.1.4.3 Active scanning**

**11.1.4.3.1 Introduction**

Active scanning involves the generation of Probe Request frames and the subsequent processing of received Probe Response frames. Active scanning can raise privacy concerns due to the ability to track a non-AP STA based on the frequency and content of Probe Request frames. A non-AP STA may set dot11PrivacyActivated to true to invoke privacy consideration and address this concern (see section 12.2.10). The details of the active scanning procedures are as specified in the following subclauses.

**11.1.4.3.2 Active scanning procedure for a non-DMG STA**

Upon receipt of the MLME-SCAN.request primitive with ScanType indicating an active scan, a STA shall use the following procedure.

For each channel to be scanned:

1. Wait until the ProbeDelay time has expired or a PHY-RXSTART.indication primitive has been received.
2. Perform the basic access procedure as defined in 10.3.4.2.
3. Send a probe request to the broadcast destination address. The probe request is sent with the SSID and BSSID from the received MLME-SCAN.request primitive.
4. When the SSID List is present in the invocation of the MLME-SCAN.request primitive, send zero or more Probe Request frames, to the broadcast destination address. Each probe request is sent with an SSID indicated in the SSID List and the BSSID from the MLME-SCAN.request primitive. When dot11PrivacyActivated is set to true, all probe requests shall be sent to the wildcard SSID. The basic access procedure (10.3.4.2) is performed prior to each probe request transmission.

***Instruct the editor to modify section 11.25a as indicated:***

**12.25a Pre-Association discovery (PAD) procedures**

**11.25a.1 General**

There are two types of PAD procedures: unsolicited and solicited. The unsolicited PAD procedure is described in 11.25a.2 and the solicited PAD procedure is described in 11.25a.3.

When dot11UnsolicitedPADActivated or dot11SolicitedPADActivated is true, a non-AP and non-PCP STA may use PAD procedures to allow the SIC to discover the availability of services that the same non-AP and non-PCP STA may access when associated. While the specification of service-specific information is outside the scope of this standard, the service-specific information in the BSS is proxied by a SIR (see 4.5.9.2.3), which might be collocated with the AP or PCP.

A non-AP STA with dot11SolicitedPADActivated set to true may invoke privacy procedures by setting dot11PrivacyActivated to true (see section 12.2.10).

An AP advertises support for PAD by setting the PAD field of the Extended Capabilities element to 1s in its Beacon and Probe Response frames.

A PCP advertises support for PAD by setting the PAD field of the Extended Capabilities element to 1 in its DMG Beacon, Announce, and Probe Response frames.

***Instruct the editor to insert new section:***

**12.2.10 Requirements for support of privacy enhancements**

If a non-AP STA desires enhanced privacy during discovery, BSS transition, and membership it shall set dot11PrivacyActivated to true. When dot11PrivacyActivated is true, a non-AP STA shall periodically change its MAC address to a random value. The smaller the period of MAC address change, down to a single MAC address per Probe Request frame, the greater the privacy these enhancements afford. The actual period used to change a MAC address is implementation dependent and outside the scope of this standard.

When dot11PrivacyActivated is true, a STA that discovers a BSS of interest and wishes to establish a connection shall again change its MAC address to a random value prior to establishing a connection to the BSS. Once connected, it shall retain that MAC address for the duration of its BSS connection.

Every time a MAC address is changed to a new random value, counters in all sequence number spaces used to identify each MSDU or MMPDU shall be reset (see 10.3.2.11.2), and the OFDM data scrambler shall be reseeded per the procedure described in section 17.3.5.5, if applicable.

STAs connecting to an infrastructure BSS should retain a single MAC address for the duration of its connection across an ESS. A PMKSA created as part of an RSNA connection will contain the MAC address used to create the PMKSA. A STA that supports PMKSA caching shall, if necessary, change its MAC address back to that value when attempting a subsequent association to the ESS using PMKSA caching.

To set a random MAC address, a STA shall assign it random 48-bit value and then shall set the sixth bit of the first octet to one (indicating a locally administered MAC address) and the seventh bit of the first octet to zero (indicating unicast). Using 46 bits of randomness will ensure that the probability of random MAC address collision on even the largest networks remains acceptably small.

To avoid leakage of possibly sensitive network identifying information, STAs should refrain from directed probing for preferred SSIDs and, instead, use passive scanning or wildcard probing.

***Instruct the editor to modify section 17.3.5.5 as indicated:***

**17.3.5.5 PHY DATA scrambler and descrambler**

The 127-bit sequence generated repeatedly by the scrambler shall be (leftmost used first), 00001110 11110010 11001001 00000010 00100110 00101110 10110110 00001100 11010100 11100111 10110100 00101010 11111010 01010001 10111000 1111111, when the all 1s initial state is used. The same scrambler is used to scramble transmit data and to descramble receive data. If the TXVECTOR parameter CH\_BANDWIDTH\_IN\_NON\_HT is not present, when transmitting, the initial state of the scrambler shall be set to a pseudorandom nonzero state. If the TXVECTOR parameter CH\_BANDWIDTH\_IN\_NON\_HT is present,

* The first 7 bits of the scrambling sequence shall be set as shown in Table 17-7 (with field values defined in Table 17-8 and Table 17-10) and shall be also used to initialize the state of the scrambler
* The scrambler with this initialization shall generate the remainder (i.e., after the first 7 bits) of the scrambling sequence as shown in Figure 17-7
* CH\_BANDWIDTH\_IN\_NON\_HT is transmitted LSB first. For example, if CBW80 has a value of 2, which is ‘10’ in binary representation, then B5=0 and B6=1

If dot11PrivacyActivated is true, the initial state of the scrambler shall be reset when the STA’s MAC address is changed.

***Instruct the editor to add the following to the end of the “Dot11StationConfigEntry ::= SEQUENCE” list:***

**C.3 MIB Detail**

dot11VHTExtendedNSSBWCapable TruthValue,

dot11FutureChannelGuidanceActivated TruthValue,

dot11SolicitedPADActivated TruthValue,

dot11UnsolicitedPADActivated TruthValue,

dot11PrivacyActivated TruthValue

}

**References:**

Vanhoef, M., et al, “*Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms*”, ASIA CCS ’16 Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, pages 413-424

Martin, Jeremy, et al, “*A Study of MAC Address Randomization in Mobile Devices and When it Fails*”, arXiv preprint, arXiv:1073.02870, March 2017.