IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Privacy Enhanced Wireless | | | | |
| Date: 2013-03-16 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | Aruba Networks | 1322 Crossman ave, Sunnyvale, CA | +1 408 227 4500 | dharkins at aruba networks dot com |
|  |  |  |  |  |

Abstract

Pervasive monitoring of traffic allows networks of activity and relationships to be built up based on mobility, location and associations of fixed addressing information, like MAC addresses. This information can be used to help uniquely identify an individual using the MAC address as well as sensitive and private information about that individual. This submission proposes using randomized MAC addresses and a behavior on STAs utilizing randomized MAC addresses to limit the effectiveness of traffic analysis.

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

**4.5.4.10 Privacy Enhancements**

When a STA connects to an infrastructure BSS or IBSS it defines the addressing of its MAC layer for the particular connection. If the STA uses a fixed MAC address, the dynamic nature of BSS membership enables a network of connections, locations, and behaviour to be established. This network can be used to glean private and sensitive information regarding the individual behind the fixed MAC address. 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. To mitigate this sort of traffic analysis mobile and portable STAs can support the ability to periodically and randomly change their MAC addresses when not connected and to use a unique random MAC addresses per established network connection.

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

**11.1.9 Requirements for support of privacy enhancements**

When a STA is not a member of a BSS it should periodically change its MAC address to a random value. The period should be not more than 1 hour and should not less than 1 minute. When a STA discovers a BSS of interest and wishes to establish a connection it should 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.

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).

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.

**References:**