Workgroup: madinas working group
Internet-Draft:
draft-henry-madinas-bcp-network-rcm-00]
Published: 13 April 2023
Intended Status: Best Current Practice
Expires: 15 October 2023
Authors: J. Henry A. Andersdotter
Cisco Systems Sky UK

Best Current Practices for network services in an RCM context

Abstract

End devices are implementing Randomized and Changing MAC addresses (RCM), with the advertised goal of improving the user privacy, by making the continued association between a MAC address and a personal device more difficult. RCM may be disruptive to some network services. This document is a collection of best practices for the general implementation of network services within an RCM context.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 15 October 2023.

Table of Contents

1. Introduction

With the fast development of unlicensed radio technologies for communication (e.g., Wi-Fi) and the explosion of smartphones and other personal devices, the association between the MAC address of a device (as detailed in https://www.ietf.org/archive/id/draft-ietf-madinas-use-cases-05.html#name-mac-address-as-an-identity-) has been a common way to identify a device in a network, both in cases where this supports delivery of data packets and where it supports ancillary services such a diagnostics or geolocational tracking. To limit that association, personal device vendors have started implementing RCM schemes, changing the MAC address of the device at intervals. Such changes may have effects on network services and may possibly exhaust network resources. https://www.ietf.org/archive/id/draft-ietf-madinas-use-cases-05.html#name-use-cases identifies 6 use cases where RCM may be encountered. This document proposes best practices for each use case, with the double objective of suggesting stable operations in an RCM context, while not exposing further the user or device identity.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in

BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Home

In a home environment, it is common that users would not be worried about other users in the home's ability to associate a MAC address with a given device. However, radio waves may travel beyond the home boundary, allowing external observers to potentially make that same association. Therefore, in such environment, limiting the over-the-air association between a device and its MAC may be desired, while obfuscating this same association vis-à-vis network services present in the home may not be a strong requirement.

Most client device operating system vendors offer RCM schemes, enabled by default (or easy to enable) on client devices. With these schemes, the device changes its MAC address, when not associated, after having used a given MAC address for a semi-random duration window. These schemes typically also allow for the device to manifest a different MAC address in different SSIDs.

Such randomization schemes enable the device to limit the duration of exposure of a single MAC address to observers, hereby reducing the ability of observers to spatially track the device using the MAC address. In 802.11-2020, MAC address rotation is not allowed during a given association session, and thus rotation of MAC address can only occur through disconnection and reconnection. Authentication may then need to reoccur, with an associated cost of service disruption and additional load on the venue and identity provider infrastructure, directly proportional to the frequency of the rotation. The scheme is also not intended to protect from the exposure of other identifiers to the venue network (e.g., DHCP option 012 [host name] visible to the network between the AP and the DHCP server).

3. Managed Residential

In the context of this document, managed residential environments differ from homes in that an external entity is providing and maintaining the various services in the former case (while the home user is managing most or all of them in the latter case). In order to provide support to non-technical users, the service provider may request knowledge of the association between a physical device and its network identity (i.e., in many cases, its MAC address).

4. Enterprise Campus (BYOD)

In an enterprise environment, an IT team is commonly in charge of the management and protection of the network. Devices allowed to connect to the network commonly must abide by rules of activity and

identity traceability. At the same time, users bringing their own devices may also occasionally perform personal tasks (e.g., check personal emails) on these devices. Thus the environment presents a mix of requirements, some where each device must be identified (from the IT team viewpoint), and some where the device owner may wish to be in control of when and to whom such device identity can be exposed.

At the time of association to a Wi-Fi access point, 802.1X authentication coupled with WPA2 or WPA3 encryption schemes allows for the mutual identification of the client device or of the user of the device and an authentication authority. The authentication exchange is protected from eavesdropping. In this scenario, the user or the device identity can be obfuscated from external observers. However, the authentication authority is in most cases under the control of the same entity as the network access provider, thus making the user or device identity visible to the network owner.

This scheme is therefore well-adapted to enterprise environments, where a level of trust is established between the user and the enterprise network operator. In this scheme, rotation of MAC address can occur through brief disconnections and reconnections (under the rules of 802.11-2020). Authentication may then need to reoccur, with an associated cost of service disruption and additional load on the enterprise infrastructure, and an associated benefit of limiting the exposure of a continuous MAC address to external observers. The adoption of this scheme is however limited outside of the enterprise environment by the requirement to install an authentication profile on the end device, that would be recognized and accepted by a local authentication authority and its authentication server. Such server is uncommon in a home environment, and the procedure to install a profile cumbersome for most untrained users. Remembering that 2022 estimations count approximatively 500 million Wi-Fi hotspots on the planet, the likelihood that a user or device profile would match a profile recognized by a public Wi-Fi authentication authority is also fairly limited, thus restricting the adoption of this scheme for public Wi-Fi as well. Similar limitations are found in hospitality environments.

5. Enterprise (MDM)

In specific enterprise environments, all networking devices are provided and controlled by the enterprise. It is common in such environment that device identity would be expected to be known by the IT team at all times, as none of these devices are expected to be of personal type.

6. Hospitality

In hospitality environments, it is common that an entity would provide the essential network services required to allow connectivity to the Internet. In this environment, a user often does not assume that any observer, participant or actor in the local network should be trusted with personal information. However, it may be common for the network operator to require some form of device or user authentication, for charging purposes.

7. Public Wi-Fi

Public Wi-Fi presents many of the same characteristic as Hospitality Wi-Fi, with the core difference that charging may be common in hospitality Wi-Fi, but is uncommon in public Wi-Fi.

7.1. OpenRoaming

The Wireless Broadband Alliance (WBA) OpenRoaming Standard introduces an intermediate trusted relay between local venues and sources of identity. The federation structure also extends the type of authorities that can be used as identity sources (compared to traditional enterprise-based 802.1X scheme for Wi-Fi), and also facilitates the establishment of trust between a local venue and an identity provider. Such procedure dramatically increases the likelihood that one or more identity profiles for the user or the device will be recognized by a local venue. At the same time, authentication does not occur to the local venue, thus offering the possibility for the user or the device to keep their identity obfuscated from the local network operator, unless that operator specifically expresses the requirement to disclose such identity (in which case the user has the option to accept or decline the connection and associated identity exposure).

The OpenRoaming scheme therefore seems well-adapted to public Wi-Fi and hospitality environments, allowing for the obfuscation of the identity from unauthorized entities, while also permitting mutual authentication between the device or the user and a trusted identity provider. Just like with standard 802.1X scheme for Wi-Fi, authentication allows the establishment of WPA2 or WPA3 keys that can then be used to encrypt the communication between the device and the access point, thus obfuscating the traffic from observers.

Just like in the enterprise case, rotation of MAC address can occur through brief disconnections and reconnections (under the rules of 802.11-2020). Authentication may then need to reoccur, with an associated cost of service disruption and additional load on the venue and identity provider infrastructure, and an associated benefit of limiting the exposure of a continuous MAC address to

external observers. Limitations of this scheme include the requirement to first install one or more profiles on the client device. This scheme also requires the local venue network to support RADSEC and the relay function, which may not be common in small hotspot networks and in home environments.

7.2. 802.1X Authentication

At the time of association to a Wi-Fi access point, 802.1X authentication coupled with WPA2 or WPA3 encryption schemes allows for the mutual identification of the client device or of the user of the device and an authentication authority. The authentication exchange is protected from eavesdropping and the user or the device identity can be obfuscated from observers external to the network.

This scheme requires a RADIUS servers to perform verification of authentication credentials of a user seeking access to the network. In practice, such servers are usually only present in enterprise environments, campus networks or perhaps a managed residential network. The authentication authority is in most cases under the control of the same entity as the network access provider, thus leaving the user or device identity visible to the network owner.

In this scheme, rotation of the MAC address can occur through brief disconnections and reconnections (under the rules of 802.11-2020). If a MAC address is rotated, authentication may then need to reoccur, with an associated cost of service disruption and additional load on the enterprise infrastructure, and an associated benefit of limiting the exposure of a continuous MAC address to external observers.

The adoption of this scheme is limited outside of the enterprise environment by the requirement to install an authentication profile on the end device. An authentication profile which is accepted by a local authentication authority and its authentication server is needed for the scheme to work. Such a server is uncommon in a home environment, and the procedure to install a profile cumbersome for most untrained users. Remembering that 2022 estimations count approximatively 500 million Wi-Fi hotspots on the planet, the likelihood that a user or device profile would match a profile recognized by a public Wi-Fi authentication authority is also fairly limited, thus restricting the adoption of this scheme for public Wi-Fi as well. Similar limitations are found in hospitality environments.

One emerging use-case is provisioning of WiFi-assisted mobile network connectivity, where an end-user or subscriber to a connectivity service expects to be able to roam between a mobile network and semi-public hotspots (local networks provisioned by

access points belonging to the mobile network operator, for instance) and where a SIM-card can be used to contain the authentication profile (effectively making it the end-device for network access and authentication purposes). For this use-case, the challenge still remains for some higher-level implementations to maintain consistency in IP-addressing after a network transition has occurred.

8. IANA Considerations

This memo has no IANA actions.

9. Security Considerations

(TBD)

10. References

10.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

10.2. Informative References

[TBD1] TBD, T.B.D., "TBD1", 2023.

[TBD2] TBD2, "TBD2", 2023, <http://TBD2.com/>.

Acknowledgements

This template uses extracts from templates written by Pekka Savola, Elwyn Davies and Henrik Levkowetz. [REPLACE]

Contributors

Thanks to all of the contributors. [REPLACE]

Authors' Addresses

Jerome Henry
Cisco Systems
United States of America

Email: jerhenry@cisco.com

Amelia Andersdotter
Sky UK
Chatham Way
Brentwood
CM14 4DZ
United Kingdom

Email: amelia.ietf@andersdotter.cc