Workgroup: madinas Working Group
Internet-Draft:
draft-richardson-madinas-bcp-00
Published: 26 March 2023
Intended Status: Standards Track
Expires: 27 September 2023
Authors: M. Richardson
Sandelman Software Works

Best Current Practices for consistent network identity in a privacy preserving way

Abstract

This document describes the best current practices to identify devices in a post Randomized and Changing MAC address environment.

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 27 September 2023.

Copyright Notice

Table of Contents

1. Introduction

[I-D.ietf-madinas-use-cases] explains the history of L2 addresses. The unchanging nature of the L2 MAC addresses has created an unwanted public association between devices and users. A response to this has been deployment of Randomized and Changing MAC addresses (RCM). The various ways in which can be done has been summarized in [I-D.ietf-madinas-mac-address-randomization].

This document concerns itself with a variety of use cases in the form of specific protocols which are affected by RCM. In each use case, the affects of different device policies is discussed. In some cases the affects are not significant and no change is recommended. In other cases, the affects are significant to end users experience, or to even damaging to device operation, and deployment of alternate protocols are recommended.

The recommendations for alternate protocols are critical and there is often a very difficult market situation: before the alternate protocol can be deployed both a client and server need to be present. Neither party benefits until both parties have deployed. A particularly negative market situation can develop when client and server implementers come to non-interoperable choices in what protocol they will implement.

2. Terminology

Although this document is not an IETF Standards Track publication, it adopts the conventions for normative language to provide clarity of instructions to the implementer. 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.

[I-D.ietf-madinas-mac-address-randomization], Section 8 defines the following terms:

*Per-Vendor OUI MAC address (PVOM)

*Per-Device Generated MAC address (PDGM)

*Per-Boot Generated MAC address (PBGM)

*Per-Network Generated MAC adress (PNGM)

*Per-Period Generated MAC address (PPGM)

3. Protocol Specific Situations

3.1. Parental Controls on dependant devices

A common concern among parents of children is that the children do not access the Internet at inappropriate times. For instance, network access may be restricted from 30 minutes before bedtime until 6am in the morning.

(There are also concerns that the devices used by the children should go through specific filtering, but that is a subset of the time-of-day access. The time-of-day access is a binary on/off function, while the filtering is some continuous function with varying access between zero and one)

In order to restrict access to the child's device, the child's device needs to be identified. In order to not restrict access to other devices, those devices also need to be identified. Any device on the network which is not identifiable as being in either of these two categories has an ambiguous policy.

A child's device which uses a PVOM, PDGM or PNGM address will be seen to have a consistent layer-2 address by the network infrastructure. The device can therefore be recognized and Internet access can be restricted at appropriate times.

The use of a Per-Boot (PBGM) or a Per-Period (PPGM) address policy will result in the child's device changing it's layer-two address periodically, and this requires that the network infrastructure have it's policy updated.

A child (particulary a teenager) may be motivated to overcome these restrictions. They may be able to control their device, either through intentional "jail-breaking", or perhaps even due to some available malware that has the same effect. Any protocol that allows the child to pick a new identity (for instance, impersonating a parent device) would allow the child to overcome the limitation.

On a network where all devices except the child's device have no limitation is easiest: all the child needs to is to pick a new randomly chosen layer-two address. A network with a constant Pre-Shared Key (WPA-PSK) allows for any device knowing that PSK to join the network with essentially any layer-two address.

It is therefore necessary for all devices which are present in this child-restricted network to identify themselves in order for the network infrastructure to know that the relevant device is not a child's device.

This identification must be specific to each device, must not be forgeable, and must contain a credential that the network infrastructure can identify.

3.1.1. Home Networks need to use WPA-Enterprise

An LDevID deployed to all devices meets all of the criteria.

- observation of the public certificate does not convey any special permissions
- the private key of the LDevID an be stored in a secure element, fTPM or other trusted executation environment
- it scales easily to many devices
- it allows for a specific device to be identified for special processing, or to be ejected from the network
- it does not require any external arrangement with external services, if the CA's key is managed by the home router itself.

There are some privacy concerns with EAP-TLS used in WPA-Enterprise. Specifically, the client-certificate is visible in EAP-TLS 1.2 handshakes, and this could be used by an observer to coordinate which connection belongs to which personal device.

The most difficult part of this change is that it requires that home routers:

1. maintain a PKI with which to sign new certificates

2. have a mechanism to easily onboard new devices, along with a mechanism to deal with IoT devices which might be in the home.

3. have a way for the first user of the router to become the administrator

4. provide a way to backup the entire mechanism to guard against home router failure, flash replacement (such as when ISPs change), or other incompatible upgrades.

3.2. Paid/Captive Internet Services

A common case for hotels, airports and coffee shops is that they have an unencrypted network id. Guests connect to this network, but the network contains a captive portal [CAPTIVE] which "hijacks" all connections, and then demands a credential. Often these credentials are somewhat trivial: a room number with a matching guest last name. Some hotels demand far more complex logins, including use of loyalty system logins to enable access.

For the coffee shop and airport situations, it is uncommon for devices to spend a significant amount of time at that location. The use of an unencrypted network makes it trivial for an attacker to do ARP or ND spoofing of the default router They can then capture logins to the captive portal (having put up their own look-alike).

It is often also trivial in these networks to allow multicast traffic, and identifiable information can be found by using mDNS queries, or other port-scanning methods. The access point can not defend against such attacks, since the official access point has been spoofed.

3.3. Well known PSK Internet access

In some coffee shops, the network is encrypted, but there is a WPA-PSK which is written on the chalkboard. They seldom change, allowing patrons who have previously sipped coffee in that location to easily return and instantly be connected again.

For the coffee shop, it is uncommon for devices to spend a significant amount of time at that location. It is unlikely that a typical 12-hour Per-Period (PPGM) policy will run into this problem in a coffee shop.

But, the PSK methods are rather weak, as they PSK is well known, so not only can any attacker setup their own access point (grabbing all the traffic, and any PII they want), but

4. Privacy Considerations

YYY

5. Security Considerations

ZZZ

6. IANA Considerations

7. Acknowledgements

Hello.

8. Changelog

9. References

9.1. Normative References

[BCP14] 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/rfc/rfc8174>.

[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/rfc/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/rfc/rfc8174>.

[RFC8995] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructure (BRSKI)", RFC 8995, DOI 10.17487/RFC8995, May 2021, <https://www.rfc-editor.org/rfc/rfc8995>.

9.2. Informative References

[CAPTIVE] Larose, K., Dolson, D., and H. Liu, "Captive Portal Architecture", RFC 8952, DOI 10.17487/RFC8952, November 2020, <https://www.rfc-editor.org/rfc/rfc8952>.

[I-D.ietf-madinas-mac-address-randomization] Zúñiga, J. C., Bernardos, C. J., and A. Andersdotter, "Randomized and Changing MAC Address", Work in Progress, Internet-Draft, draft-ietf-madinas-mac-address-randomization-06, 11 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-madinas-mac-address-randomization-06>.

[I-D.ietf-madinas-use-cases]
Henry, J. and Y. Lee, "Randomized and Changing MAC Address Use Cases and Requirements", Work in Progress, Internet-Draft, draft-ietf-madinas-use-cases-05, 13 March 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-madinas-use-cases-05>.

[RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", RFC 7030, DOI 10.17487/RFC7030, October 2013, <https://www.rfc-editor.org/rfc/rfc7030>.

Author's Address

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca