Abstract

This document describes a method by which an unconfigured device can use EAP to join a network on which further device onboarding, network attestation or other remediation can be done. While RFC 5216 supports EAP-TLS without a client certificate, that document defines no method by which unauthenticated EAP-TLS can be used. This draft addresses that issue. First, by defining the @eap.arpa domain, and second by showing how it can be used to provide quarantined network access for onboarding unauthenticated devices.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-richardson-emu-eap-onboarding/.

Discussion of this document takes place on the anima Working Group mailing list (mailto:anima@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/anima/.

Source for this draft and an issue tracker can be found at https://github.com/mcr/eap-onboarding.git.

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 12 January 2023.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction ...................................................... 3
2. Terminology ....................................................... 4
3. Protocol Details ................................................... 4
   3.1. Discovery .................................................... 4
   3.2. Authentication ............................................... 5
   3.3. Authorization ............................................... 5
   3.4. Characteristics of Quarantine Network ........................ 5
4. Captive Portal .................................................... 6
5. Privacy Considerations ............................................ 6
6. Security Considerations ........................................... 6
   6.1. Use of eap.arpa .............................................. 7
7. IANA Considerations ............................................... 7
8. Acknowledgements .................................................. 7
9. Changelog .......................................................... 7
10. References ......................................................... 7
    10.1. Normative References ........................................ 7
    10.2. Informative References ....................................... 8
Authors' Addresses ................................................... 9
1. Introduction

There are a multitude of situations where a network device needs to join a new (wireless) network but where the device does not yet have the right credentials for that network. As the device does not have credentials, it cannot access networks which typically require authentication. However, since the device does not have network access, it cannot download a new configuration which contains updated credentials.

The process by which a device acquires these credentials has become known as onboarding [I-D.irtf-t2trg-secure-bootstrapping]. There are many onboarding protocols, including [RFC8995], [RFC9140], [dpp], CSA MATTER, and OPC UA Part 21. Some of these protocols use WiFi Public frames, or provide for provisioning as part of EAP, such as [RFC7170]. Other systems require pre-existing IP connectivity in order to configure credentials for a device, which causes a circular dependancy.

This document defines a method where devices can use unauthenticated EAP in order to obtain network access, albeit in a captive portal [RFC8952]. Once the device is in a captive portal, it has access to the full suite of Internet Protocol (IP) technologies, and can proceed with onboarding. We believe that the method defined here is clearer, safer, and easier to implement and deploy than alternatives. This method also allows for multiple onboarding technologies to co-exist, and for the technologies to evolve without requiring invasive upgrades to layer-2 infrastructure.

The method detailed in this document uses the unauthenticated client mode of EAP-TLS. While [RFC5216] defines EAP-TLS without a client certificate, that document defines no method by which unauthenticated EAP-TLS can be used.

This draft addresses that issue. First, by defining the @eap.arpa domain, and second by showing how it can be used to provid network
access for onboarding unauthenticated devices.

Note that this specification does not specify the exact method used for onboarding devices. There are many possibilities, with some methods yet to be defined. Not all of them are enumerated here!

2. Terminology

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.

3. Protocol Details

The onboarding is divided into the following phases:

* Discovery – the supplicant determines that a network can do onboarding,

* Authentication – the supplicant connects to the network as an unauthenticated device,

* Authorization – the network provides limited connectivity to the device,

* Onboarding – the device uses standard IP protocols to perform onboarding,

* Full network access – the device has provisioned credentials, and can proceed with normal network access.

3.1. Discovery
The network should use 802.11u to signal that it can potentially perform onboarding, by using 802.11u and indicating that it supports the realm "eap.arpa". When a supplicant which requires onboarding sees this realm, it knows that the network may be suitable for onboarding.

Note that not all such networks are suitable for onboarding. There may be multiple such networks available, and only one (or none) may be willing to onboard this particular device. Further, the device does not necessarily trust any such network.

There are situations where there may be many hundreds of networks which offer onboarding, and a supplicant device may need to try all of them until it finds a network to which it can successfully onboard. An example of such a situation is in a large (dozens to hundreds of floors) apartment building in a downtown core, where radio signals may leak from adjacent units, other floors, and even across the street from adjacent buildings. This document does not address this issue, but anticipates future work in 802.11u involving some filtering mechanism involving Bloom Filters.

Supplicants MUST limit their actions in the onboarding network to the action of onboarding. If this process cannot be completed, the device MUST disconnect from the onboarding network, and try again, usually by selecting a different network. As soon as the device has been onboarded, the device MUST disconnect from the onboarding network, and use the provided configuration to authenticate and connect to a fully-capable network.

3.2. Authentication

The supplicant presents itself as an unauthenticated peer, which is allowed by EAP-TLS [RFC5216] Section 2.1.1. TLS 1.2 or TLS 1.3
[RFC9190] may be used, but TLS 1.3 or higher is RECOMMENDED.

The supplicant uses an identity of onboarding@eap.arpa, and provides no TLS client certificate. The use of the "eap.arpa" domain signals to the network that the device wishes to use unauthenticated EAP-TLS.

3.3. Authorization

Upon receipt of a supplicant without any authentication, the AAA server returns instructions to the authenticator to place the new client into a quarantined network. The exact method is network-dependent, but it is usually done with a dedicated VLAN which has limited network access.

3.4. Characteristics of Quarantine Network

The quarantine network SHOULD be segregated at layer-two (ethernet), and should not permit ethernet frames to any destination other than a small set of specified routers.

For some onboarding protocols such as [RFC8995], only IPv6 Link-Local frames are needed. Such a network MUST provide a Join Proxy as specified in [RFC8995], Section 4.

For other onboarding protocols more capabilities may be needed, in particular there need for a DHCPv4 server may be critical for the device to believe it has connected correctly. This is particularly the case where a normal "smartphone" or laptop system will onboard via a captive portal.

Once on the quarantine network, device uses other protocols [RFC6876] to perform the onboarding action.

4. Captive Portal

While we can impose no requirements on the rest of the network, captive portals [RFC8952] have been used for almost two decades. The administration and operation of captive portals is typically within the authority of administrators who are responsible for network
access. As such, we can define additional behavior on, and requirements for, captive portals, so long as those changes materially benefit the network access administrator.

5. Privacy Considerations

Devices should take care to hide all identifying information from the onboarding network. Any identifying information MUST be sent encrypted via a method such as TLS.

6. Security Considerations

Devices using an onboarding network MUST assume that the network is untrusted. All network traffic SHOULD be encrypted in order to prevent attackers from both eavesdropping, and from modifying any provisioning information.

Similarly onboarding networks MUST assume that devices are untrusted, and could be malicious. Networks MUST make provisions to prevent Denial of Service (DoS) attacks, such as when many devices attempt to connect at the same time. Networks MUST limit network access to onboarding protocols only. Networks SHOULD also limit the bandwidth used by any device which is being onboarded. The configuration information is likely to be small (megabytes at most), and it is reasonable to require a second or two for this process to take place.

Any device which cannot be onboarded within approximately 30 seconds SHOULD be disconnected. Such a delay signals either a malicious device / network, or a misconfigured device / network. If onboarding cannot be finished within a short timer, the device should choose another network.

6.1. Use of eap.arpa

Supplicants MUST use the "eap.arpa" domain only for onboarding and related activities. Supplicant MUST use unauthenticated EAP-TLS.

Networks which support onboarding via the "eap.arpa" domain MUST require that supplicants use unauthenticated EAP-TLS. The use of EAP types MUST result in rejection, and a denial of all network access.
The "eap.arpa" domain MUST NOT be used in any other context, such as in an NAI [RFC7542], etc. in any other protocol.

7. IANA Considerations

The special-use domain "eap.arpa" should be registered in the .arpa registry (https://www.iana.org/domains/arpa (https://www.iana.org/domains/arpa)). No A, AAAA, or PTR records are requested.

8. Acknowledgements

TBD.

9. Changelog

10. References

10.1. Normative References


10.2. Informative References


Authors' Addresses

Alan DeKok
FreeRADIUS
Email: aland@freeradius.orf

Michael Richardson
Sandelman Software Works
Email: mcr+ietf@sandelman.ca