Workgroup: IOTOPS? Working Group
Internet-Draft:
draft-richardson-homerouter-provisioning-02
Published: 14 November 2021
Intended Status: Best Current Practice
Expires: 18 May 2022
Authors: M. Richardson
Sandelman Software Works

Provisioning Initial Device Identifiers into Home Routers

Abstract

This document describes a method to provisioning an 802.1AR-style certificate into a router intended for use in the home.

The proceedure results in a certificate which can be validated with a public trust anchor ("WebPKI"), using a name rather than an IP address. This method is focused on home routers, but can in some cases be used by other classes of IoT devices.

(RFCEDITOR please remove: this document can be found at https://github.com/mcr/homerouter-provisioning)

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 18 May 2022.

Copyright Notice

Table of Contents

1. Introduction

The increasing push to move all web interactions to HTTPS is a good thing. [RFC6797] section 2.3.1 explains some of the attacks that this defeats.

Residential use devices, particularly home routers, have some very unfortunate challenges. The router provides access control for the entire home network: controlling access to the router is critical. Malware has been, so far, content to attack the outside of home routers, exploiting poor authorization controls, and the fact that so few devices have their password changed (see [sixtypercent]).

Malware continues to arrive by email and by trojan download, and one must assume that at least some devices within the home may be infected.

An obvious next step for malware is to attack home routers and IoT devices from within the home. An unencrypted administrative interface to these devices presents two problems:

1. for devices that continue to use passwords as authorization, the passwords can easily be seen by active eavesdropping of the network, including use of IP address spoofing attacks. In residential configurations, the most common Layer Two (ethernet) wifi encryption does nothing to prevent address spoofing attacks at Layer Three (IP, ARP).

2. the lack of a useable TLS/HTTPS mechanism makes it difficult to use any kind of other non-password authorization mechanisms, such TLS Client Certificates, or OAUTH2 (Bearer) Tokens.

In addition to the above arguments relating to the control interface to these devices, there are some significant advantages in management if every device has a cryptographic identity. They include: ability to do remote attestation, ease of use of "Enterprise" versions of WPA, such as EAP-TLS for WiFi connectivity, detection of counterfeit devices, and better security for interactions with a cloud.

[I-D.richardson-t2trg-idevid-considerations] describes a number of different scenarios and considersation for manufacturer installation of keying material into devices. This document is much more specific, as it focuses on:

1. primarily Home Routers (as described in [RFC7084])

2. provisioning of certificates with public trust anchors (those that follow [CABFORUM])

3. manufacturers or ISPs that provision many devices, and who can control the firmware

4. users who use web browsers to do routine and management tasks

The next four sections expand the explanation of the above applicability, explaining why the boundaries have been set up as such.

1.1. Primarily Home Routers

As will be explained below, in order for the user's browser to be directed to the right system by name, it is easiest if the DNS names can be mapped to local IP addresses correctly. The Home Router is usually in a position to answer DNS queries from other devices in the home, so it can easily map names that should lead to the home router, to one of the home router's IP addresses.

As an extension to the mechanism described here, a new mechanism is described in Section 6 that provides for compatible naming of devices when control over DNS queries is not possible.

1.2. Provisioning of certificates with public trust anchors

The [CABFORUM] provides a set of guidelines agreed to by Browser authors and Certification Authorities (CA). A well funded CA that follows the guidelines is likely to be able to negotiate to have their trust anchor included by default into the trusted set distributed by browsers and operating systems.

Few of the details of the guidelines concern this document: but the key point is that an arbitrary manufacturer is unlikely to be able to negotiate directly, and will need to arrange to obtain certificates from one of the existing certification authorities, or it's suborbinate customers.

There are two details that do matter:

1. CAs will not sign private names or reserved IP addresses. Names used must be public and listed in the https://publicsuffix.org/list.

2. CAs are not to create certificates longer than a CABForum defined limit, which is currently set to approximately 1 year (in debate from approximately 2 years). However, some CAs, such as https://letsencrypt.org/, use a lifetime of 90 days, and many CAs are moving in this direction as well.

1.3. Manufacturers or ISPs do provisioning

The mechanism described in this document assumes that the entity doing the provisioning has control over the firmware. This is most easy for an hardware manufacturer who is building the devices and who performs the provisioning step in the factory. This provisioning step could also occur some time later in a Quality Assurance step where blank devices are first loaded with firmware. This is common for OEMs that have outsourced the actual manufacturing elsewhere, but bring the various components together in another place.

An ISP who purchased a large quanity of home routers, and then upgrades the firmware could also easily adapt this mechanism. The upgraded devices are then put back into their boxes, and into a warehouse or logistics center before shipping them to customers. It is not uncommon for ISPs, particularly those that use PPPoE, to need to provision a PPP username/login to be used for initial provisioning into every device. Upon first being connected, the device uses this default username to login to the ISP (to some

captive network), at which point customer-specific username and login are configured, often using TR-069.

1.4. Users who use web browsers

The process in this document benefits users with browsers (whether desktops or mobile browsers) who need to access a management interface of a home router or similiar device (such as a NAS or home automation system).

Devices which are exclusively configured using smartphone apps, and which have no other interfaces will find some of the mechanism superfluous. Smartphone apps can be provided with a private-CA trust anchor, and could easily be programmed to validate different parts of the certificate.

The lifetime and DNS name issues are of significantly less of an issues as a result.

However, the level of sophistication required to do the above coding is difficult to find in cross-platform mobile developers, and smartphone OS vendors are increasingly discouraging the use of private trust anchors.

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 Overview

Upon booting the device checks to see if it has been provisioned with a certificate already. (Note that an expired certificate is still considered to be been provisioned, see below)

Assuming that it has not, then it generates private key if necessary. Some classes of devices may have a private key provisioned by a firmware or physical TPM module during the manufacuring process.

The home router generates a Unique Local IPv6 Address (ULA, see [RFC4193] and [RFC7084] section 4.3), if it hasn't generated one already. It must store this generated prefix in the same place as the private key and certificate. If any of the ULA, or private key changes, then the certificate will need to be changed as well.

The home router uses all or a portion of the ULA to form a DNS name that is unique with the manufacturer's realm. For instance, given the ULA fd96:8d23:4fea::/48, one could drop the initial 7 bits which are always the same, skip a bit, and truncate to 6 bytes, giving: 8d234f. A name is formed, for instance: n8d234f.r.example.net.

With this name, a Certificate Signing Request is formed, binding the name n8d234f.r.example.net to the public key derived above.

The router then looks and waits for a network attachment on any of it's (physical) ethernet interfaces. This mechanism does not work for devices with only WiFi interfaces, but typical home routers have at least one physical interface used to connect to the Internet. Even integrated VDSL or LTE modems with a primarily WiFi orientation usually have at least one physical LAN port.

Some devices distinguishes a "WAN" interface, and other devices either only one network interface, or do not initally distinguish a specific one. A recommendation is to listen on any interface, as this makes provisioning the systems require less skilled labour: any connector that fits is acceptable.

Upon finding a network connection, the home router uses the [I-D.ietf-anima-grasp] protocol to do an M_DISCOVER for a service called "PROVISIONING". This is done using Link-Layer IPv6 addresses. The result will be a Link-Layer IPv6 address and port number on which the home router should connect.

A TLS/HTTPS connection is made to that address, using a virtual Host: that has been provisioning into the firmware by the manufacturer. (The same FQDN should go into the SNI for the TLS connection). The home router uses a trust anchor provisioned by the manufacturer, and [RFC6125] DNS-ID policy, to validate that the home router has been connected to an appropriate factory provisioning system.

The CSR along with some particulars about the device (the chosen ULA, some serial number information), is transmitted in an HTTPS POST. The provisioning system treats this as a secure connection because it originates on an IPv6-Link-Local address. (It is reasonable that the provisioning system is elsewhere, but that there is a local provisioning device which will relay traffic to the provisioning system)

The provisioning system obtains a certificate using ACME, and an [RFC8555] DNS-01 challenge. This may require up to a minute in order to do the DNS update, wait for propogation, and then receive the resulting certificate.

The device has provided its DNS name to the provisioning system, so the provisioning system installs that name into the DNS with a AAAA record giving the ULA address that the device has provided. (As part of the DNS-01 challenge, some challenge records are installed as proof of control of the name)

The provisioning system then returns the certificate to the device. The provisioning system SHOULD keep a copy of the certificate in a database; should the provisioning process fail before the device writes all its state to non-volatile memory, then the provisioning system need not repeat the certificate process.

The device now has a certificate for a name that it knows is its own. The device now creates a local DNS mapping (aka "/etc/hosts") from the name it has chosen to the ULA address it has chosen. The device, even when not connected to the Internet, will answer DNS queries for that name from client systems, mapping the name to the address, and then responding on port 443 to HTTPS queries for that name.

4. Protocol Details

Many small details to fill in.

5. Certificate Expiry/Renewal Protocol

Via store-and-forward with some javascript on port 80 and/or an App.

6. Using wildcard certificates with private network addresses

To be further described.

7. Privacy Considerations

Many to be discussed.

8. Security Considerations

9. IANA Considerations

10. Acknowledgements

Hello.

11. Changelog

12. References

12.1. 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/info/rfc8174>.

[I-D.ietf-anima-grasp] Bormann, C., Carpenter, B., and B. Liu, "GeneRic Autonomic Signaling Protocol (GRASP)", Work in Progress, Internet-Draft, draft-ietf-anima-grasp-15, 13 July 2017, <https://www.ietf.org/archive/id/draft-ietf-anima-grasp-15.txt>.

[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>.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, DOI 10.17487/RFC4193, October 2005, <https://www.rfc-editor.org/info/rfc4193>.

[RFC6797] Hodges, J., Jackson, C., and A. Barth, "HTTP Strict Transport Security (HSTS)", RFC 6797, DOI 10.17487/RFC6797, November 2012, <https://www.rfc-editor.org/info/rfc6797>.

[RFC7084] Singh, H., Beebee, W., Donley, C., and B. Stark, "Basic Requirements for IPv6 Customer Edge Routers", RFC 7084, DOI 10.17487/RFC7084, November 2013, <https://www.rfc-editor.org/info/rfc7084>.

[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>.

[RFC8555] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", RFC 8555, DOI 10.17487/RFC8555, March 2019, <https://www.rfc-editor.org/info/rfc8555>.

[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/info/rfc8995>.

12.2. Informative References

[CABFORUM] CA/Browser Forum, "CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.7.3", October 2020, <https://

cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.7.3.pdf>.

[I-D.richardson-t2trg-idevid-considerations]
Richardson, M., "A Taxonomy of operational security considerations for manufacturer installed keys and Trust Anchors", Work in Progress, Internet-Draft, draft-richardson-t2trg-idevid-considerations-05, 21 June 2021, <https://www.ietf.org/archive/id/draft-richardson-t2trg-idevid-considerations-05.txt>.

[RFC6125] Saint-Andre, P. and J. Hodges, "Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)", RFC 6125, DOI 10.17487/RFC6125, March 2011, <https://www.rfc-editor.org/info/rfc6125>.

[sixtypercent] "The economics of the security of consumer-grade IoT products and services", 24 April 2019, <https://www.internetsociety.org/resources/doc/2019/the-economics-of-the-security-of-consumer-grade-iot-products-and-services/>.

Author's Address

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca