Workgroup:
Operations and Management Area Working Group
Internet-Draft:
draft-wing-opsawg-authenticating-network-01
Published: 6 November 2022
Intended Status: Informational
Expires: 10 May 2023
Authors: D. Wing T. Reddy
Citrix Nokia

Asserting Wireless Network Connections Using DNS Revolvers' Identities

Abstract

This document describes how a host uses the encrypted DNS server identity to reduce an attacker's capabilities if the attacker is emulating a wireless network.

About This Document

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

The latest revision of this draft can be found at https://example.com/LATEST. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-wing-opsawg-authenticating-network/.

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

Source for this draft and an issue tracker can be found at https://github.com/danwing/authenticating-network.

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 10 May 2023.

Table of Contents

1. Introduction

When a user connects to a wireless network the user or their device want to be sure the connection is to the expected network, as different networks provide different services in terms of performance, security, access to split-horizon DNS servers, and so on. Although 802.1X provides layer 2 security for both Ethernet and Wi-Fi networks, 802.1X is not widely deployed -- and often applications are unaware if the underlying network was protected with 802.1X.

An attacker can operate a rogue WLAN access point with the same SSID and WPA-PSK as a victim's network [Evil-Twin]. Also, there are many deployments (for example, coffee shops and bars) that offer free Wi-Fi connectivity as a customer incentive. Since these businesses are not Internet service providers, they are often unwilling and/or unqualified to perform advanced (sometimes, complex) configuration on their network. In addition, customers are generally unwilling to

do complicated provisioning on their devices just to obtain free Wi-Fi. This leads to a popular deployment technique -- a network protected using a shared and public Pre-Shared Key (PSK) that is printed on a sandwich board at the entrance, on a chalkboard on the wall or on a menu. The PSK is used in a cryptographic handshake, defined in [IEEE802.11], called the "4-way handshake" to prove knowledge of the PSK and derive traffic encryption keys for bulk wireless data. The same deployement technique is typically used in residential or small office/home office networks. If the PSK for the wireless authentication is the same for all devices that connect to the same WLAN, the shared key will be available to all nodes, including attackers, so it is possible to mount an active on-path attack.

This document describes how a wireless client can utilize network-advertised encrypted DNS servers to ensure that the attacker has no more visibility to the client's DNS traffic than the legitimate network. In cases where the local network provides its own encrypted DNS server, the client can even ensure it has re-connected to the same network, offering the client enough information to positively detect a significant change in the encrypted DNS server configuration -- a strong indicator of an attacker operating the network.

The proposed mechanism is also useful in deployments using Opportunistic Wireless Encryption [RFC8110] and in LTE/5G mobile networks where the long-term key in the SIM card on the UE can be compromised (Section 1 of [AKA]).

The theory of operation is described mainly from the perspective of a host that connects to a network. Further interactions may be considered to seek for specific actions from a user (e.g., consent, validation). Whether and how such interactions are supported is implementation-specific and are, as such, out of scope.

The document assumes that the host supports at least one encrypted DNS scheme (e.g., DNS over TLS or DNS over HTTPS).

The current version of the specification focuses on wirless networks. The applicability to other network types may be assessed in future versions.

2. Conventions and Definitions

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. Theory of Operation

A host connects to a network and obtains network-related information via DHCPv4, DHCPv6, or RA. The network indicates its encrypted DNS server using either [DNR] or [DDR]. If the host supports an encrypted DNS scheme that is advertised by the network, the host then connects to at least one of the designated encrypted DNS servers, completes the TLS handshake, and performs public key validation of the presented certificate following conventional procedures.

The host can associate the network name with the encrypted DNS server's identity that was learned via [DNR] or [DDR]. The type of the network name is dependent on the access technology to which the host is attached. For networks based on IEEE 802.11, the network name will be the SSID of the network and the PSK. The PSK is used along with SSID to uniquely identify the network to deal with common Wi-Fi names such as "Airport WiFi" or "Hotel WiFi" or "Guest" but are distinct networks with different PSK. The combination of SSID and PSK is useful in deployments where the same Wi-Fi name is used in many locations around the world, such as branch offices of a corporation. It is also useful in Wi-Fi deployments that have multiple Basic Service Set Identifiers (BSSIDs) where 802.11r coordinates session keys amongst access points. However, in deployments using Opportunistic Wireless Encryption, the network name will be the SSID of the network and BSSID. For 3GPP access-based networks, it is the Public Land-based Mobile Network (PLMN) Identifier of the access network, and for 3GPP2 access, the network name is the Access-Network Identifier (see [RFC7839]).

If DDR is used for discovery, the host would have to perform verified discovery as per Section 4.2 of [DDR] and the encrypted DNS server identity will be the encrypted DNS server's IP address.

If DNR is used, the encrypted DNS server identity will be the Authentication Domain Name (ADN).

If this is the first time the host connects to that encrypted DNS server, the hosts follows [DNR] or [DDR] validation procedures, which will authenticate and authorize that encrypted DNS server's identity.

Better authentication can be performed by verifying the encrypted DNS server's certificate with the identity provided in an extended Wi-Fi QR code (Appendix A), consulting a crowd-sourced database, reputation system, or -- perhaps best -- using a matching SSID and SubjectAltName described in Section 4.

After this step, the relationship of SSID, PSK, encrypted resolver discovery mechanism, and SubjectAltName are stored on the host.

For illustrative purposes, Figure 1 provides an example of the data stored for two Wi-Fi networks, "Example WiFi 1" and "Example WiFi 2" (showing hashed PSK),

```
{
  "networks": [
    {
      "SSID": "Example WiFi 1",
      "PSK-ID": 12,
      "Discovery": "DNR",
      "Encrypted DNS": "resolver1.example.com"
    },
    {
      "SSID": "Example WiFi 2",
      "PSK-ID": 42,
      "Discovery": "DDR",
      "Encrypted DNS": [
           "8.8.8.8",
           "1.1.1.1"
      ]
    }
  ]
}
```

Figure 1: An Example of Data Stored for Two WiFi Networks

For illustrative purposes, Figure 2 provides an example of the data stored for two 3GPP2 networks,

```
{
  "networks": [
    {
      "realm": "ims.mnc015.mcc234.3gppnetwork.org",
      "Discovery": "DNR",
      "Encrypted DNS": "resolver2.example.com"
    },
    {
      "realm": "ims.mnc016.mcc235.3gppnetwork.org",
      "Discovery": "DDR",
      "Encrypted DNS": [
           "8.8.8.8",
           "1.1.1.1"
      ]
    }
  ]
}
```

Figure 2: An Example of Data Stored for Two 3GPP2 Networks

If this is not the first time the host connects to this same SSID, then the Wi-Fi network name, PSK identifier, encrypted resolver disovery mechanism, and encrypted DNS server's identity should all match for this re-connection. If the encrypted DNS server's identity differs, this indicates a different network than expected -- either a different network (that happens to also use the same SSID), change of the network's encrypted DNS server identity, or an Evil Twin attack. The host and/or the user can then take appropriate actions. Additionally, in a mobile network, the UE can send the discovered encrypted resolver's identity securely to the Mobile Core Network to assist it in identifying compromised base stations [NIST.SP.800-187]. It complements existing techniques [TR33.809] used to identify fake base stations.

4. Avoiding Trust on First Use

Trust on First Use can be avoided if the SSID name and DNS server's Subject Alt Name match. Unfortunately such a constraint disallows vanity SSID names. Also, social engineering attacks gain additional information if the network's physical address (123-Main-Street.example.net) or name (John-Jones.example.net) is included as part of the SSID. Thus the only safe SSID name provides no information to assist social engineering attacks such as a customer number (customer-123.example.net), assuming the customer number can safely be disclosed to neighbors. Such attacks are not a concern in deployments where the network name purposefully includes the business name or address (e.g., Public WiFi hotspots; 123-Main-Street.example.com, coffee-bar.example.com).

The Extensible Authentication Protocol (EAP), defined in [RFC3748], provides a standard mechanism for support of multiple authentication methods. EAP-TLS [RFC5216] specifies an EAP authentication method with certificate-based mutual authentication utilizing the TLS handshake protocol for cryptographic algorithms and protocol version negotiation and establishment of shared secret keying material. Many other EAP methods such as Flexible Authentication via Secure Tunneling (EAP- FAST) [RFC4851], Tunneled Transport Layer Security (EAP-TTLS) [RFC5281], the Tunnel Extensible Authentication Protocol (TEAP) [RFC7170], as well as vendor-specific EAP methods such as the Protected Extensible Authentication Protocol (PEAP) [PEAP], depend on TLS and EAP-TLS. In networks that use the EAP-TLS method or an EAP method that depends on TLS, if the SSID name matches one of the subjectAltName entries in the EAP-TLS server certificate, Trust on First Use can be avoided. It is especially useful in deployments where the endpoint is not managed using an MDM. For instance, it can be used during the device registration process (e.g., using Over-The-Air (OTA) enrollment [OTA] to provision the device with a certificate and configuration profile) or in networks (e.g., emergency services as discussed in Section 2.1.5 of [RFC9190]) where client authentication is not required or in networks that use password to authorize the client to access the network (e.g., using password authenticated key exchange with TLS).

5. Security Considerations

The network-designated resolver may or may not be local to the network. DDR is useful in deployments where the local network cannot be upgraded to host a encrypted resolver and the CPE cannot be upgraded to support DNR. For example, DDR is typically used to discover the ISP's encrypted resolver or a public encrypted resolver. The encrypted resolver discovered using DNR may be a public encrypted resolver or hosted by the local network or by the ISP. The mechanism specified in this document does not assist the client to identity if the network-designated resolver is hosted by the local network. However, it significantly reduces the attacker's capabilities if the attacker is emulating a network (that is, operating a look-alike network).

More and more content delivery networks, sensitive domains and endpoints are migrating to TLS 1.3 and ECH. If the attacker's network conveys the same encrypted revolver's identity as the legitimate network, it will not have any visibility into the private and sensitive information about the target domain. However, the attacker's network will still have visibility into the traffic metadata like the destination IP address, sequence of packet lengths, inter- arrival times, etc.

The network authentication mechanism relies upon an attacker's inability to obtain an application PKI certificate for the victim's configured encrypted DNS server.

Neither a plain-text PSK nor hash of the PSK is necessary for the mechanism described in this document; rather, an implementation can use a key identifier.

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. Normative References

[DDR] Pauly, T., Kinnear, E., Wood, C. A., McManus, P., and T. Jensen, "Discovery of Designated Resolvers", Work in Progress, Internet-Draft, draft-ietf-add-ddr-10, 5 August 2022, <https://www.ietf.org/archive/id/draft-ietf-add-ddr-10.txt>.

[DNR] Boucadair, M., Reddy.K, T., Wing, D., Cook, N., and T. Jensen, "DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)", Work in Progress, Internet-Draft, draft-ietf-add-dnr-13, 13 August 2022, <https://www.ietf.org/archive/id/draft-ietf-add-dnr-13.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>.

[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>.

7.2. Informative References

[AKA] Arkko, J., Norrman, K., Torvinen, V., and J. P. Mattsson, "Forward Secrecy for the Extensible Authentication Protocol Method for Authentication and Key Agreement (EAP-AKA' FS)", Work in Progress, Internet-Draft, draft-ietf-emu-aka-pfs-08, 23 October 2022, <https://www.ietf.org/archive/id/draft-ietf-emu-aka-pfs-08.txt>.

[Evil-Twin] Wikipedia, "Evil twin (wireless networks)", June 2022, <https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks)>.

[IEEE802.11]
Wikipedia, "IEEE802.11", August 2022, <https://en.wikipedia.org/wiki/IEEE_802.11>.

[NIST.SP.800-187] OTA, "Over-the-Air Profile Delivery Concepts", April 2018, <https://developer.apple.com/library/archive/documentation/NetworkingInternet/Conceptual/iPhoneOTAConfiguration/OTASecurity/OTASecurity.html>.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", RFC 3748, DOI 10.17487/RFC3748, June 2004, <https://www.rfc-editor.org/info/rfc3748>.

[RFC4851] Cam-Winget, N., McGrew, D., Salowey, J., and H. Zhou, "The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST)", RFC 4851, DOI 10.17487/RFC4851, May 2007, <https://www.rfc-editor.org/info/rfc4851>.

[RFC5216] Simon, D., Aboba, B., and R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216, DOI 10.17487/RFC5216, March 2008, <https://www.rfc-editor.org/info/rfc5216>.

[RFC5281] Funk, P. and S. Blake-Wilson, "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)", RFC 5281, DOI 10.17487/RFC5281, August 2008, <https://www.rfc-editor.org/info/rfc5281>.

[RFC7170] Zhou, H., Cam-Winget, N., Salowey, J., and S. Hanna, "Tunnel Extensible Authentication Protocol (TEAP) Version 1", RFC 7170, DOI 10.17487/RFC7170, May 2014, <https://www.rfc-editor.org/info/rfc7170>.

[RFC7839] Bhandari, S., Gundavelli, S., Grayson, M., Volz, B., and J. Korhonen, "Access-Network-Identifier Option in DHCP", RFC 7839, DOI 10.17487/RFC7839, June 2016, <https://www.rfc-editor.org/info/rfc7839>.

[RFC8110] Harkins, D., Ed. and W. Kumari, Ed., "Opportunistic Wireless Encryption", RFC 8110, DOI 10.17487/RFC8110, March 2017, <https://www.rfc-editor.org/info/rfc8110>.

[RFC8792] Watsen, K., Auerswald, E., Farrel, A., and Q. Wu, "Handling Long Lines in Content of Internet-Drafts and

RFCs", RFC 8792, DOI 10.17487/RFC8792, June 2020, <https://www.rfc-editor.org/info/rfc8792>.

[RFC9190] Preuß Mattsson, J. and M. Sethi, "EAP-TLS 1.3: Using the Extensible Authentication Protocol with TLS 1.3", RFC 9190, DOI 10.17487/RFC9190, February 2022, <https://www.rfc-editor.org/info/rfc9190>.

[TR33.809] 3GPP, "Study on 5G Security Enhancement against False Base Stations", June 2022, <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3539>.

Appendix A. Extending WiFi QR Code

This section is non-normative and merely explains how extending the Wi-Fi QR code could work.

QR codes come with their own security risks, most signficant that an attacker can place their own QR code over a legitimate QR code.

Several major smartphone operating systems support a QR code with the following format for the SSID "example" with WPA-PSK "password",

```
WIFI:T:WPA;S:example;P:password;;
```

This could be extended to add a field containing the identity of the encrypted DNS server. As several DNS servers can be included in the QR code with "D:", each DNS server with its own identity using [RFC8792] line folding,

```
=============== NOTE: '\' line wrapping per RFC 8792 ================

WIFI:T:WPA;S:example;P:password; \
D:ns1.example.net,D:ns.example.com;;
```

Acknowledgments

This document was inspired by both Paul Wouters and Tommy Pauly during review of other documents.

Thanks to Mohamed Boucadair for the review.

Authors' Addresses

Dan Wing
Citrix

Email: danwing@gmail.com

Tirumaleswar Reddy
Nokia

Email: kondtir@gmail.com