Technical Disclosure Commons

Defensive Publications Series

July 03, 2019

SECURE WIRELESS CLIENT ONBOARDING AND SEGMENTATION

Amine Choukir

Roberto Muccifora

Domenico Ficara

Vincent Cuissard

Antonio Trifilo

See next page for additional authors

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation

Choukir, Amine; Muccifora, Roberto; Ficara, Domenico; Cuissard, Vincent; Trifilo, Antonio; and Valenza, Salvatore, "SECURE WIRELESS CLIENT ONBOARDING AND SEGMENTATION", Technical Disclosure Commons, (July 03, 2019)
https://www.tdcommons.org/dpubs_series/2323

This work is licensed under a Creative Commons Attribution 4.0 License.

This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

Inventor(s)
Amine Choukir, Roberto Muccifora, Domenico Ficara, Vincent Cuissard, Antonio Trifilo, and Salvatore Valenza

This article is available at Technical Disclosure Commons: https://www.tdcommons.org/dpubs_series/2323

SECURE WIRELESS CLIENT ONBOARDING AND SEGMENTATION

AUTHORS:
Amine Choukir
Roberto Muccifora
Domenico Ficara
Vincent Cuissard
Antonio Trifilo
Salvatore Valenza

ABSTRACT

Techniques are described herein for preventing Media Access Control (MAC) address spoofing attacks based on the two-step onboarding process for open Service Set Identifiers (SSIDs) due to Virtual Local Area Network (VLAN) override after the Internet Protocol (IP) address is learned. These techniques leverage Opportunistic Wireless Encryption (OWE) and an access token to provide a secure channel between the wireless network and the client.

DETAILED DESCRIPTION

Wireless client onboarding and segmentation through open Service Set Identifiers (SSIDs) require the client to join a base Virtual Local Area Network (VLAN) associated with the SSID, acquire an Internet Protocol (IP) address to proceed with web authentication, and then change VLANs based on the type of service/policies that need to be applied. The change of VLAN involves changing subnetworks after the client has already acquired an IP address on the base VLAN. Current solutions for VLAN override after Web Layer 3 (L3) Authentication are brittle and require disassociating the client while retaining the client state on the wireless controller for some time while awaiting client rejoin. The Media Access Control (MAC) address of the client is used to fetch the state of the client without an additional re-authentication, which potentially allows for MAC address spoofing attacks.

Accordingly, techniques are presented herein which leverage Opportunistic Wireless Encryption (OWE) to provide a secure channel between the wireless network and the client. During the authentication procedure, a results page from the portal returns a secure token as part of a new Hypertext Transfer Protocol (HTTP) header. The token is

Published by Technical Disclosure Commons, 2019

supplied during rejoin through the same HTTP header to the portal, which skips the credential request based on the validation of the token.

Universally Unique Identifiers (UUIDs) version 4 variant 1 as defined in Internet Engineering Task Force (IETF) Request for Comments (RFC) 4122 are leveraged for the token. Furthermore, a new Access_token HTTP header is added. Browsers may be requested to store and return cookies to improve seamlessness on the client side.

Figure 1 below illustrates a sequence diagram that provides an example onboarding flow.

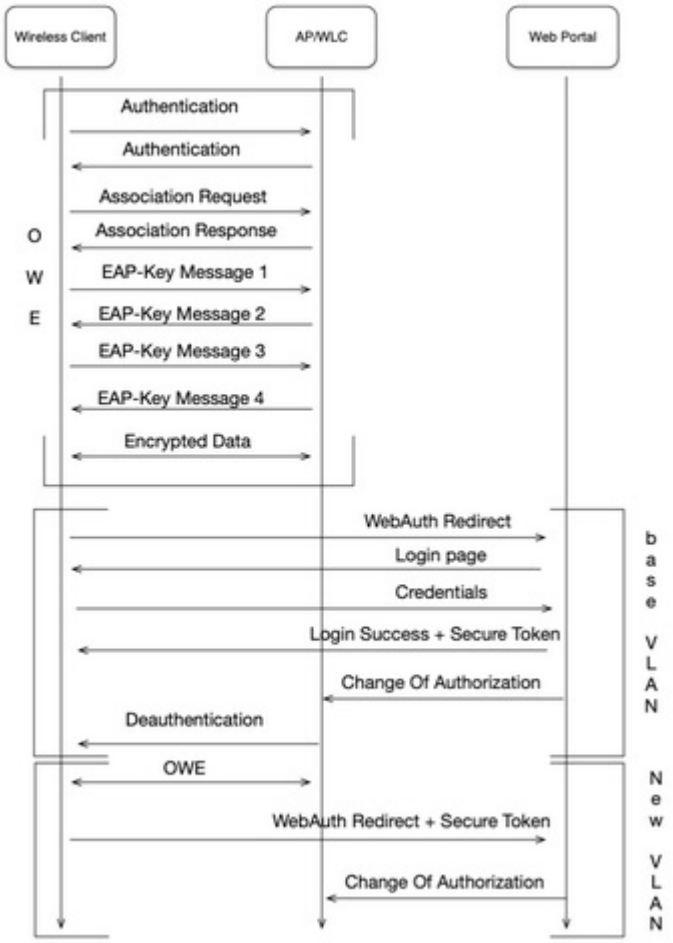

Figure 1

This solution prevents MAC address spoofing attacks after client de-authentication upon VLAN override, providing an additional level of security to the VLAN override functionality. These techniques also integrate seamlessly into the web authentication process.

The solution may be further enhanced by extending OWE to at least perform Access Point (AP) - side certificate validation. This may be similar to operations currently performed by the browser based on pre-installed root chains.

If OWE is not required, the solution may still apply by requiring HTTP Secure (HTTPS) during the web authentication process. The procedure for generating the token and validating on the portal may remain the same, but the secure channel mechanism may change.

This solution is also compatible with other Layer 2 (L2) authentication procedures (e.g., dot1x, Pre-Shared Key (PSK), etc.) because the access token is provided during the web authentication phase.

In summary, techniques are described herein for preventing MAC address spoofing attacks based on the two-step onboarding process for open SSIDs due to VLAN override after the IP address is learned. These techniques leverage OWE and an access token to provide a secure channel between the wireless network and the client.