July 2021

PRESENCE VALIDATION USING SECURED INTERNET PROTOCOL (IP) ADDRESS

Patrick Wetterwald

Eric Levy- Abegnoli

Pascal Thubert

Jonas Zaddach

PRESENCE VALIDATION USING SECURED INTERNET PROTOCOL (IP) ADDRESS

AUTHORS:
Patrick Wetterwald
Eric Levy- Abegnoli
Pascal Thubert
Jonas Zaddach

ABSTRACT

Various presence-based validation technologies exist that provide for the ability add identity and presence validation to a laptop-based system. However, these technologies are primarily limited to computers (e.g., desktops and laptops) and do not include location validation. There is a need to extend these capabilities to other devices connected to a network and also to eliminate the need for a hardware-assisted solution. There is also a need to offer network location to avoid any type of attack from devices that are not connected to a local area network (LAN) or even to the same port. This proposal provides a technique to ensure that a device/person is present at a location by observing that the device/person performed an activity on-site, which can be observed by a trusted third-party.

DETAILED DESCRIPTION

Current technologies that utilize a presence check of a device to provide device/network security involve a user interaction but do not check/verify the network location of the device. Further, current technologies do not utilize IP version 6 (IPv6) capabilities.

This proposal provides a unique software security solution that provides for the ability to check the presence of any network device, including device identity and device location. In particular, the solution of this proposal ensures that a device/person is present at a location by observing that the device/person performed an activity on-site that can be observed by the third-party, for example, adding a link-local address in a network binding table and/or in router neighbor caches, and asking that trusted third-party whether the activity was performed.

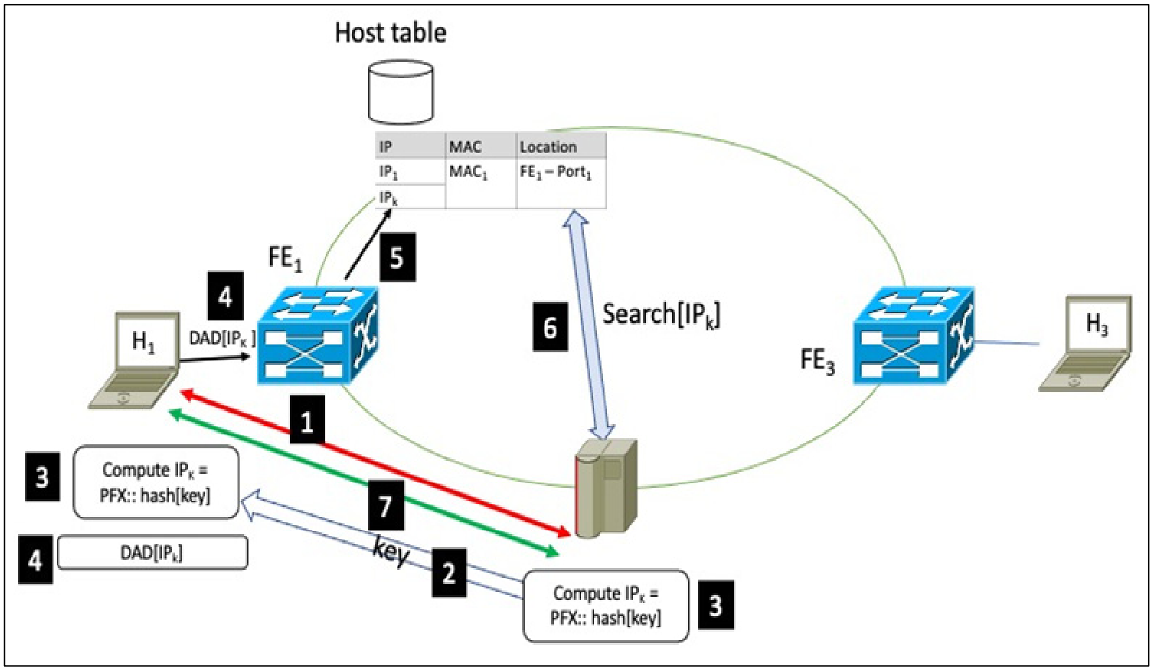
The solution is based on IPv6. For example, in a first step, a certificate is installed in a device to be authenticated (e.g., via a soft token or other similar mechanism). This first step (1) can be performed offline during a commissioning phase of the device. For a second step (2), when an application running on a server needs to check the presence of the device (identify and location), the application sends a request (including a generated session key) to the IP address of the device. As referred to herein, the term "location" is meant to refer to a network location (e.g., for access switch). Access switches are very often geographically located (in a building, office, home, etc.).

For a third step (3), when receiving this request, the device builds a second IPv6 address using the auto-configuration capability and computes the Interface Identifier (IID) part of the address by using the certificate and the key obtained from the server. The result of this computation provides a topologically correct IPv6 address that could be installed in the network. The server on its side performs the computation, so now both the device and the server know this IPv6 address. According to the security requirement, this address will have a specific lifetime. In one instance, the time for the computation performed by each of the device and the server can also be introduced as an additional layer of security.

For a fourth step (4), the computed address is installed in the network. In a switch fabric, it will be populated in the host table. In a standard LAN, it will use the regular IPv6 mechanism with Duplicate Address Detection (DAD). For a fifth step (5), the server or application can now regularly check that the address is still present (e.g., by using an Internet Control Message Protocol (ICMP) PING). The fact that this address is valid and installed in the network proves the presence and identity of the device.

In another instance, switch security functionality can be enhanced to also check that the second IPv6 address is on the same port as the device address adding a location check to this system. Other capabilities such as regular IP address checking, attack, IP address removal, etc. may be provided by such switch security functionality. In some instances, if needed and if 64-bits is not seen as a sufficient security level, a third IP address could be generated adding another 64-bits to the address.

Figure 1 below illustrates example details associated with an application of this solution within a Software-Defined Access (SDA) network, including a Fabric Edge (FE) switch and a centralized Host Table through which all IP addresses are known. In one instance, the Host Table can be accessed using the Locator/ID Separation Protocol (LISP).



IP	MAC	Location
IP$_1$	MAC$_1$	FE$_1$ – Port$_1$
IP$_k$		

Figure 1: Solution Application within an SDA Network

Consider a bootstrap sequence that can be performed via the SDA network of Figure 1, as follows:

1. Host H$_1$ establishes a session with the server that requires double authentication.
2. The server generates the session key and sends it to the host H$_1$.
3. The host computes an IPV6 address, IP$_K$, (e.g., using Stateless Address Auto-Configuration (SLAAC)) with a link-id built after a hash of the key. The server does the same.
4. The host "registers" this address to the network (using Neighbor Discovery (ND) registration), and simply checks for duplication (e.g., DAD).
5. In both cases, an ND packet is sent that the Fabric Edge, FE$_1$, intercepts and uses to push the IP$_K$ into the host table.

6. The server queries the host table for IP_K. If it is present, it means: (i) That the host H_1 received the key, and (ii) that the host is attached at the expected location (FE_1).
7. The host session can proceed.

It should be noted that only the host H_1 can remove the address IP_K (there is always a location check before allowing a removal) and only H_1 can add the address IP_K (the key was sent only to the host).

IPv6 has become the standard evolution of current networks. Almost all the devices, including personal computers, laptops, mobile devices (e.g., utilizing 5G mobile networks), etc. support IPv6. Further, industrial wireless networks, such as International Society of Automation (ISA) protocol ISA100, utilizes IPv6. Additionally, the United States government has issued a directive to move to all of their networks to "IPv6 only" (not only dual stack) by 2025 (e.g., 80%).

IPv6 offers a huge address space and also utilizes DAD mechanisms as discussed for the solution of this proposal. Thus, in the rare case of a duplicate address, the duplication can be detected by the network/device and the device just asks the server to generate a new session key to restart the process from the beginning, similar to SLAAC. Thus, the solution of this proposal fits perfectly within the evolution of today's networks.

It should be noted, however, that while the solution described herein involves a device running IPv6, the solution does not require the network to support IPv6 for routing, etc. Rather, the IPv6 address set by the device application is pushed to the application's point of attachment and become an opaque (cryptographic) token, which happen to be 128-bits. From there, the token is installed in the host table and accessed. The token can be accessed using IPv4 standards if a network has not enabled v6.

Although a similar solution could be provided in the IPv4 space, the limitation of IPv4 in term of number of bits may be too restrictive for the average required security level. Still, even if a device is not using IPv6 for an application's communication, the device can forge an IPv6 address to support the solution of this proposal if the access network supports IPv6.

Further, it should be noted that the authentication solution of this proposal does not require a custom server to poll for the presence of the IP address regularly. Many popular fabric-based networks involving a host table can utilize standard technologies to implement the authentication solution of this proposal, such as LISP, NETCONF/YANG, Border Gateway Protocol (BGP), etc.

In contrast to other authentication mechanisms, such as dot1x (.1x), it is noted that while .1x offers a trusted/authenticated LAN network access mechanism, the solution of this proposal provides more of an application-level authentication solution, which, in some sense, may even also be above Virtual Private Network (VPN) solutions. In essence, the solution of this proposal provides an application-to-application authentication solution.

In summary, the solution of this proposal provides for the ability to ensure that a device/person is present at a location by observing that the device/person performed an activity on-site, which can be observed by a trusted third-party. As one example, the solution involves forming a link local IPv6 address with a cryptographic IID that only the correct device can compute and observing that the address is present on link. For instance, the trusted third-party can check that the address that is added is a link-local address in a network binding table / router neighbor caches, and it is possible, at any time to, to ask the trusted third-party whether the activity was performed and possibly to assert the presence of the link local address by pinging the address.