April 2021

PASSWORD-LESS CONTINUOUS MULTIFACTOR AUTHENTICATION (CFMA) FOR WIRELESS NETWORKS

Vinay Saini

Jerome Henry

Tim Szigeti

Robert Barton

PASSWORD-LESS CONTINUOUS MULTIFACTOR AUTHENTICATION (CFMA) FOR WIRELESS NETWORKS

AUTHORS:
Vinay Saini
Jerome Henry
Tim Szigeti
Robert Barton

ABSTRACT

The new generation of wireless networks can involve a mix of radio technologies, especially for industrial environments. As devices roam back and forth between different radio networks, it is very difficult to continually monitor the security posture and identity of devices connected to the network. Presented herein are techniques that involve the combination of a Device-Generated Trust Card and a Network-Generated Trust Card that can be used to validate device identity (e.g., an Internet of Things (IoT) device identity) and behavior using a continuous Multi-Factor Authentication (cMFA) structure.

DETAILED DESCRIPTION

With the mix of many different radio technologies in current wireless networks, it can be difficult to continually monitor the security posture and identity of a device connected to a network as the device roams back and forth among different radio networks (e.g. Wi-Fi, 5G, etc.). Most radio technologies perform a single authentication of a device at the time of association and then never examine the device again. In the case of human users of a device, continuous Multi-Factor Authentication (cMFA) can be utilized via biometrics, etc. to continually ensure that the human is the correct user of the device. However, it is not possible to do this for a wirelessly connected machine that may use a variety of wireless access methods.

Stated differently, there is currently no mechanism to provide differentiated access based on the state of a machine. For example, when a machine behaves differently with excessive vibrations or heat, etc., it might be due to an ongoing cyber-attack or other issues (e.g., Stuxnet, etc.) that need to be treated differently based on device behavior. Traditional methods of Subscriber Identification Module (SIM)/SIM-based authentication also do not

consider the machine state and its behavior on the network before providing access (which provides context to the device). Even traditional Wi-Fi systems are looking forward to password-less authentication and on-boarding, but most methods involving Wi-Fi systems are targeted at identifying users as opposed to continuous authorization of machines on network.

For example, authentication methods such as Pre-Shared Key (PSK) authentication or Extensible Authentication Protocol Transport Layer Security (EAP-TLS) allow a device to gain access to the network but once this access is gained, however, these methods do not implement any mechanisms to continuously validate if the device should still be allowed to communicate through the network.

Thus, there is a need for a secure and efficient method for Wi-Fi cMFA that goes beyond standard methods of one-time authentication/authorization that is used in current communication systems.

For critical communication systems that involve non-human connected devices, one-time authentication and authorization is not enough. This proposal provides a cMFA technique for wireless devices that continuously authenticates and authorizes devices. Figure 1, below, illustrates an example system flow that can be utilized in accordance with the techniques of this proposal in order to achieve continuous authentication/authorization for wireless devices.

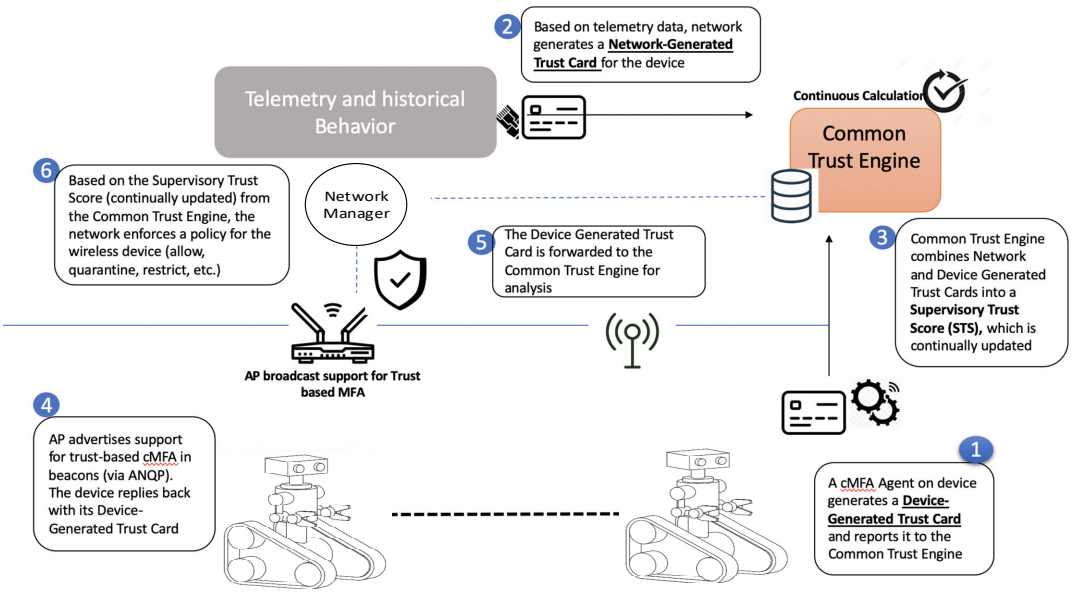

Figure 1: Example System Flow for Continuous Authentication/Authorization of a Device

As illustrated in Figure 1 at (1), any machine/device within the environment is to host a cMFA agent in a Trusted Execution Environment (TEE). The cMFA agent runs on the device and collects information about the device to which it is connected, such as:

- Identity of the device (in various formats);
- Running behavior and uptime of the device; and/or
- IoT sensor data of the device (vibrations, temperature, pressure, etc.).

This list of metrics can be used to create a real-time profile of the device called, referred to herein as a Device-Generated Trust Card that is continually updated with fresh data as it is collected on the device. The Device-Generated Trust Card is reported to a Common Trust Engine (CTE) in the network, as discussed below.

At (2), as the device communicates over the network, its interaction is continuously monitored using existing techniques of telemetry collection and a Network Generated Trust Card is generated and continually updated for this device. There are now two trust cards: the Device-Generated Trust Card and the Network-Generated Trust Card. The concept of trust decay can be applied to the two trust cards to continually update information about the behavior of the device.

As shown at (3), a new entity referred to herein as the Common Trust Engine combines the Device-Generated and the Network-Generated trust cards to create a global Supervisory Trust Score (STS) for the device that is centrally stored and can be queried for various authentication and authorization purposes. The Supervisory Trust Score is meant to include the perspectives both from the device level (from the Device-Generated card) and from the network level (from the Network-Generated card), both of which are continually reassessed.

When a device, such as an Automated guided Vehicle (AGV), tries to connect to the Wi-Fi network, the following operations can be performed, as shown at (4):

- The Wi-Fi AP broadcasts support for trust-based MFA. This could be done in specific areas based on need (e.g., per AP group/Location); and
- The device sends a request to initiate on-boarding by providing its unique Device-Generated Trust Card. It should be noted that the Device-Generated

Trust card can reveal anomalies in the device of which the network may not be aware.

As part of the on-boarding process as shown at (5), the Device-Generated Trust Card is forwarded to the Common Trust Engine and the Common Trust Engine combines the Device-Generated Trust Card with the Network-Generated Trust Card (if one exists from previous behavior). If the device is a known device, the Supervisory Trust Score is updated. If the device is unknown to the network (e.g., a new device to the network), a Network-Generated Trust Card is created with default values until more information for the device is learned and the Supervisory Trust Score can be updated.

Based on the Supervisory Trust Score (STS), the network policy may allow the device to continue to communicate with the network (if the score is high enough), may restrict the device (such as a quarantine, if the score is within one or more ranges), or may disconnect the device if the score falls below a critical value, as shown at (6). The Wi-Fi access point (AP) and/or network manager can continuously poll the trust engine to check the trust score. Anomalies can reduce the trust score and force the device into maintenance/limited interaction.

Validation of the Device-Generated Trust Card can take several forms. For example, 50 identical devices are expected to behave the same way, thus, one technique may involve a probabilistic comparison of trust card values between similar devices. Another technique may involve a mechanism such as Manufacturer Usage Description (MUD) to retrieve a card profile range for a target device from a vendor of the target device. In contrast, validation of the Network-Generated Trust Card is based on traffic activity and can utilize any known techniques for validation.

As compared to other authentication mechanisms such as PSK or EAP-TLS, use of cMFA provides not only provides for the ability for a device to gain access to a network, but also provides for maintaining the access once connected. Consider an example in which a device is allowed to access a network (via PSK or EAP-TLS) and establishes a secured connection to a server. Thereafter, if the server is compromised, an attacker could use the trusted connection to push additional daemons to the device that could allow the device to explore the local area network. EAP-TLS has no mechanism to prevent this issue.

However, following the techniques of this proposal, the device-generated trust score would suddenly drop in such a scenario. For any peer-to-peer (P2P) exchange, the network would not detect anything (such as the value of the Device-Generated card) and for infrastructure-based exchanges, the Network-Generated card would also be affected. Thus, the techniques proposed herein would detect such an attack.

In summary, techniques presented herein involve the combination of a Device-Generated Trust Card and a Network-Generated Trust Card that can be used to validate device identity and behavior using a cMFA structure. An advantage of such techniques is that anomalies or impersonations can be detected from either the device side or the network side of an authentication; thus, each side moderates possible poisoning from the detection logic of the other side.