June 2021

PASSWORD-LESS TRUST BASED ACCESS AUTHORIZATION FOR REMOTE INTERNET-OF-THINGS (IOT) DEVICES

Shweta Palande

Shivani Suri

Madhuri Dewangan

Vinay Saini

PASSWORD-LESS TRUST BASED ACCESS AUTHORIZATION FOR REMOTE INTERNET-OF-THINGS (IOT) DEVICES

AUTHORS:
Shweta Palande
Shivani Suri
Madhuri Dewangan
Vinay Saini

ABSTRACT

The industry is moving away from password-based authorizations as they are often difficult to manage and are associated with various risks. Techniques herein solve an important issue with regard to remote Internet of Things (IoT) gateway access by utilizing a password-less trust-based authentication mechanism through which dynamic trust-based authorizations can be provided for devices utilizing a combination of a user trust score and a device risk profile in a unique manner. Such an approach will improve IoT security and will also help to solve an important security issue within the IoT/industrial world.

DETAILED DESCRIPTION

A typical IoT environment may include thousands of sensors that connect to their respective gateways. As this network continues to grow, more and more edge devices, sensors, and gateways to manage the devices are typically added to such a network. As the sensors often come from different vendors, there is often continuous maintenance work that occurs as new sensors are added to the network or older ones are replaced.

Such network management/updates typically involve access to the edge gateways by different vendors in order to make configuration adjustments and/or install specific applications/micro-services. There are different mechanisms to access edge devices, such as remote access via some cloud management service, direct console access, or access via standard remote connections such as a virtual private network (VPN). All of these methods involve some form of password-based authentication and authorization mechanism to login to edge devices, which many times are based on a standard active directory for a common troubleshooting access. This poses a great security threat in which the chances of misconfiguring or exposing sensor data and/or information is very high.

Thus, existing method of access control rely on the credentials for providing access to IoT gateways. It is often observed that such credentials are shared between employees to avoid the hassle of creating new accounts. This also creates a security issue for the entire network as sensors from different vendors are often connected to these edge devices. There is no existing technique to control access to a specific section of a gateway configuration based on the true identity of the requestor or a trust factor associated with that individual.

As per the Open Web Application Security Project (OWASP) 2018, the top vulnerabilities for IoT networks are primarily concerned with security aspects, such as:

- Weak Guessable or Hardcoded Passwords;
- Insufficient Privacy Protection and Authorization;
- Lack of Device Management;
- Insecure Default Settings; and/or
- Lack of Physical Hardening.

One can easily find a list of commonly used passwords on the web and apply brute force to break-in to/access a secure system. Statistics that show even with the awareness of weak passwords and their associated security threats, many companies still are not 100% safe from the threats that originate from secure access.

Another major concern with a password-based or simple Multi-Factor Authentication (MFA)-based solution is that a user is authenticated or authorized only once during an initial login and is not continuously monitored if the same person is accessing the network device post-validation.

Accordingly, there is a dire need for a solution that tackles these issues and strengthens the accessibility of IoT gateways or endpoints, especially in an environment in which these gateways cannot be physically secured.

To combat such issues as noted above, this proposal provides a novel solution that generates a risk profile of any user who wishes to attempt a login into a gateway, edge device, or an IoT console. The risk profile is a unique profile of a user that calculates a risk factor of the user and determines what type of access are recommended for the user. The risk profile can be stored into a device. There are a multitude of parameters that can be used to ensure that a given user accessing a given endpoint is exposed to only the specific portion of the endpoint, which goes beyond the standard password-based authentications that are typically provided in networks. Accordingly, techniques of this proposal provide a novel solution that allows password-less continuous authentication/authorization of a user to access a specific configuration on an IoT gateway via different access methods.

In order to explain the solution of this proposal, consider, as an example, a situation involving a healthcare IoT infrastructure in which there are hundreds of medical sensors deployed at a network edge that are connected to the IoT gateways. In a scenario in which a technician is required to login to the IoT gateways to access the sensors, a generic company username and password may be provided that the technician can use to login to the gateways. At times, the technician can also login via a personal computer and establish a Secure Shell (SSH) or Telnet connection. However, there may be scenarios where a fellow colleague uses the authorized personal device to gain quick access. Many times, the generic username/password is also passed to others in order to perform a quick fix over the devices. Scenarios like this open-up possibilities for security breaches and misconfigurations or exposure of data.

In order to augment secure access, this proposal provides for applying the concept of a trust score in a novel manner so that it can be integrated into a Continuous MFA (CMFA) ideology.

Common endpoints such as mobile devices are the bridge to many Two-Factor Authentication (2FA) mechanisms such that the same mobile endpoint can be used as a tool in continuously authenticating a user and the user's identity. In accordance with techniques of this proposal, a trust score can be tied to a mobile endpoint using a CMFA agent that could be deployed as dedicated hardware and/or software in a trusted execution environment (TEE). This trust score can include:

- Who a user is, based on his/her gait, biometrics, personality traits, etc., which can be sent by the mobile device; and
- The previous history of login attempts, resets, domain access, and device configuration change of devices (e.g., collected from logs). This information can be collected from the mobile device and added by a cloud server to create an enhanced trust score.

Consider an example workflow, as follows:

1) A user performs a login to an *IoT Operations Center* with credentials;

   Note: IoT Operations Center is assumed to be a cloud-based application/platform to manage IoT gateways and devices.

2) When a user tries to access one of the connected gateways remotely, the user trust score is pulled from the CMFA agent running on a mobile device of the user. A domain name that includes the domain associated with the user and the user's device details are sent to a trust engine or logic that calculates the enhanced trust score based on: the trust score of the user + the domain name + any previous configuration changes and device access details;
3) This trust score is sent to an Identity and Access Management (IAM) server, which generates tokens based on the trust score and role assigned to the user. This generated token can then be used to connect to a gateway remotely with allowed access that is based on various factors;
4) Configuration on the device will be categorized into a specific zone that can include:
   - Critical connectivity;
   - Device configuration;
   - An Organizationally Unique Identifier (OUI)-based show configuration; or
   - A protocol-based configuration (e.g., Message Queuing Telemetry Transport (MQTT), connectors, micro-service access, etc.).

The access token authorizes the user/vendor to access a specific part of a configuration and keeps sending accounting updates associated with the token. If the trust score reduces or the user attempts to make unauthorized changes, this results in the token being invalidated and the trust score decayed for the individual. Figure 1, below, illustrates an example system flow for providing console access to an IoT gateway using a trust-based access token.

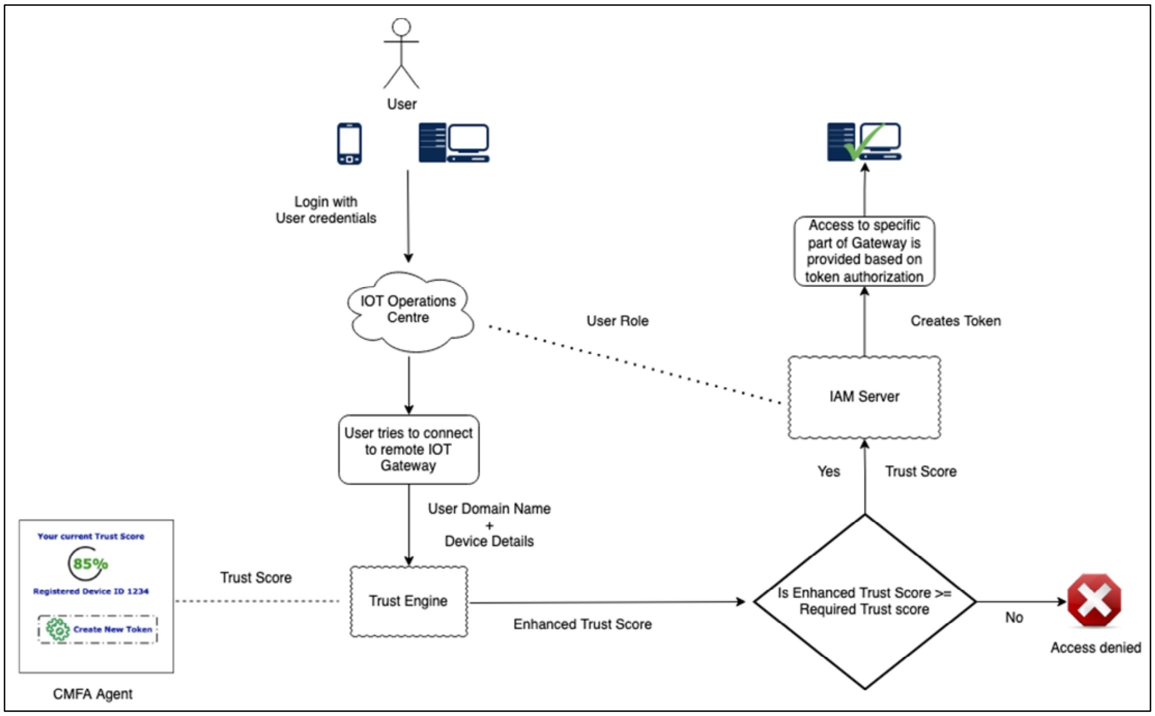

Figure 1: Example Operational Flow Involving Local Access to an IoT Gateway using a Trust-Based Access Token

For the technique as illustrated in Figure 1, it is assumed that the IoT gateway has connectivity to an IoT Operations Center, but the user is trying to access the device using local console access. In such a use-case, the user authentication would proceed as follows:

1) When the user opens the trust score application, the most current, valid trust score is generated. The mobile device of the user already has its device identity (ID) registered. (Device ID is a parameter that determines the authoritative access of the user within the user's organization);
2) When the user clicks on 'Create Token' within the application, the access token is created based on the combination of the trust score and the device ID. Thus, the access token that can be created is based on:
    i. Device ID parameters that indicate an access level for the user; and
    ii. Trust score parameters that indicate how much access is safe to give to the user.
3) The access token is now passed to the Operations Center, which determines the level of access to be granted to its user. The Operations Center

commands the remote gateway to display a Quick-Response (QR) code on the device screen, which the user can scan via the user's mobile device;

4) If this scan proceeds correctly, the client/mobile endpoint will send an OK signal to the server and the user obtains access to the remote gateway;
5) The trust score is continuously verified by the trust engine in the IoT Operations Center. In one instance, the verification could be facilitated via a Near-Field Communication (NFC) or Bluetooth™ link between the device and the user's mobile device.

The entire method can be transparent to the user and he/she just needs to scan the QR code.

Consider another technique, for a use-case in which it is assumed that the IoT gateway does not have connectivity to the IoT Operations Center vendor and a user desires direct console access.

For this use-case, the authentication would proceed via out-of-band authorization provisioning, as described below and as illustrated in Figure 2, as follows:

1) With the help of Bluetooth™ or any NFC technology, the IoT gateway can detect the presence of the mobile device requesting access to the direct console (assuming that IoT gateway is enabled for NFC/Bluetooth™ communications). The user will generate the access request and will share the access request with the gateway. Based on the request received, the device will generate an Access-Request Code that includes a hash of the device ID, serial number, Media Access Control (MAC) address, and/or other details;
2) The generated Access-Request Code is passed to CMFA agent on the mobile device, which then combines the trust score and user domain and submits the same to the IoT Operations Center for console access approval; and
3) The IoT Operations Center will generate an access token with a specific access level binding and passes the access token back to the mobile device, which the user can use to obtain direct console access.

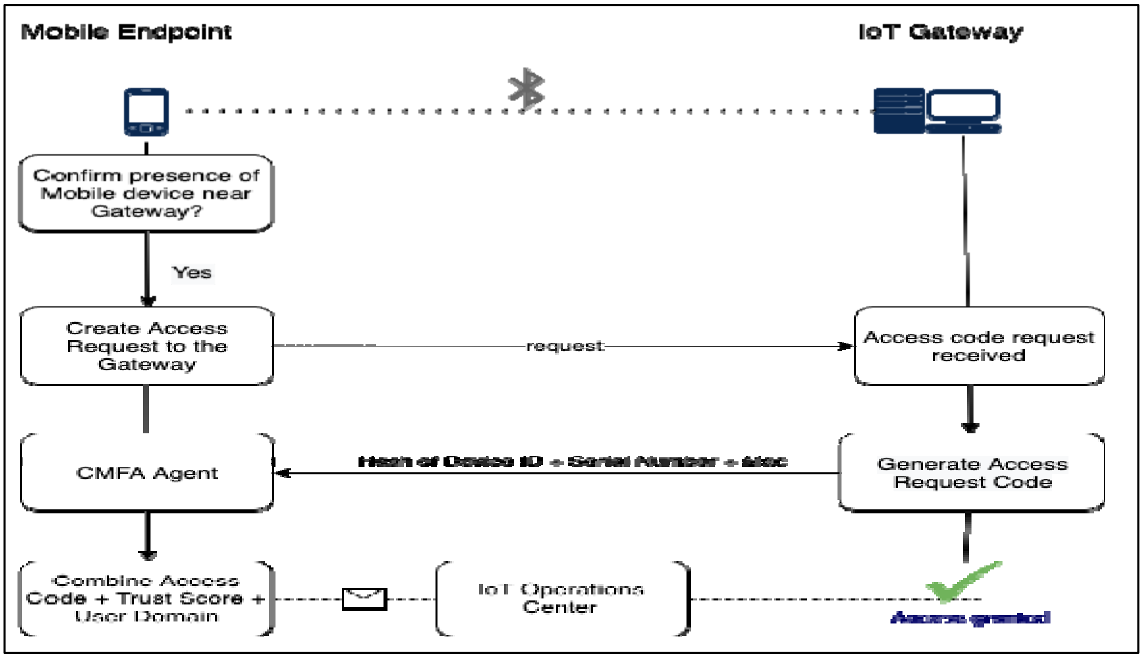
Mobile Endpoint
IoT Gateway
Confirm presence of Mobile device near Gateway?
Yes
Create Access Request to the Gateway
request
Access code request received
CMFA Agent
Hash of Device ID + Serial Number + Mac
Generate Access Request Code
Combine Access Code + Trust Score + User Domain
IoT Operations Center
Access granted

Figure 2: Example Operational Flow

Thus, techniques herein provide for establishing and verifying user identity in a continuous manner by combining: a continuous validation if the same user is accessing the network all the time, a continuous validation of the user's behavior with a specific device on the network; and historical access to the device and/or changes from the same or different user sets. Additionally, techniques herein can be utilized through both in-band or out-of-band transport scenarios that facilitate CMFA-based authorizations in a secure, yet easy-to-use solution.

In contrast to other potential solutions involving cryptographic operations, techniques herein provide for authenticating a user based on an enhanced trust score that is calculated based on the user's previous activity on the network, the device in-use, and continuous validation of user-device combination. Along with this, the solution of this proposal seeks to authenticate users based on an updated risk factor in a continuous interval of time so that impersonation of the critical infrastructure or session hijacking types of attacks can be prevented. In the solution provided herein, if a user's risk factor degrades from a certain amount then access for the user can be reduced and/or denied altogether.

Further, the solution provided herein utilizes MFA in a continuous manner while having the ability to use different parameters that identify both a user and the user's device, in a unique manner in order to facilitate dynamic access control. The trust score can be continuously generated or updated based on various parameters, such as device behavior, history of changes, and user authorization. Thus, the unique solution of this proposal provides for utilizing a combination of human, machine, and network-based continuous authorization in a novel manner in order to provide access to network devices without the need for usernames/passwords.

In summary, techniques herein provide a unique and novel solution that involves generating an enhanced trust score that allows CMFA for a specific user in context of the devices that the user is trying to access. This is a novel concept that differs from existing solutions involving basic MFA-based authorizations. However, such a solution could be integrated into MFA-based authorizations to support password-less intelligent device access. Thus, a unique solution is provided herein that facilitates access to specific controls within a device configuration and is tied to dynamic validation against an enhanced trust score. This provides real time control to what a user can do/configure when having access to a device. This a very different and novel concept as compared to Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+) offerings. Further, techniques herein allow continuous in-band validation and authorization of users for device access by using a screen generated QR code, while also using the continuous trust score from the mobile agent or allow continuous out-of-band validation and authorization using near field access technologies and hashing methods.

While the techniques presented herein are discussed with reference to remote IoT device access, it is to be understood that the same concepts as described herein can be used for any network device access that today relies on any MFA/RADIUS/TACACS+ authorization scheme. As the IoT industry is looking for password-less network access methods, this proposal fits well with a unique approach that uses a combination of human, network and device logs for providing access.