Application Authentication, Authorization, and Identification:

Why are they Different and Important

Introduction

Machine identification refers to the process of uniquely identifying a machine or device, typically within a network, system, or manufacturing setup. This process is crucial for monitoring, controlling, securing, and optimizing the operation of machines or devices. Below are common contexts in which machine identification is applied:

1. **Networked Devices**
   - **IP Address:** Unique identifiers assigned to devices on a network
   - **MAC Address**: Hardware address unique to a network interface card (NIC)
   - **Device Names**: User-assigned or system-generated names for devices, such as "DESKTOP-12345."
2. **Industrial Machines**
   - **Serial Numbers:** Unique numbers assigned by manufacturers to identify a specific unit.
   - **QR Codes/Barcodes:** Scannable codes linked to machine details in inventory systems.
   - **RFID Tags:** Radio-frequency tags for wireless identification in industrial automation.
3. **IoT Devices**
   - **Unique Device Identifier (UDID):** A unique identifier for smart devices.
   - **Digital Certificates:** Cryptographic means of uniquely identifying and securing IoT machines.
   - **Machine IDs in Cloud Systems:** Identifiers for virtual or physical devices managed in cloud platforms
4. **Machine Learning/AI**
   - **Hardware Identifiers:** Identifiers such as CPU, GPU IDs, or machine fingerprints, often used in distributed AI tasks.
   - **Telemetry IDs:** Used in logging and performance monitoring tools for identifying machines running AI models.
5. **Cryptographic and Security Systems**
   - **Secure Machine Fingerprinting:** Combines hardware and software attributes to create a unique machine identifier.
   - **Trusted Platform Module (TPM):** Hardware-based security for ensuring the integrity of a machine.

Would you like details on a specific type of machine identification?

Enterprise applications that are widely distributed must ensure that the connecting user is not only Authenticated, but also Authorized to use the application. However, the proper identification of the user is many times overlooked. This document outlines these important concepts and explains why they are equally important.

The Problem

Machine identification and spoofing problems often arise in scenarios where devices are authenticated or monitored based on their unique identifiers, like MAC addresses, IP addresses, or other hardware signatures.

Common Problems

a. Machine Spoofing

- **MAC Address Spoofing:** Attackers change the MAC address of their device to mimic another machine, bypassing filters or gaining unauthorized access.
- **IP Spoofing**: Fake IP addresses are used to disguise the origin of network traffic.
- **Device ID Spoofing**: Manipulation of unique identifiers used by applications, such as hardware serial numbers or UUIDs.

b. Identification Failures

- **Dynamic Identifiers:** IP addresses can change dynamically due to DHCP, making them unreliable for long-term identification.
- **Shared Devices**: In environments like NAT, multiple devices may appear as a single machine.
- **Compromised Devices**: Malware can alter device identifiers.

c. Identification Failures

- Inadequate encryption or hash verification may allow attackers to intercept and manipulate machine identification data.

Application Authentication, Authorization, and Identification:

Why are they Different and Important

Authentication

When a user begins to use an application, they must be authenticated. The process of authentication verifies the user's identity to ensure that their credentials are properly vetted to some internal process and that the user can participate in the application.

Authorization

Once a user has been authenticated to the application, that is they are allowed to use it, they then must ensure that they are qualified to perform specific actions within the application. For example, an administrator will have more rights and therefore have more capability than a user. A user may have more access than a public non-authenticated user. Authorization is tied to specific actions within an application and the privileges (roles) that the authenticated user has.

Identification

Identification is like Authentication, but for it to be absolutely secure, it must be separated from merely the credentials used to gain access to the application. This can be accomplished by the "something you know" / "something the system knows" paradigm, but it can also be accomplished though a unique property of the device that is used to contact the application (such as a device serial number or IMEI).

However, if the method by which the device is identified is static and / or tied to the physical device, it can be compromised which renders this method of identification insecure. Many applications now rely on 2FA (two factor authentication) to ensure that each session with an application has been vetted through a channel that is not part of the application or part of the physical device. This is quite robust, but it is still tied to the complete session from startup to shut down. It is also a bit cumbersome for the end user.

Another Solution

What if each individual interaction throughout the entire session was individually and uniquely identified? And, what if this process did not rely on any property of the physical device, nor require any interaction with the user?

Eclypses MTE-Relay offers such a solution. Once a session begins, a Quantum resistant handshake takes place between the originating endpoint and the consuming endpoint. This then is further augmented in that each exchange of data relies on a patented algorithm to ensure that the consuming application will only accept information from the paired originator. This is true whether it is an application running on a mobile device or web browser is communicating with the intended API, or an API communicating with another API. It is also applicable when a machine is sending important data to an analysis or processing application with no human intervention.

Conclusion

In today's environment, management of proper Authentication, Authorization, and Identification is a tedious task, so the advent of handing the work of consistent and secure identification off to an automated process along with the unique protection of each transmission of information is now something that is solvable and should be a part of every system where protection of the information is of significant importance to the enterprise.