End-to-end Security for the Internet of Things

The Internet of Things (IoT) is revolutionizing business. Connected devices can streamline processes and allow companies to create innovative and convenient services for their customers. But this innovation does not come without risk as much of the IoT is coming online without adequate security measures.

As systems begin to operate autonomously with more and more automated decisions, IoT devices must be trusted and their data secured. If an automated system is fed incorrect data, whether erroneously or maliciously, the whole integrity of the system is compromised. Incorrect smoke detector data can trigger building sprinklers, inaccurate temperature readings can cause control systems to make potentially harmful adjustments, and so on.

Trust begins with identity. In order to ensure the integrity of the entire system, it is crucial to securely establish and maintain the full lifecycle of IoT devices themselves, and the data they generate. These identities and their associated credentials must be trusted and useable across numerous connected ecosystems, between different devices, from devices to humans, and from devices to all varieties of cloud services. The data from these devices must be kept confidential and secure, and the system needs to be able to verify where it came from and control what systems can access it.

Existing solutions in the new “connected everything” world have tried to employ cryptographic security methods that were barely sufficient in the old, mostly disconnected and siloed landscape. They involve hard coded usernames and passwords that are an easy target for bad actors, or managing individual X.509 certificates on thousands of devices, which isn’t scalable and creates a huge management burden.

What’s needed instead is a system for establishing the trust and to manage the full lifecycle of IoT devices and their data. Enter ForgeRock, the leading platform provider of digital identity management solutions. By applying our vast knowledge of using digital identity to map the relationships between people, devices, and things to machine-to-machine (M2M) IoT environments, we are able to provide a security solution purpose-built for the internet of things.

ForgeRock® Edge Security offers complete end-to-end security for IoT deployments. It ensures the integrity of IoT devices and their communication using secure, standards-based tokens instead of insecure hard coded usernames and passwords, or managing thousands of individual PKI certificates. It adds a rock solid security layer to IoT hardware used at the edge, including leveraging highly secure on-chip Trusted Execution Environments (TEE) if available, and comprehensive, policy based controls for publishing and subscribing to data streams from edge devices, making it as easy to protect data coming from IoT devices as it is to protect a web page.

ForgeRock Edge Security is part of the ForgeRock Identity Platform, and is comprised of two products designed specifically for IoT:

ForgeRock Identity Edge Controller (IEC)

The ForgeRock Identity Edge Controller runs on smart edge devices and establishes a cryptographic Root of Trust that is used to create a trusted identity for each device. IEC ensures unauthorized traffic is intercepted before it enters your network. With a broad range of deployment options, even where network access is not always guaranteed, you can ensure trusted relationships between devices at all times. The ForgeRock Identity Edge Controller, part of the ForgeRock Identity Platform, enables you to harness further capabilities of the platform such as standards-based tokens, authentication, and authorization, and authorization to every user and every thing.

- Secure device attestation and on-boarding of trusted device identities
- Device authentication and authorization
- Proxied on-boarding of simple and constrained edge devices
- Secure configuration endpoints for connected devices and services
- Root of trust-based signing and encryption

Identity Message Broker

Organizations today need a way to secure and identity-enable industrial IoT data flows. Unfortunately, many IoT data flows lack identity integration needed for secure authentication and authorization, such as sending and receiving data through popular, yet not as secure protocols like MQTT (Message Queuing Telemetry Transport). Token-based validation of devices, for example, allow revocation and expiration of credentials, ensuring the trust of the device identity.

The ForgeRock Identity Message Broker, part of the ForgeRock Edge Security compliments the device security provided by the Identity Edge Controller by providing message-level security over native IoT protocols. The Identity Message Broker installs on-premises, in cloud, or on the edge, and can receive data streams from thousands of IoT devices. It authenticates the source and secures the data, and authorizes the data flow with the proven policy-based mechanism of ForgeRock Access Management. The Identity Message Broker can even be configured to install on the same hardware as the ForgeRock Identity Edge Controller, providing an all in one IoT edge security solution.

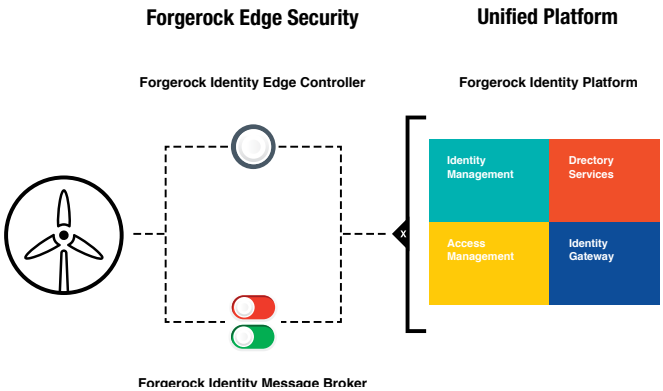
» Authentication and authorization enforcement for MQTT secures and hardens the sending and receiving of MQTT dataflows between an edge client and the cloud in Internet of Things (IoT) systems

» Evaluate access policies at the moment of action

» Token-based validation of devices enables revocation and expiration of credentials, ensuring device identity

The two products together form a strong and secure foundation to ensure the trust of the device identity, in combination with using the same device credential as the trusted source of data being authenticated and authorized for sending data to the cloud.

These components work together with the complete ForgeRock Identity Platform solution and provide a new level of security for IoT deployments. The ForgeRock Identity Platform brings carrier grade scalability, contextual security, and trusted relationships to IoT, supporting on-premises, dynamic cloud architectures, and hybrid cloud deployments.



Don't let security be a limiting factor in the design of your IoT hardware, software, and solutions. Close the IoT security gap with innovative security, proven open standards, high scale, and advanced management tools with ForgeRock Edge Security, part of the ForgeRock Identity Platform.

/ABOUT FORGEROCK

ForgeRock® is the Digital Identity Management company transforming the way organizations interact securely with customers, employees, devices, and things. Organizations adopt the ForgeRock Identity Platform™ as their digital identity system of record to monetize customer relationships, address stringent regulations for privacy and consent (GDPR, HIPAA, FCC privacy, etc.), and leverage the internet of things. ForgeRock serves hundreds of brands, including Morningstar, Vodafone, GEICO, Toyota, and Pearson, as well as governments like Norway, Canada, and Belgium, securing billions of identities worldwide. ForgeRock has offices across Europe, the USA, and Asia.

www.forgerock.com