An end-to-end approach to IoT security

The IoT ecosystem is composed of many standards, vendors using different hardware, software and third-party services and APIs. This huge fragmentation makes the ecosystem very vulnerable to all sorts of attacks, both at the Edge and in the Cloud. To achieve IoT security, we need to establish solid solutions for device discovery with secure identity, authentication and encrypted communications or the underline protocols are subject to abuse.

Eurotech

Eurotech is a multinational company that designs, develops and supplies Edge Computers and Internet of Things (IoT) solutions – complete with services, software and hardware – to system integrators and enterprises. By adopting Eurotech solutions, customers have access to IoT building blocks and software platforms, to Edge Gateway to enable asset monitoring and to High Performance Edge Computers (HPEC) conceived also for Artificial Intelligence (AI) applications. To offer increasingly complete solutions, Eurotech has activated partnerships with leading companies in their field of action, thus creating a global ecosystem that allows it to create “best in class” solutions for the Industrial Internet of Things. Learn more about Eurotech at www.eurotech.com.

Advanet

Advanet, a member of Eurotech Group, develops and manufactures a broad range of industrial equipment to support social infrastructure, such as medical devices,semiconductor manufacturing and transportation equipment, which are embedded as their core product. The reliability that is strongly required for such equipment can only be realized because of Advanet’s integrated system, from proposal through the development, production and the ongoing support capabilities. The advantage of Advanet is that it combines the philosophy of manufacturing, which has been forged in the Japanese market, and the global market competitiveness acquired as a member of the Eurotech Group, in a unique value proposition.

Common mistakes when planning an IoT project

The IoT ecosystem is composed of many standards, vendors using different hardware, software and third-party services and APIs. This huge fragmentation makes the ecosystem very vulnerable to all sorts of attacks, both at the Edge (Figure 1) and in the Cloud (Figure 2).

Often companies make important mistakes when planning IoT solutions, for example:

- Use of hardware and software without built-in security features to prevent root access
- Transmission of not encrypted data
- Lack of tools to perform devices updates (also from remote)
- Hard-coded credentials
- No integrity check of the software and OS installed on edge devices
- API tokens not encrypted
- Not proper authentication and authorization systems

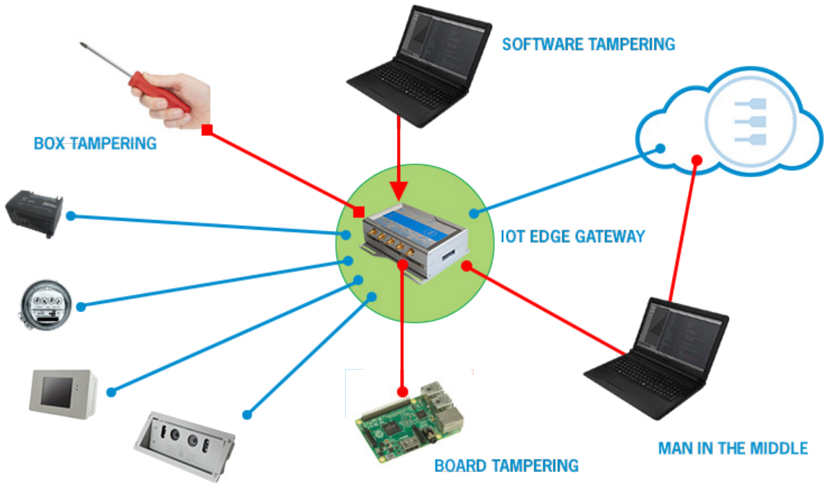


Figure 1. IoT security issues at the Edge

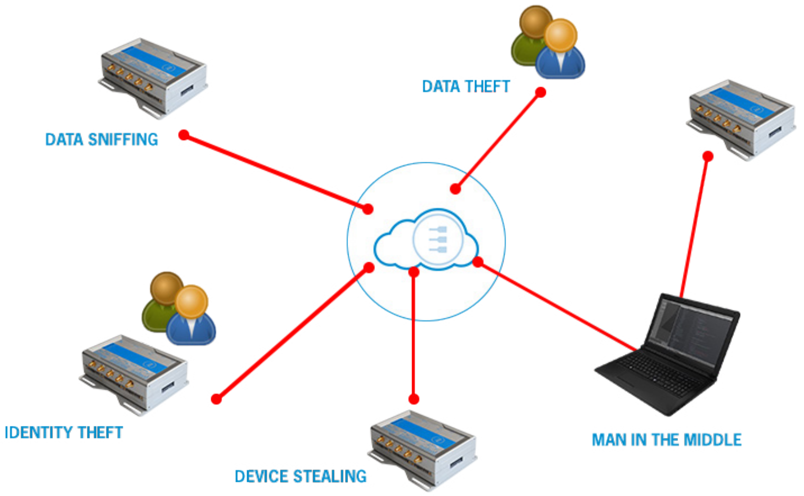


Figure 2. IoT security issues on the Cloud

To achieve IoT security, we need to establish solid solutions for device discovery with secure identity, authentication and encrypted communications or the underline protocols are subject to abuse.

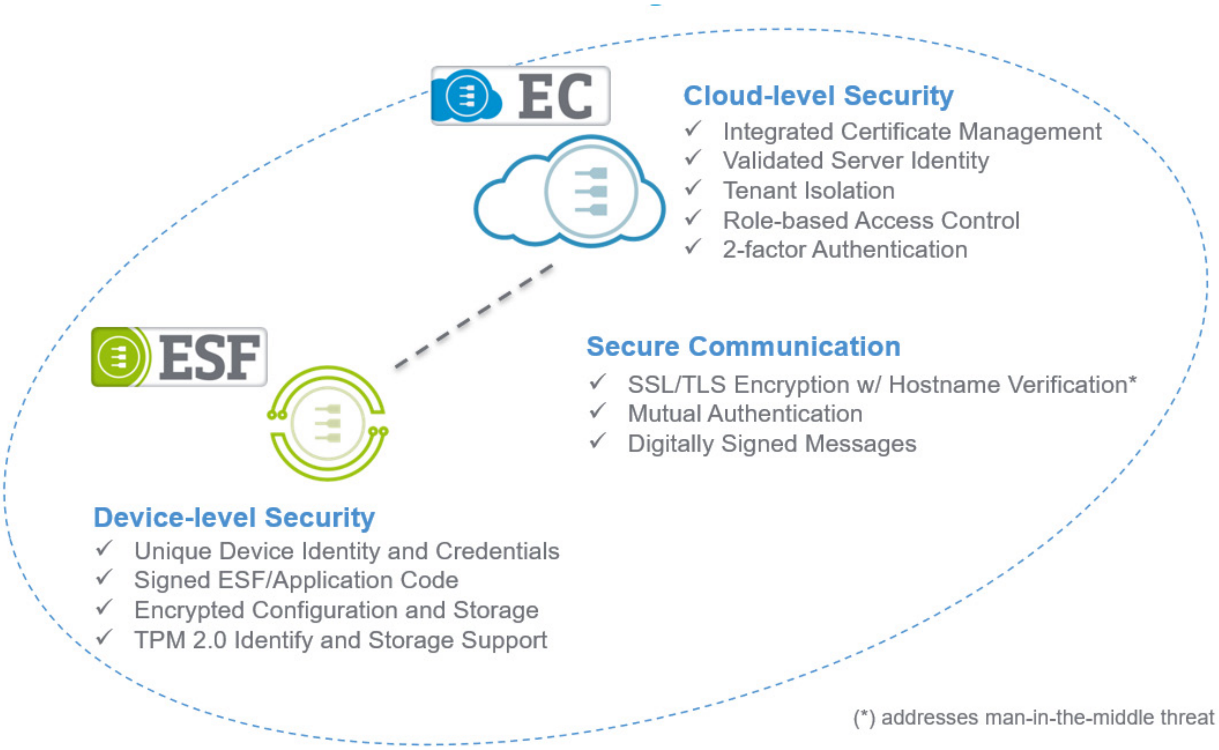
IoT Security best practices

Best practices need to consider the specific aspects of distributed mobile systems and devices. We need a secure execution environment for all devices and the IoT integration platform, as well as secure software management distribution. Above all, connected devices and the IoT platform must have a validated identity. To achieve this, we must:

- Build solution based on open and industry standard
- Leverage proven security technology and partnership
- Include security, scalability and resilience in the design from day one
- Identify each connected node and unique ID and credentials
- Mutually authenticate nodes in the IoT infrastructure
- Encrypt all communication to protect data
- Implement controls for automatic revocation of certificates
- Digitally sign all communications over an encrypted channel
- Digitally sign software and configuration to ensure integrity and authenticity of the systems
- Role-Based Access Control (RBAC)

Eurotech: Security by Design

As described before, IoT security must be designed from day one. The illustration below shows how the architecture of an IoT Solution can be divided into three layers:



Cloud-level Security
✓ Integrated Certificate Management
✓ Validated Server Identity
✓ Tenant Isolation
✓ Role-based Access Control
✓ 2-factor Authentication

Secure Communication
✓ SSL/TLS Encryption w/ Hostname Verification*
✓ Mutual Authentication
✓ Digitally Signed Messages

Device-level Security
✓ Unique Device Identity and Credentials
✓ Signed ESF/Application Code
✓ Encrypted Configuration and Storage
✓ TPM 2.0 Identify and Storage Support

(*) addresses man-in-the-middle threat

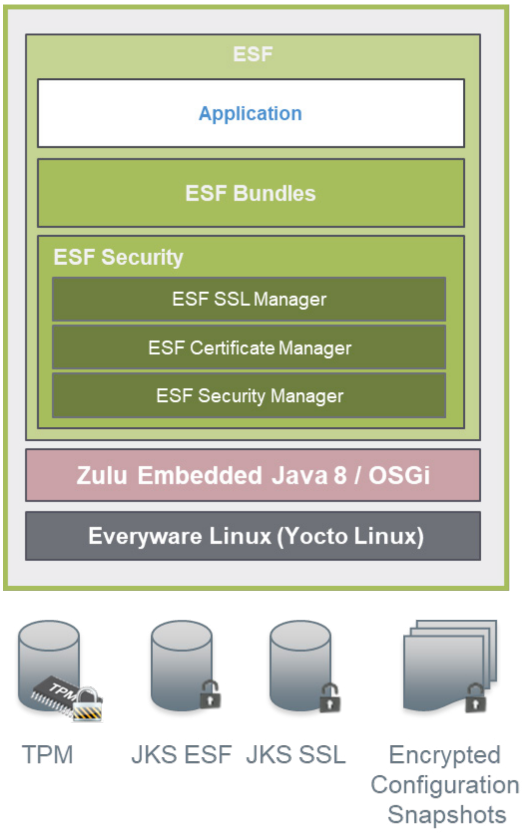
Device level security

Security mechanisms are an integral component of the Everyware Software Framework (ESF), which in turn is embedded in the IoT Gateway.

The ESF architecture is based on different software layers. The OSGi (Open Services Gateway Initiative) layer provides a good foundation for securely managing software components (signed bundles). ESF ensures that strict Java and OSGi security policies are enforced at runtime and verifies that only software signed by the approved authorities is installed and enabled.

The ESF Security layer encapsulates all the security features and it is supplemented by other measures like secure boot, appropriate hardware design and other measures, thereby ensuring proper protection of the solution on the Edge.

An operation overview of the ESF security can be found here.

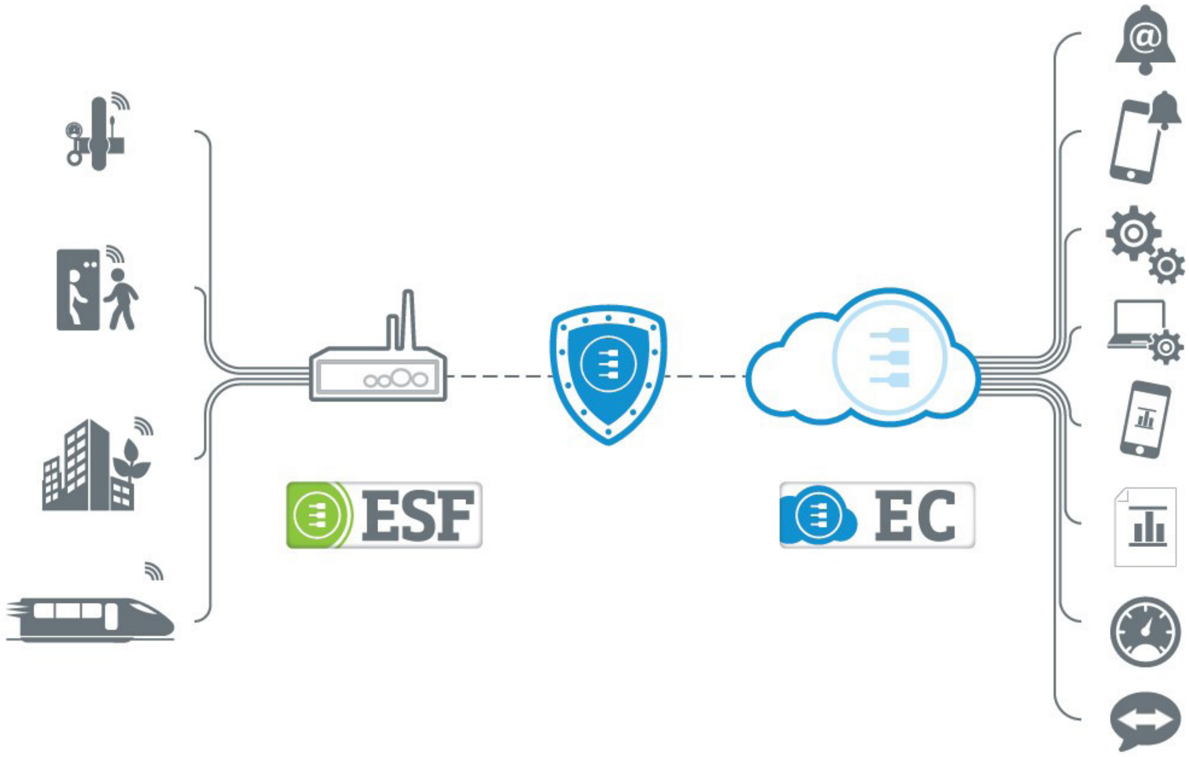


Moreover, maintains a list of security guidelines to be followed when hardening an IoT device for a production deployment. The guidelines are compiled following the recommendation of Industry Standards such the Center of Internet Security (CIS) and the IEC 62443. The Eurotech hardening guidelines are available here.

Secure communication

Eurotech supports different protocols, but we advocate the use of MQTT (Message Queue Telemetry Transport), which is a lightweight protocol optimized for IoT device communications:

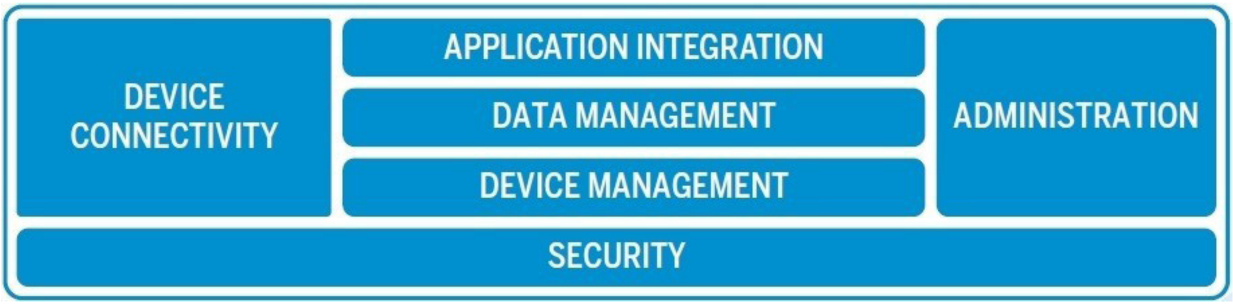
- All MQTT traffic is originated from the gateway and encrypted over an SSL connection.
- All console accesses are exclusively available over an encrypted HTTPS connection.
- All REST API accesses are exclusively available over an encrypted HTTPS connection.
- Robust authentication is enabled by strong, well-understood technologies like X.509 Certificates and encrypted credentials.
- Device management messages published by the IoT Platform are signed to guarantee authenticity and message integrity.



IoT cloud security

Everyware Cloud unites the operational technology (OT) domain and the information technology (IT) domain, which means that it is the single, most important interface. A success attack would enable access to the enterprise environment. Everyware Cloud also functions as an M2M / IoT integration platform that acts like an operating system for the infrastructure.

On the operational technology side it provides all the data, device and embedded application management required to deploy and maintain distributed intelligent systems in the field. This schematic indicates how security is embedded in Everyware Cloud.



Everyware Cloud, Eurotech's IoT Integration Platform, incorporates X.509 Certificate based authentication plus Integrated PKI Certificate management

- Security mechanisms in the cloud ensure that authorized traffic is secure and authenticated
- It employs firewalls, so all in-bound ports other than broker ports are closed and secure (encrypted and authenticated)

- Device authentication uses strong username/password credentials or a per device certificate
- Security mechanisms in the cloud ensure that authorized traffic is secure and authenticated
- It employs firewalls, so all in-bound ports other than broker ports are closed and secure (encrypted and authenticated)
- Device authentication uses strong username/password credentials or a per-device certificate
- Each device can be automatically provisioned during first activation with a secure, randomized, device-specific password. In addition, the device credentials can be strongly tied to a specific device so the IoT Integration Platform will refuse authentication requests with the same credentials from a different device.
- The device authorization policy can further restrict the device data communication limiting the MQTT topics that the device can publish to and blocking device to device communication.
- Access control is centralized and authenticated via HTTPS / SSL
- Role-based access control is employed as well as user management and roles and permissions. A strict segregation of tenants down to a data level is another important element ensuring that other parties cannot access data and infrastructure.
- Logins to Everyware Console can be further protected using a Two Factor Authentication (2FA)