ZDMP Blog

Secure communication channels in Industry 4.0

By David Todoli, ITI Technology Center

Some questions for you

- Do you have or plan to have devices sharing sensitive process data with any external system?
- Do you consider updating the encryption/key exchange mechanisms that provide security to your communications?
- Do you consider the risks to your business from data leaks or compromised IT systems?

The impact of security in Industrial Internet of Things

The Internet of Things (IoT) is a key enabler of digital transformation. From smartphones and tablets to vehicles and even industrial devices such as Programmable Logic Controllers (PLCs), these smart systems and devices can be found worldwide. This has brought benefits to society and industry, which is increasingly requiring increased connectivity.

These technologies are rapidly gaining acceptance due to their lower installation time and cost, and their ability to bring Operational Technologies (OT) and Information Technologies (IT) worlds together in industrial settings. However, this popularity has raised significant concerns about security and privacy when using this type of technology and devices. Especially when talking about critical applications in industry and transport, where security requirements are stricter, often with mandatory regulations.

IIoT faces many threats that are often ignored but is a problem that can be addressed by following specific policies.

Security mechanisms to address the most common threats vary depending on the technology selected, but also depending on the environment and application requirements. In short, there is no "one size fits all" solution, so the first step for any IoT deployment should be to go through a security risk assessment that examines vulnerabilities in devices, network systems and user and customer backend systems.

Securing devices and their communication

Encryption and secrecy are absolute requirements of IoT deployments. This is why the most important security requirements include authentication and tracking, data and information integrity, mutual trust, privacy, and digital forgetting. These concepts are used for securing communication, shielding firmware and software, and protecting the users.

The main mechanisms to take into account during the implementation of these IIoT technologies focus on the following aspects / levels:

- Medium access layer (MAC): Where the information is transmitted over the air, which requires the implementation of encryption and authentication mechanisms for packets, such as AES-CCM

- Network layer: For example, with IPsec, VPN, and firewalls
- Transport and application layer: Use of TLS and SSL through certificates at both ends (client and server), user authentication / authorization
- Protecting physical access: Includes to equipment, through on-site mechanisms for authorization of device commissioning (NFC tags, biometric access, etc.), and with hardware with crypto chips that encrypt the content of the device's memory to avoid reverse engineering

As can be seen, some of these options are out of scope for many devices and equipment, whilst others rely directly on the know-how of the IT & networking departments of each company.

Limitations inherited

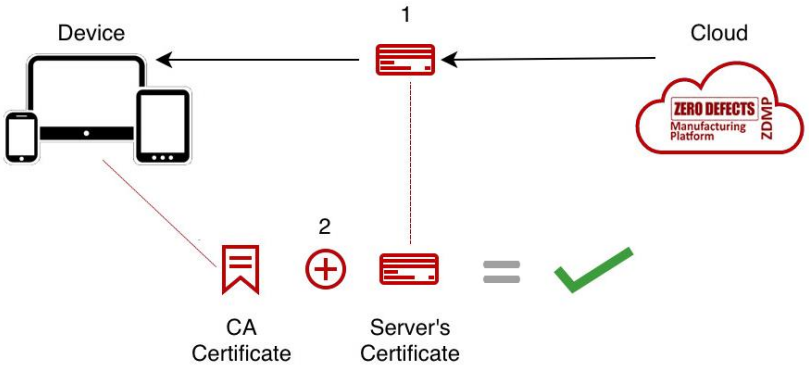
IoT devices are generally inexpensive and have limitations in terms of computing power, available storage, and power consumption. But these problems are often also present when integrating devices inherited from previous installations in the manufacturing line, because replacing every controller and machine with updated models is too expensive.

In addition, devices establish infrastructure-less communications based on short-term connections between peers that may never have communicated before.

All these factors are limiting during the selection of cryptographic algorithms and security protocols, and are very influential in defining the security architecture, since the establishment and maintenance of communications between devices must be conducted with care.

What will ZDMP achieve?

The Secure Communication component of ZDMP integrates a fully featured PKI and services that allows users and administrators to address the Transport & Application layer security, by enabling a simplified management of certificates and therefore solve the security aspects that require encryption, data integrity, privacy and mutual trust.



By using this PKI, users can receive client and server certificates, signed by the Authorities of choice, in order to encrypt, has , and authenticate communication channels and all the data transmitted through them. Digital certificates use an asymmetric, encryption based, authentication system designed to authenticate a transaction and encrypt the channel between peers even before the authentication takes place. They can also enable cryptographic identification difficult to achieve with common id & password.

ZDMP Links

Architecture Component(s)@	Secure Communications
Work Package@	WP5: Core Services and Middleware
Tasks@	T5.2 – Robust Industrial Network Support

References

None