MOCANA

Protecting Unpatchable Legacy Industrial Control System (ICS) Devices

Unpatchable Workstations and Devices

The vast majority of vulnerable industrial control system (ICS) devices are legacy devices that have been in the field operating for years or decades. These devices, such as programmable logic controllers (PLCs), sensors, drives, intelligent edge devices (IEDs), gateways, or even workstations are so out-of-date that they are no longer patchable. These devices cannot be upgraded, oftentimes, because the software or operating system is not upgradable.

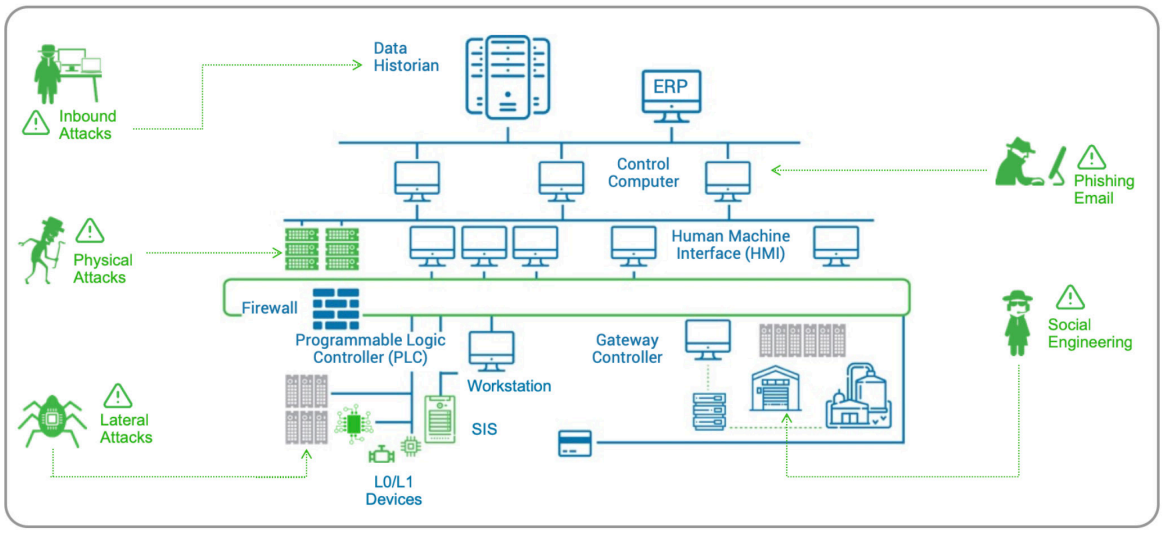

Figure 1. Vulnerable ICS Distributed Control System (DCS)

End of Support for Windows OS

Workstations and devices using unsupported versions of the Windows operating system are especially vulnerable because they are no longer patchable. Mainstream support has ended for Microsoft Windows XP, Vista, 7 and 8. Furthermore, Windows XP, Vista and 7 have reached the end of their Extended Support period, which means that Microsoft no longer provides bug fixes and security patches.

Unupgradable Applications

As operating systems reach their end of life, application developers begin reducing the support of their applications running on these older operating systems. It is not uncommon for applications running on ICS devices and workstations to reach their end of life before the lifespan of the device. These applications become unupgradable and unpatchable. Complicating matters, the lifespan of a device often exceeds the timeframe for the applications support.

Average lifespan of a device:

- Distribution transformer – 25 years
- Substation switchgear – 9 to 36 years
- Wind turbine – 20 to 25 years
- Manufacturing device – 10 to 20 years.

Insecure Industrial Protocols

Legacy devices may be using insecure industrial protocols. Protocols such as Modbus, CANBUS, BacNet and DNP3 have very little inherent security for authentication or encryption. Industrial device data may be transported in the clear, unencrypted, with very weak authentication. Communicating securely with these devices is challenging and remotely managing keys or digital certificates can be difficult.

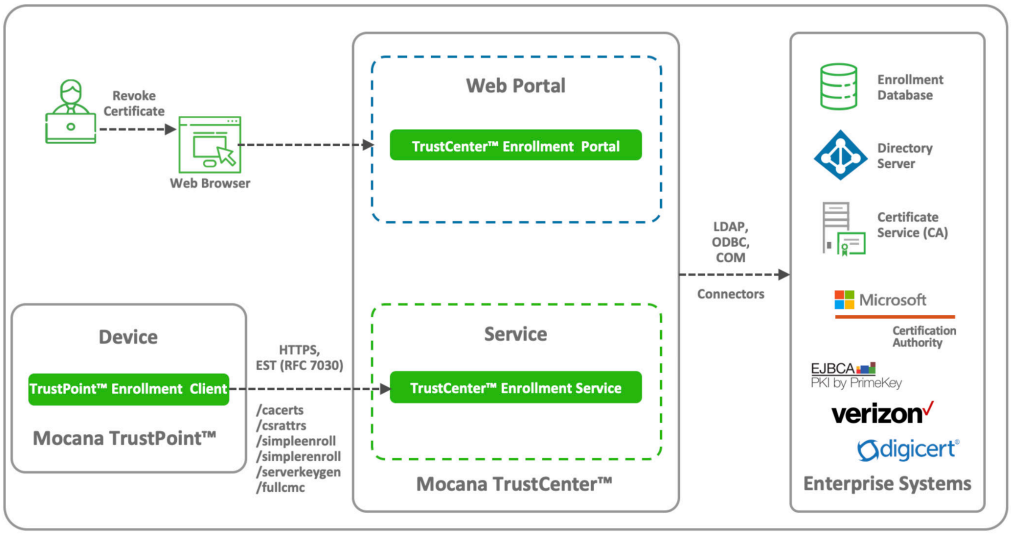

Fig 2. Mocana TrustCenter™ Automated Lifecycle Management

Mocana TrustCenter™ - Automated Device Security Lifecycle Management

Mocana TrustCenter™ is a services platform that provides a system of cybersecurity to automates device security lifecycle management. The Mocana TrustCenter™ Enrollment Service (TCES) runs on private or public cloud servers. TCES automates key and certificate provisioning and management.

The TrustCenter Enrollment Portal (TCEP) provides a unified and elastic approach for authentication, authorization, issuance, renewal and revocation of device and application certificates. TPEC includes a command line utility (sdec) for certificate enrollment, renewal, rekey operations that enables secure device onboarding, trusted updates, secure transport and data protection required by IoT applications.

Mocana TrustPoint™ Enrollment Client (TPEC)

The Mocana TPEC is a binary client that runs on Linux, Windows or a real-time operating system. The TPEC can be installed as a binary to the target operating environment without impacting the application. The TPEC includes secure session management, certification chain verification, support for containers and virtual machines, and a comprehensive set of Enrollment over Secure Transport (EST) commands. TPEC leverages the TCES as a protocol translation layer between the EST protocol (RFC 7030) and a plurality of COM/REST API connectors to Enterprise and commercial certificate authorities (CA) for certificate lifespan management.

The TPEC has a minimum code footprint of 1.2MB and peak SRAM usage of 100KB.

Simple, Scalable Key and Certificate

Operators and asset owners can use Mocana TrustCenter™ to securely and remotely provision and manage keys, digital X.509 certificates or other device credentials. Using TrustCenter™ simplifies the management of the device security lifecycle. This dramatically simplifies key and certificate management and eliminates and lowers the cost of operational device security management.

Mocana Corporation
111 W Evelyn Ave, Ste 210
Sunnyvale, CA 94086
tel (415) 617-0055 toll free (866) 213-1273
iotsales@mocana.com