Protecting your critical infrastructure from modern threats in the world of IoT

Attacks against critical infrastructure, such as the Triton infiltration of the control and safety systems of an oil and gas plant, have become more frequent globally. While the financial toll of cyber-attacks has become an unfortunate norm, attacks to connected systems that put human lives and property at risk are emerging with new regularity. Connected systems are growing in complexity and components. For secure operation of critical infrastructure, end-to-end solutions inherently rely on trust between components including cloud services, edge devices and endpoints. A breach in one component can compromise entire systems as these recent attacks show.

Microsoft, along with industry partners, is looking to help mitigate these attacks with a new project, codenamed Trusted Cyber Physical Systems (TCPS).

Microsoft's Trusted Cyber Physical Systems (TCPS) efforts address the unique challenges to secure critical infrastructure, creating security assets to protect critical functions throughout distributed systems with:

Separation of critical execution

Help protect critical infrastructure from malware threats by separating non-critical from critical operations and concentrate on using hardware isolation to protect control of physical systems.

Inspectability of execution process

Ensure that any code that handles critical operations must be auditable by operators through source code review.

Attestability of processing environment

During operation, each component must be able to verify that data is received and sent only from trustworthy sources. A component also needs to attest its trustworthiness to other components.

Minimizing number of entities that need to be trusted

Reducing the number of trusted entities significantly reduces the attack surface for critical infrastructure. In the ideal TCPS solution, the operator will maintain the only root of trust for critical code execution.

The key security principle is: the infrastructure owner/ operator must not lose control over their critical systems.

Microsoft is working with industry partners on solutions that provide infrastructure operators with hardware, software, and trust mechanisms that put the operator in complete control of their critical systems.

Key Takeaways

- Critical infrastructure needs strict prevention measures, versus just relying on detection and remediation.
- There are only two entities an owner/operator should need to trust: their own administrators, and their chosen TEE chip manufacturer.
- Today's low-cost devices with Trusted Execution Environments (TEE) can be deployed without requiring changes to existing investments and equipment.
- Open source code and industry standard protocols provide transparency and ability to vet software controlling critical operations.

Why work with Microsoft on securing your critical infrastructure?

- We take a holistic approach based on years of security, cloud, and embedded experience
- Code inspection by customers and 3rd-parties on Microsoft-provided trusted applications and services
- Azure confidential computing brings trusted execution to the cloud
- The Windows IoT Device Update Center can be used to deliver patches via the Windows Update global CDN
- Windows 10 IoT Core support for NXP i.MX 6 and i.MX 7 enables TCPS to the wire
- Leaders in cross-platform industry standards efforts (ex: OPC, IIC, TCG, IETF)

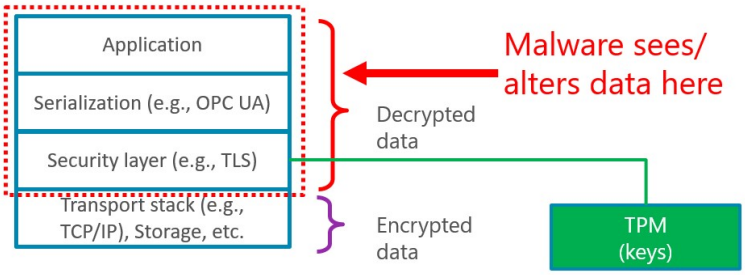
Learn more about securing critical infrastructure at aka.ms/TCPS_HMI2018

Microsoft and our partners are seeking to unlock trusted execution in the cloud, on devices controlling infrastructure and on edge devices. The power of TCPS brings trusted execution to the wires and pins that control critical infrastructure, enabling end-to-end critical infrastructure solutions.

Our TCPS properties are realized through the use of Trusted Execution Environments (TEE), and tying those to physical environments and a trusted cloud.

Trusted execution

One common misconception is that it is sufficient to protect data in flight and data at rest. This leaves a vulnerability in data in execution.



Data in execution can be protected by Trusted Execution Environments (TEEs) such as Intel SGX, ARM TrustZone, and SecureElements. TEE hardware enforces three guarantees:

1. The device has a unique security identity
2. Any code inside the TEE is operator-authorized code
3. Any data inside the TEE cannot be read by code outside the TEE

End-to-end scenarios often involve many components, including human interaction devices, public or private cloud services, and edge compute devices. All devices that could potentially control critical systems must be protected with trusted execution. In practice, there are only two entities an owner/operator should need to trust: their own administrators, and the manufacturer of the security chip in their hardware.

Trusted cloud computing

It is important to protect any public or private cloud services that could directly or indirectly control critical operations. Examples include: provisioning, key management, certificate authority, patch management, and logging. These must not only use secure protocols, and protect keys and data at rest, they must also perform all critical operations in a TEE that is protected from public cloud hosters and OS vendors. Azure confidential computing enables cloud hosting of these services.

Trusted physical control

Physical security is needed to prevent tampering with connections to actuator/sensor functionality that is electrically controlled. If malware can access such connections, for example via a kernel compromise, then vulnerabilities exist. To defend against them, it is necessary to treat such connections as trusted peripherals that can only be accessed from within a TEE; TrustZone, for example, on an iMX.6 can do this today.

Since it is impractical to require replacing expensive equipment to put in hardware security chips, a "brownfield" deployment is possible by putting a TEE gateway in front of such equipment. The connections between the security gateway and the existing equipment are protected the same way as the connections to the actuators: physical security. The key requirement for such a gateway is that communication to the existing equipment must only be possible from within the TEE, isolated even from OS code.

Trusted human interface

A brownfield gateway can defend against attacks on the equipment behind it, but not against a compromised user device or SCADA system that can send commands that appear legitimate. For example, a compromised device could trick an operator into performing the wrong action, or simply initiate an action without informing the operator.

A "Secure Confirmation Terminal" that requires confirmation can help defend against such attacks. Without having to change existing software, it can be placed inside or next to a human interface system, similar to a chip-reading payment terminal in retail systems being used separate from a cash register.

Any unusual operation that policy deems as requiring confirmation results in a message on a secure display. An operator can confirm the intended operation, where the display and input device are only accessible from a TEE, out of reach of any malware. Once confirmed, the TEE signs operations for use by the rest of the system.

Contact tcps@microsoft.com for more information on partnering with us on:

Deploying into a variety of environments | Enabling an ecosystem of compatible devices | Expanding protocol support and industry standards engagements