accenture

Strategy | Consulting | Digital | Technology | Operations

Accenture Labs

Security for the Industrial Internet of Things

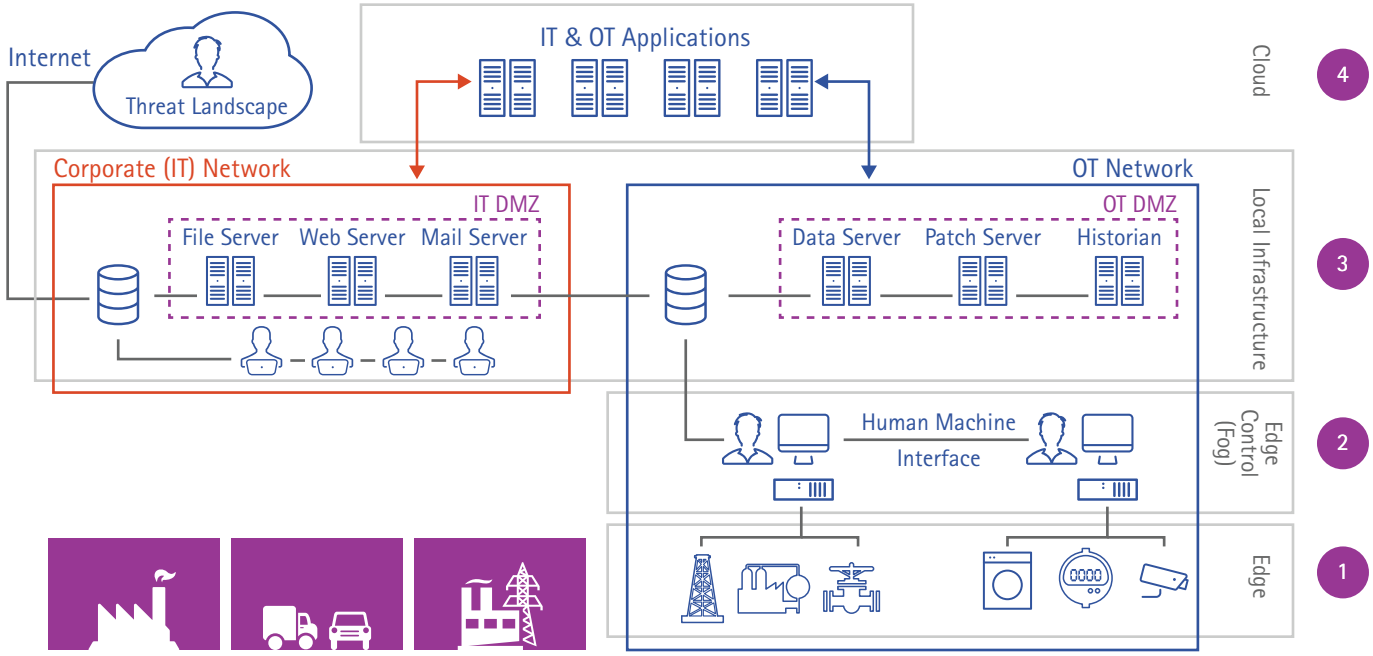
Security framework for IT and OT optimizes security architecture and capabilities

The Industrial Internet of Things (IIoT) introduces various operational technology (OT) architectures–including healthcare, manufacturing, transportation, and energy production and distribution—with inherently different threat vectors to the enterprise's traditional information technology (IT). For instance, field equipment that controls configuration and operation of a distribution system, and manufacturing equipment tightly controlled within a manufacturing infrastructure, result in different attack surfaces than the usual IT footprint. However, regardless of the IIoT enterprise architecture, today's IT-centric cyber security frameworks are not adequate to address the unique security and resilience needs of the industrial domains' operational technology.

In order to fill this gap, **Accenture Labs developed a holistic, scalable and strategic framework for IIoT security that can be used to assess, prioritize, implement and optimize both security architecture and security capabilities within IIoT environments.** In developing this framework, we considered trustworthiness and resilience requirements, as well as implications across IT and OT architectures, including data integrity and privacy considerations. The security framework can be used to identify security requirements for an IIoT architecture, or to determine security capability and mission assurance gaps in an IIoT network. The following presents our security framework and IIoT security solutions along the different levels of the IIoT architecture.

Consider a representation that shows various tiers of the IIoT reference architecture with IT and OT components (see Figure 1). This reference model is a conceptual framework for grouping IIoT components with similar business mission, operational scope and computational resources. The components in each layer have, therefore, similar functional requirements and are exposed to similar cyber risks. These shared requirements and concerns call for a set of unique and complementary security solutions at each architectural layer.

Figure 1: Security framework for IT and OT optimizes security architecture and capabilities.



Edge tier is self-organizing and self-reliant

The edge tier is where the cyber-physical devices or the smart "things" reside. The "things" at this tier can sense the surrounding physical environment and may interact with it. Examples of these devices include video cameras, temperature sensors or furnaces. Some may be able to execute control logic or actuation to trigger desired physical outcomes.

Devices at the edge of the network include resource-constrained legacy and remote computing devices. Edge devices need lightweight security functionality to achieve a real-time, vendor-agnostic, protective mechanism that efficiently reduces the communication and computation overhead imposed on upper-level security agents.

Existing IIoT edge security solutions offer mainly unauthorized device detection, device key management and physical security capabilities such as USB port lock services. There are missing pieces in the edge security puzzle, including gaps caused by failing to properly deal with resource constraints, data provenance and trust, and more importantly vendor diversity (i.e., the wide variety of hardware and software systems).

Ideally, a rigorous edge security solution must carry a complete set of security controls and capabilities to provide asset protection, device and data security assurance, and resilience in the presence of cyber attacks. These capabilities must be applicable to various IIoT environments.

Examples of protective and detective mechanisms suitable for IIoT edge devices include:

1. a mechanism to detect and prevent any physical or remote tampering with an edge device based on a generic hardware add-on that can be attached to the device;
2. a distributed intrusion detection mechanism that optimally assigns different security functions to resource-constrained edge devices in order to provide maximum threat detection coverage at the edge;
3. a distributed incident response tool running on a device management platform and providing federated access to all security-related data on the edge devices.

The latter monitors all devices as they join and leave the network, as well as the data that they carry. This tool provides security analysts with a current picture of the security posture of their organization's network and the ability to run security analytics at the edge of the network with minimal communication overhead. The tool also leverages semantic technologies to assist security analysts with threat detection through automated reasoning capabilities, making IT system information readily usable for attack forensics, tactical cyber defense and shortening the incident response lifecycle.

Fog tier augments brownfield devices

The fog tier is formed by near-user devices such as gateways that consolidate a number of lower-powered and lower-capability edge devices in order to carry out a notable amount of computing, communication and storage capabilities on their behalf. This consolidation may be achieved by configuration or dynamically.

Control systems in this architectural level supervise, monitor and control physical processes during their runtime. Gateways, IP networking protocols, real-time controls, human machine interfaces (HMIs) and alerting systems, as well as supervisory control and data acquisition (SCADA) systems are various examples of systems that provide computational, communication and storage capabilities.

Fog-tier functionality allows security administrators to integrate the primary security functions—such as intrusion detection and prevention, user and device authentication, and secure communication—into process control functions. The implementation of IT-centric security controls at the fog level is challenging, however, due to the inherently different characteristics of the OT environment. For instance, a firewall may attempt to block a command that is critical to the operational cycle.

A majority of the security solutions and products offered for the IIoT domain reside on this architectural level. Network segmentation and zoning solutions, traffic encryption and tunneling tools, network-based intrusion detection systems, firewalls, and asset discovery and management tools are the most common security products that get deployed within the fog tier.

Expanding the security functions of these solutions can be a daunting task, without a complete re-design of their architectures due to the limited scope of their initial designs. More precisely, the solution space at the fog level lacks a scalable and modular security platform that can perform multiple IIoT security controls, while being adaptable to changes introduced through new protocols, standards and technology requirements for better protection.

Accenture Labs' fog security solutions are devised to meet these criteria. They comprise a security agent platform residing on IoT gateways. The platform adds IT-based security functions to the legacy devices that lack them. Another component ingests industrial telemetry data that is currently used only for safety and reliability checks. We model telemetry data and leverage domain-specific knowledge to distinguish between cyber security attacks and process faults. Distinguishing between malicious activity or equipment failure helps the organization to identify the right course of action in order to ensure the integrity and reliability of its operations.

Local infrastructure tier customizes for domain-specific deployments

Business and operation management of enterprise (IT) and manufacturing (OT) zones are provided in the local infrastructure layer of each zone. IIoT's unique characteristics make enterprise IT cyber security frameworks unsuitable to OT networks. Furthermore, geographically dispersed IIoT deployments have numerous edge devices that require frequent and dynamic configuration based on security policy implementation.

These issues make it challenging to identify the most effective security capabilities for each infrastructure (IT and OT) and how to apply them efficiently to different IIoT architectural levels. Our research addresses this empirically by developing an IIoT domain-specific cyber security framework and measuring the effectiveness of various security controls.

Some solutions propose a security tool suite that provides few security capabilities (such as vulnerability scanning, traffic monitoring and/or security configuration management) in multiple architectural levels in IIoT environments. One issue in dealing with a variety of security vendors, devices and platforms is that it can be almost impossible for any multi-level solution to effectively interact with proprietary systems. Thus, a solution proposed for one critical sector or organization—that is designed based on their own technology providers—hardly ever applies to other sectors or organizations.

To address this limitation, consider applying software-defined security (SDSec) principles to OT environments. SDSec has recently emerged as a security model for enterprise networks. The model separates security management tasks from security control actions, thus making security management vendor agnostic, while abstracting it from the underlying networking, storage and compute infrastructure. Greenfield devices, which have embedded control and external connectivity capabilities, enable SDSec to provide a global awareness and local action framework.

In such a framework for the IIoT environment, security policies are defined, controlled and managed in a centralized fashion, while security actions are taken locally on the edge devices. For example, SDSec can dynamically apply a new access control policy to multiple remote edge devices in order to mitigate IIoT threats such as Night Dragon[1] or Stuxnet.[2] It can quarantine compromised devices or assets having a lower trust level and isolate them from uncompromised ones, thus achieving autonomous attack containment and freeing security administrators from manually changing security configurations.

[1] http://www.pcworld.com/article/219251/article.html

[2] https://en.wikipedia.org/wiki/Stuxnet

Cloud tier provides cross IT-OT situational awareness

This layer focuses on the aggregation of data and compute for IIoT within the wide-area network. Securing critical infrastructures requires improved situational awareness, and the ability to detect anomalous activities across converged IT and OT infrastructures. Existing cyber security approaches and solutions available on the market--such as intrusion detection systems or security information and event management (SIEM) tools—typically operate in a single domain.

So while they are capable of correlating security events/alerts and detecting compromises, they are not able to provide cyber defenders with a full picture of what is going on their network. At best, the full extent of the detected compromises may not be known since any potentially related threat activity from other domains is not considered. At worst, the correlation of activities within a single domain fails to yield any threat insights, thus leaving the defenders unaware of the malicious activity occurring on their network.

Detecting complex threat vectors within connected and heterogeneous industrial infrastructure necessitates a multi-domain event correlation engine. Such an engine will be able to detect malicious activity that traverses from the IT domain (enterprise network) to the OT domain (control zones) and vice versa.

Data correlation across IT and OT domains based on events informed by a combination of security components not only offers the advantages of traditional event correlation found in SIEMs, but also serves in detecting complex attacks (including the temporally distributed, multi-step and multi-session attacks) and in providing a single vantage point to security administrators. The use of semantically enriched, graph-based models for identifying the complex attack patterns significantly improves situational awareness throughout the entire IIoT environment.

Accenture Labs is currently developing such a system. The system could exchange STIX[3] -format data about IIoT security incidents with intelligent-driven threat mitigation systems that provide publicly available threat intelligence feeds to further improve its intrusion detection capability.

[3] https://stixproject.github.io/

IIoT security through a tiered approach

Taking into consideration all of the above mechanisms, a comprehensive approach to securing any critical infrastructure must begin with analyzing the topological model of the IIoT network. Next, it is essential to identify the risks corresponding to each architectural level. Equipped with this information, organizations can prioritize and implement security solutions within each tier and provide effective cross-tier governance in order to protect their businesses.

In summary, traditional perimeter solutions are inadequate. IIoT security is complex and requires a multi-layered solution that works as a comprehensive unit. Accenture Labs' framework provides the mechanism to put together and assess such a comprehensive and modular solution, which is composed of point solutions that work together within and across tiers.

Contact us

Teresa Tung, Ph.D.
Technology Labs Fellow – Systems & Platforms
teresa.tung@accenture.com

Malek Ben Salem, Ph.D.
R&D Principal – Security
malek.ben.salem@accenture.com

Amin Hassanzadeh, Ph.D.
R&D Associate Principal – Security
amin.hassanzadeh@accenture.com

About Accenture Labs

Accenture Labs invents the future for Accenture, our clients and the market. Focused on solving critical business problems with advanced technology, Accenture Labs brings fresh insights and innovations to our clients, helping them capitalize on dramatic changes in technology, business and society. Our dedicated team of technologists and researchers work with leaders across the company to invest in, incubate and deliver breakthrough ideas and solutions that help our clients create new sources of business advantage. Accenture Labs is located in seven key research hubs around the world: Silicon Valley, CA; Sophia Antipolis, France; Arlington, Virginia; Beijing, China; Bangalore, India; Herzilya, Israel and Dublin, Ireland. The Labs collaborates extensively with Accenture's network of nearly 400 innovation centers, studios and centers of excellence located in 92 cities and 35 countries globally to deliver cutting-edge research, insights and solutions to clients where they operate and live

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business andtechnology to help clients improve their performance and create sustainable value for their stakeholders. With more than375,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

16-2526U/23-7128