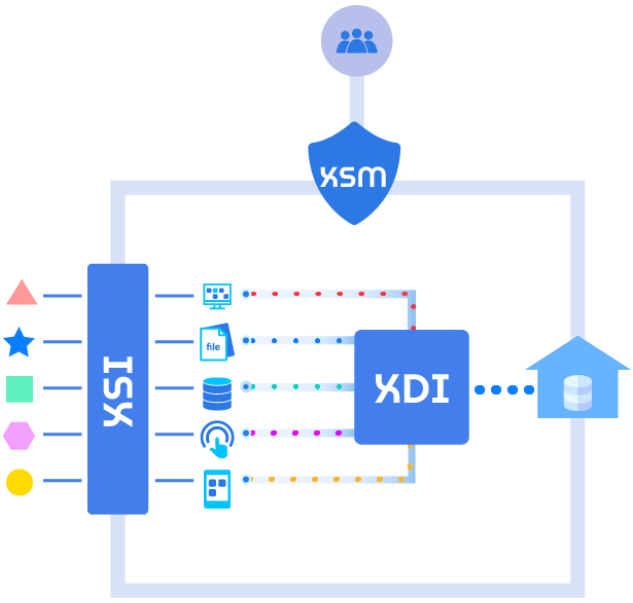
The Role of the Cross Integration Suite in the Security of Utility Systems, IT and OT environment

By - Matt Lampe, 3Insys CSO

3Insys' Cross Integration Suite is a trio of products to bridge the increasingly complex interactions between the world of Information Technology (IT) and Operational Technology (OT). This world consists of various applications, infrastructures, and protocols. In the Electric Utility world, this complex landscape includes such applications as outage management, SCADA, distribution management, demand management, voltage support, metering and asset management, and devices as diverse as meters, inverters, wind turbines, generators, transformers, circuits, capacitor banks, relays, switches, and a wide variety of sensors. These devices may communicate on an IP network, on direct circuits, via wireless networks, or SCADA-focused protocols like DNP3 or 68070. Data flows among these systems are increasingly complex as software becomes more critical to effective management of the grid. Moreover, while these more complex data flows and the need for data sharing are growing, there is a necessary increase in the attention to cyber security.

The Cross Integration Suite has three key components that provide the middleware layer to simplify the integration of these applications and systems, provide a strong layer of security for these interactions, and provide an effective solution for managing the extensive volumes of data that effective management of this environment requires. These applications are the Cross System Integrator (XSI), the Cross Data Integrator (XDI), and the Cross Security Manager (XSM).



I. I. The landscape, IT and OT, and the muddy middle

Over the last few years, considerable attention has been paid to the differences between IT and OT technology, focusing on cultural differences. Historically, these two areas were very separate, with OT staff coming out of the instrument technology and electrical engineering background and IT Staff coming out of the system administration, database administration, and programming backgrounds. Design philosophies were also very different. IT expected regular infusions of new technology and change, and the OT world focused on absolute reliability (once it works, don't touch it!). Over the years, the divide between the two areas has shrunk with the introduction of IP networks to transport data and the use of computer-based applications. Minimalizing the divide has occurred by required updates and patching instead of strictly mechanical controls. More recently, the systems need to share data for more effective grid management, planning, and operation.

While there still exists a widely held view of these worlds as separate due to NERC Critical Infrastructure Protection (CIP) with its Electronic Security Perimeter, (e.g., the logical border surrounding a network to which BES Cyber Systems (BCS) are connected using a routable protocol), the recognition that there is a “muddy middle” continues to grow. The recent Colonial Pipeline ransomware attack highlighted the issue. The OT system had to be shut down even though the attack never reached the OT systems. Operations required the interaction between IT systems (e.g., billing, scheduling, etc.) and the OT systems (industrial controls over the pipeline SCADA). In today's electric utility world, and certainly tomorrow, these boundaries become stressed with the integration of additional renewable energy and the addition of Electric Vehicle (EV) charging loads. Adding to this stress are advances such as using meters to provide voltage feedback, last gap outage signals, the tie-in with demand response automation to help balance the grid operations, and automated distribution management. Use cases for data from multiple devices routinely need to cross the IT/OT divide.

The continued barrage of attacks on systems and the continuing success in breaching perimeter defenses leaves us, from a security perspective, having to abandon the notion that a solid perimeter and a solid separation between IT and OT is still feasible and desirable. Instead, the focus has to be on a security approach recognizing that breaches will happen. This approach begins by breaking down the notion that system interactions can be trusted. Logical Network segmentation for the use cases identified, such as incorporated in the PCI credit card standard, was a method to limit the trust within the network. However, with the increasing complexity of the data and application integration required for the modern electrical grid, the focus has shifted to implementing Zero Trust Architecture (ZTA) principles to promote the needed security.

II. NIST 800-207 on Zero Trust Architecture

Zero Trust Architecture has become the rage, and with good reason. Perimeter defenses alone have led to numerous breaches of systems and data. Zero Trust has been used to promote products as with any theory du jour. Shamelessly, we will make the case that the Cross Integration Suite provides a significant foundation for Zero Trust implementation.

Nevertheless, first, let us review Zero Trust Architecture as discussed in NIST 800-207.
At the basic level, ZTA is:

"Zero Trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be evaluated continually. Zero Trust Architecture is an end-to-end approach to enterprise resource and data security that encompasses identity (person and nonperson entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure."

NIST has identified fundamental principles for Zero Trust:

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. A dynamic policy determines access to resources, including the observable state of client identity, application/service, and the requesting asset, and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current assets, network infrastructure, and communications and uses it to improve its security posture.

NIST outlines three fundamental approaches to the design and implementation of Zero Trust Architecture:

ZTA Using Enhanced Identity Governance - The enhanced identity governance approach uses the identity of actors as the critical component of policy creation. Enterprise resource access policies are based on identity and assigned attributes for this approach. The primary requirement for resource access is based on the access privileges granted to the given subject. Other factors such as the device used, asset status, and environmental factors may alter the ultimate access authorization.

ZTA Using Micro-Segmentation - An enterprise may choose to implement a ZTA based on placing individuals or groups of resources on a unique network segment protected by a gateway security component. In this approach, the enterprise places infrastructure devices to protect each resource or small group of related resources.

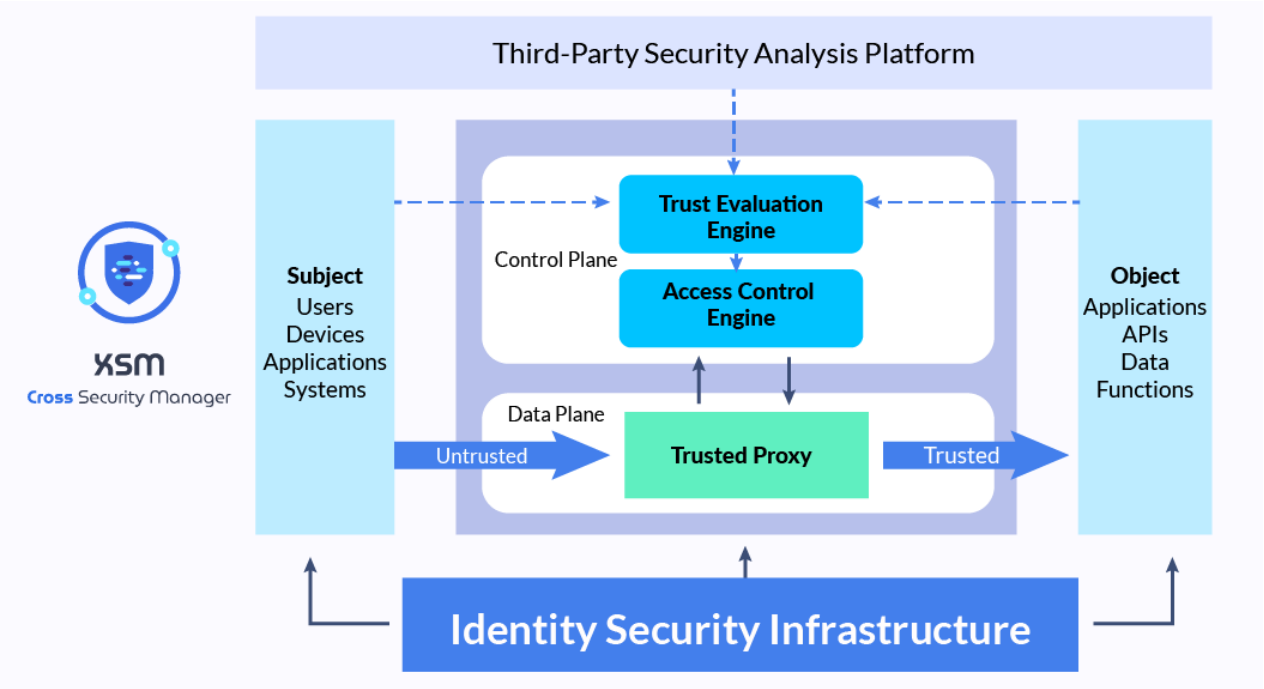
ZTA Using Network Infrastructure and Software Defined Perimeters - The last approach utilizes the network infrastructure to implement a ZTA. The ZTA implementation could be achieved by using an overlay network. In this implementation, the agent and resource gateway establish a secure channel for communication between the client and the resource. With this background, it is

time to show how the Cross Integration Suite can underpin the NIST vision of a ZTA using the Enhanced Identity Governance approach.

III. Cross Integration Suite and the implementation of Zero Trust Architecture

The three components of the Cross Integration Suite are Security (XSM), System Integration (XSI), and Data (XDI) management that all play an essential role in fulfilling the key attributes of Zero Trust Architecture.

Cross Security Manager (XSM) contains the user information, the user authorization information, and the device information. Its API structure can populate the user and device information from other existing applications and directories. XSM contains the engine that provides user requests to access applications and/or data. This engine can allow adaptive authentication, providing for higher levels of verification depending on the request. From simple passwords to MFA to specific certificates, XSM can assure the appropriate credentials for every action. XSM, with its security rules engine, provides the dynamic capabilities to adapt the authorization process based on criticality and other analytical inputs. In conjunction with XSI and XDI, the Cross Integration Suite assures that all access to resources is session-based, all access and activities are verified acceptable for the combination of person, device, service, and data and that all interactions are logged into a database to assist in the identification of anomalies.



Cross System Integrator (XSI), with its API management core and microservices architecture, provides a layer 7 gateway to application resources whether they are IT, OT, or the "muddy middle", thus shutting off access to unauthorized microservices. Beyond the security role, XSI, with its microservices foundation, provides a more Plug-and-Play integration irrespective of protocol and data conversion requirements and a powerful engine for business process automation. This robotic process automation (RPA) simplifies the tying of the authentication engine rules into the business process by providing the necessary checks to the XSM for appropriate authentication.

Cross Data Integrator (XDI) plays a similar role to XSI with its collection of elastic search databases, a data mart, and operational data store roles in the data warehouse. In addition, microservices access the various data objects, assuring XSM that access to data resources is appropriately authorized. XDI also serves the essential repository function to maintain log and activity data to monitor the organization's security posture. As the system is API and microservices-based, this monitoring is especially critical with the slow nature of most API attacks.

IV. The Cross Integration Suite is not a complete implementation of ZTA. However, it substantially supports the enhanced identity governance approach described in NIST 800-207, with its store of identities, devices, and its rules engine to drive the proper authorization to specific functions and data as a web access gateway access to APIs. This capability is significantly expanded using the capacity in XSI and XDI to block unauthorized access in the interactions between applications and between applications and data sources. In some settings, additional network-based security measures are appropriate. These may include the use of Data Diode technology to assure one-way data movement and the use of security devices in front of IoT devices without native authentication capability, such as sensors, grid switches, or cap banks, and network micro-segmentation. Micro-segmentation can be accomplished through either ACL based approaches (although not recommended in complex environments without robust ACL auditing tools), or through Software Defined Networking. In the Industrial Control World, where many devices and sensors lack the inherent ability to authenticate, an overlay network (such as Tempered Networks and Blue Ridge Networks) provides the additional authentication, cloaking these insecure devices denying connections to inappropriate users/devices.

V. Conclusion:

In Gartner's recent hype cycle for security technology, they identified that:

"Turnkey and highly integrated solutions continue to trend upward. Smaller, less security-mature organizations are growing into new security operations requirements as they become more dependent on connectivity and SaaS and become dominated by compliance and regulatory requirements. Alongside turnkey requirements, consolidation is a key theme, with OT and IT security slowly converging. Differences in requirements are fading. Cloud access security brokers (CASB) are more frequently associated with network security technologies such as Zero Trust Network Access (ZTNA) and Secure Web Gateway (SWG). Security and risk management leaders responsible for security operations should be looking to reduce overlapping capability across different technologies and become more risk-focused."

The Cross Integration Suite addresses this sweet spot by providing API access control, zero-trust application access, control over data flows, and enhancing these with a robust rules engine and robotic process automation tools.