Lanner

IIoT

Computing

Innovative Platforms for Next Generation IIoT

Industrial IoT Edge Security Kit

Version: 1.0

Date of Release: 2019-05-13

Cybersecurity Threats to IIoT

The IT/OT converged IIoT infrastructure has revealed numerous vulnerability due to its connectivity over public networks, exposing exploitable opportunities for hackers. According to the Global ICS and IIoT Risk Report by CyberX, one-third of the OT networks where the processes are controlled by industrial control systems (ICS) are exposed to the public internet.

Meanwhile, the implementation of IP-based connectivity used to communicate between multiple industrial devices, and also the growing use of sophisticated microprocessors in the industrial facility, has actually led to greater security risks which did not exist previously. This makes industrial control systems (ICS) one of the most vulnerable targets in the industrial world. Several issues have been addressed toward current unsecure IIoT adoption which includes:

1. Insecure interface
2. Insufficient Authentication/Authorization
3. Insecure Network Services
4. Lack of Transport Encryption/Integrity Verification
5. Weak protections of the confidential
6. Insecure Cloud Interface

For years, the industrial section is seeking the most effective solution to protect IIoT deployment in an end-to-end architecture in order to protect their data assets, critical operations and privacy vulnerabilities.

Securing the Industrial Control Systems of Industrial IoT

IIoT infrastructure should be protected by an aggregated security solution that does not compromise operations, service reliability or profitability. In addition, securing the OT operations should be conducted locally and at small-footprint so that no latency will be generated to mission-critical operations. Thus, a secure IIoT architecture requires a scalable edge architecture that enables real-time protections to avoid hackers exploitation.

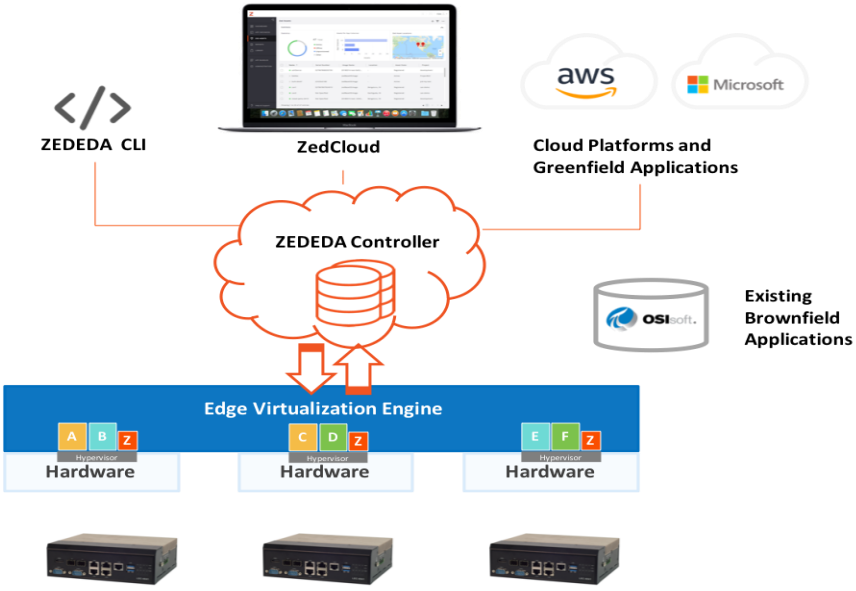
To secure millions of IoT endpoints, controllers and gateways in complex, multi-vendor environments, a comprehensive Edge Security Platform should be equipped with following capabilities:

- Hardware root-of-trust on each device, gateway and controller
- Mutual Authentication between device and gateway
- Secure Communication Overlays design

- Real-time Monitoring and Analysis towards non-trusted code execution
- Flexible Remote Deployment Framework to secure software assets migration and recovery

Lanner Edge Security Kit

Comprised of all the necessary pieces to secure IIoT Industrial Control Systems, the Lanner Edge Security Kit is a turnkey solution that provides seamless endpoint authentication, software property protection, service lifecycle management and advanced device/application monitoring capabilities to enable mission-critical operation, high-availability and mitigate a variety of cyberattacks. The kit itself contains three cutting-edge elements to secure Industrial Control Systems:



Lanner Security Gateway LEC-6041

Lanner's security gateway, LEC-6041, is designed to protect the communication in both IT and OT domains. LEC-6041 series is empowered by Intel Atom x7-E3950 or Celeron N3350 for low power consumption and capable processing performance. As the security gateway, LEC-6041 is designed with two key hardware features, including programmable LAN bypass technology and TPM 2.0 onboard.

Furthermore, as a rugged firewall deployed in challenging environments, LEC-6041 is compliant

with IEC 61850-3 and IEEE 1613 certification, as well as 1.5 KV magnetic isolation protections for LAN port and 15KV ESD Protection for I/O ports. The system can operate in a wide range of operating temperature from -40°C to 75°C. All of the designs is to make sure this security gateway LEC-6041 will never fail while operating in hazardous surroundings which OT environment is always be.

Lanner Platform Guard

To ensure secure communication from both device-to-gateway and gateway-to-IT layers, Lanner security gateway LEC-6041 is protected with comprehensive firmware security features, encrypted platform identity and TSS2.0 compliant middleware. Beyond the hardware layer, Lanner Platform Guard provides a set of solid designed and validated APIs to make sure that:

- software code execution is being measured
- data-at-rest is protected
- data-in-transit is encrypted
- confidential are being sealed

To list out in details, Lanner Platform Guard delivers:

1. **Secure Boot and Intel Boot Guard**

   Intel Boot Guard is provided by Intel to enable ACM-based secure boot that verifies a known and trusted BIOS is booted on platform. By establishing a trust chain, secure boot utilizes cryptographic code signing techniques, ensuring that firmware, OS and application are only executed by a trusted party. Use of secure boot technology prevents hackers from inserting malicious instruction sets, thereby preventing attacks.

2. **Encrypted Platform Identity API**

   Every time a smart actuator in the manufacturing floor connects to the network, it should be authenticated prior to receiving or transmitting data. This ensures that the data originates from a legitimate device and not a fraudulent source. Secure, mutual authentication—where two entities (device and service) must prove their identity to each other in order to build up trust and helps protect against malicious attacks. As a critical position in OT network topology, Lanner security gateway is empowered with a set of encrypted platform identity which is unique for every shipped device and its identity is not allowed to be modified permanently. To allow the authentication process being executed, Lanner provides a set of easy-to-use APIs to grant secondary development to secure the communication and protected every piece of code being executed on the computing space.

3. TSS2.0 compliant API

With newly launched TPM architecture 2.0, a better secured hardware level of trust is given. In Lanner Platform Guard, you can also find TSS2.0 compliant APIs which allows you to seal your keys in NVRAM, measure your code by PCR and utilizing the cryptographic algorithms involving symmetric cryptography and asymmetric cryptography as follows:

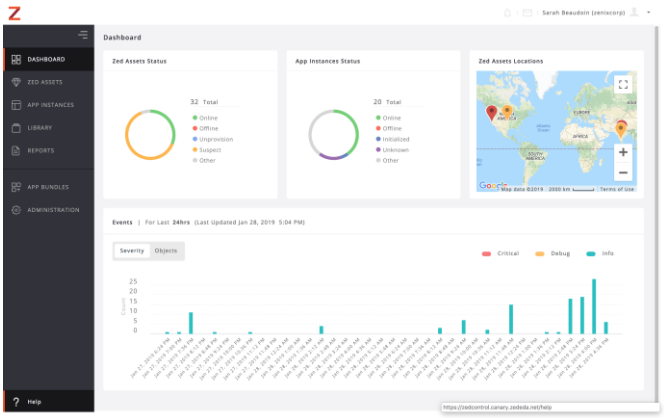
Symmetric cryptography

- HMAC
- SHA1
- SHA256

Asymmetric cryptography

- ECC
- ECC BN-256
- ECC NIST P-256
- ECC256
- ECDH
- RSA1024
- RSA2048

Zededa Real-time Edge Platform



ZEDEDA is an application orchestration platform company that offers 100% cloud-managed deployment, operation, and security automation for your real-time edge applications. ZEDEDA's Edge Application Platform provides a consistent, automated, hardware agnostic, and secure operating model for mass-deployed edge devices and applications - eliminating manual configuration processes, requirements for on-site expertise, or any need to manually update software.

1. One-Click, Full Stack Provisioning

100% cloud managed makes it possible to deploy hundreds, thousands, or millions of remote, autonomous embedded devices with a centralized operations team. Rather than requiring each application, OS, and device be provisioned, configured, and tested manually, embedded devices are full-stack provisioned automatically from the cloud. Once they come online the ZEDCloud automatically downloads and provisions all software without any manual intervention.

2. Global Deployments Centrally Managed

ZEDEDA provides powerful tools to simplify and automate management of your entire deployment from any browser through the ZEDCloud interface. Complete visibility into device and application health, and automated, secure over-the-air software updates to millions of devices globally, and one-click disaster recovery of applications provides unprecedented control, visibility, and service reliability to large scale deployments.

3. Industrial App Store Simplifies Future Service Deployment

Industrial computing has witnessed a technological leap with the emergence of IoT and ubiquitous connectivity of edge computing making it possible for devices with long, multi-year lifecycles to act as a platform for deploying new, revenue enhancing capabilities on existing hardware. ZEDEDA's platform powers secured method of deploying new industrial applications on existing equipment.

About Lanner Electronics

Lanner Electronics Inc. (TAIEX 6245) is a world-leading hardware provider in design, engineering, and manufacturing services for advanced network appliances and rugged industrial computers. Lanner provides reliable and customizable computing platforms with high quality and performance. Today, Lanner has a large and dynamic manpower of over 1,000 well-experienced employees worldwide with the headquarters in Taipei, Taiwan and subsidiaries in the US, Canada, and China.

About Zededa

ZEDEDA is an application orchestration platform company that offers 100% cloud-managed deployment, operation, and security automation for your real-time edge applications. ZEDEDA's Edge Application Platform provides a consistent, automated, hardware agnostic, and secure operating model for mass-deployed edge devices and applications - eliminating manual configuration processes, requirements for on-site expertise, or any need to manually update software.