Agora

Security for the Agora Platform

Securing an Edge Computing and IIoT Landscape

Agora IIoT platform contains various elements of security for both the edge computing as well as transmission and ingestion into the cloud environment

Agora utilizes a holistic security strategy that spans secure design, secure deployment, and secure operations through end of life. As such, security is built into the entire product lifecycle. Agora security includes people, process, and technology measures to build comprehensive protection for the platform. The Agora security strategy is aligned with well-established standards and best practices in the industry, such as the Industrial Internet Consortium, NIST Cyber Security Framework, and the Cloud Security Alliance. Elements from these industry standards and frameworks that are applicable to Agora are taken and implemented as security mechanisms, controls, technologies, and security processes within the Agora ecosystem.

Agora leverages Schlumberger's internal standards and best practices like the secure software lifecycle management (SLM) for software and concurrent lifecycle management (CLM) for hardware. SLM specifies software security best practices like security requirements, threat modeling, static and dynamic code analysis, and penetration testing, among others. CLM includes security requirements for the hardware platform like hardware root of trust and secure boot. To ensure that Agora security mechanisms also comply with industry standards, an external audit was performed against the SOC 2 standard and Agora's security controls were certified for compliance.

SECURITY FOR THE AGORA PLATFORM

Alignment with industry standards and best practices

The Agora security strategy is well aligned with well-known security standards and best practices. Prominent among them are the NIST security standards, NIST cyber security framework, industrial internet consortium, and the cloud security alliance.

NIST has a number of cyber security guidelines published in the sub-areas of security like cyber security framework [CSF], cryptography [NIST SP 800-175B], security controls [NIST SP 800-53], cyber security feature baseline for IoT [NISTIR 8259], and ICS security [NIST SP 800-82] among others. Agora security incorporates the relevant parts of these guidelines in developing the Agora platform. For instance, all the cryptography mechanisms like encryption, digital signing, hashing, and key management are compliant with the NIST cryptography guideline. Also, Agora security team reviews changes and updates in these guidelines to ensure that the updated recommendations are implemented in the platform.

Similarly, Agora platform is also aligned with the IIC security framework and security controls from the cloud security alliance. Suggested controls from IIC security framework related to endpoint protection, secure connectivity, security monitoring, security configuration, and data protection are implemented in the Agora platform.

Data protection throughout the data lifecycle

.

AES-256

256 BITS ADVANCED ENCRYPTION STANDARD

Approved by the National Security Agency for top secret information..

All data in the Agora ecosystem is protected during its entire lifecycle. Security controls are in place to protect data at rest, during transit, or while in use. All transmitted data is permanently stored at rest in the Google Cloud platform, where it is encrypted using AES-256. The keys for this algorithm are managed securely through the platform itself. Configuration and device management data is stored on Microsoft Azure platform, where it is encrypted using AES-256 and the keys are permanently stored in hardware security modules (HSMs). A small amount of data is stored on the Agora gateway during its acquisition and transit to the cloud. This data is again encrypted using AES-256 and the encryption key is stored in a secure hardware storage (TPM chip).

All data in transit is protected using Transport Layer Security (TLS 1.2), regardless whether the data is sent over HTTPS or secure MQTT. While the data is at rest or in use in the cloud, strong separation is enforced where the data is not available outside its tenant. Strong access control is enforced to ensure that raw and processed data is accessible only to authorized entities with the tenant. On the gateway, data at rest or in use is encrypted on the LUKS filesystem. Supporting techniques like memory map randomization and continuous security monitoring are implemented to provide enhanced security.

A secure by design edge device

.

The AgoraGateway is the central IoT edge device for connectivity and security. Agora has provided protection for the gateway by implementing strong security controls in the design. A hardware-based root of trust is implemented using a Trusted Platform Module (TPM) 2.0 chip on the hardware. The TPM chip provides unforgeable identity to the device and acts as a secure storage for cryptographic secrets. The TPM endorsement key is used to authenticate the device to the cloud services and this authentication is leveraged to initiate a secure communications session from the gateway to the cloud. Cryptographic secrets like encryption keys, passwords, and private keys are stored inside the TPM memory for secure storage.

The gateway enforces secure boot by leveraging the TPM chip for providing protection against software tampering and malware infection. Secure boot only allows trusted software to run on the gateway, whereas any untrusted software will be identified, and alerts will be sent out to the operators. The secure boot process measured the integrity of the software that is being run on the gateway against a known set of trusted references values. It is assisted by the TPM 2.0 chip, which stores the trusted references values. When the gateway is booted, integrity of every layer from the boot loader, to operating systems, to the applications is checked against the values stored in the TPM. If the values do not match, then an alert is sent out.

A common weakness to industrial IoT systems is that they deploy services that are accessible over the Internet.

Attackers attempt to connect to these services and exploit their vulnerabilities. Agora mitigates this threat by ensuring that no Internet facing services are allowed and all incoming traffic on the firewall ports are blocked. When connected to external systems, the Agora gateway always initiates outbound connections to trusted and whitelisted external entities.

Federation and identity management

.

IoT systems generally implement weak authentication. Oftentimes, the password hashes are stored on the device itself. This weakness makes the IoT system vulnerable to attackers, especially when incoming connections are not blocked. Agora avoids these issues by ensuring that there are no credentials stored on the device, while still enabling strong authentication. This is achieved by leveraging identities used for authentication with corporate authentication systems such as Active Directory Federation Services (ADFS) or with cloud-based authentication like Azure Active Directory (AAD). The credentials are stored and verified in these external servers where sophisticated IT controls are protecting these servers. This also enhances the usability as now the users in the field or in the cloud can authenticate by using a single identity.

For offline environments, a secure hardware token is used to authenticate the users. It contains a public-private key pair that is used to identify the user to the gateway-based services. Example of such hardware are Yubikey and Google Titan.

Authorization and access control

Authentication is followed by secure access control. Agora implements strong role-based access control (RBAC) in the cloud and on the edge. In cloud environments, user and application roles are configured and users and applications are mapped to them. Access privileges on data and control actions are then mapped to these roles. RBAC enforcement ensures that each customer will only have access to its own data and can perform control actions only on its deployments.

Similarly, RBAC is enforced on the gateway device to limit access to data and gateway management functions User roles and their access rights are downloaded on the gateway to ensure enforcement. Only the applicable subset of user roles and access rights is downloaded from the global access control lists, so that authorized personnel in that region can access the gateway but the gateway does not need to store the global access control database.

Utilize a secure connectivity approach

Secure connectivity to external networks is provided by using a defense-in-depth approach. The AgoraGateway can only send data to selected trusted destinations as prescribed in the gateway configuration.

The AgoraGateway can connect via cellular, ethernet, and satellite infrastructure for northbound connectivity. The exposure over Ethernet over customer's network or over satellite is lower as compared to the cellular LTE connection. To minimize the attack surface on the cellular networks, the AgoraGateway uses an Access Private

Network (APN) over cellular network to directly send the traffic to a landing point in the Schlumberger DMZ. This enables superior protection since the data is traveling only over a private network.

At the DMZ, the landing point is a next-generation firewall that inspects the headers and ensures that only data destined for whitelisted locations is allowed while everything else is denied. From the DMZ, data destined for Microsoft Azure cloud is sent over a Microsoft Azure ExpressRoute, which is a private direct connectivity between the Schlumberger DMZ and the Azure data center. At the protocol level, TLS 1.2 is used to protect all traffic.

Southbound connections are secured using an adaptive approach. Communications with web servers is using HTTPS using TLS 1.2. Network and application configuration services are accessed over SSH using the common well-established method of certificate-based authentication.

Cloud security strategy

Agora follows a multi-cloud strategy that currently contains Microsoft Azure and Google Cloud Platform (GCP). Device commissioning and management is performed through Microsoft Azure services. This includes the device provisioning service (DPS) and the IoT Hub. Telemetry data can be sent to Google cloud, Azure cloud, or the customer's private cloud depending on the deployment use case. Agora cloud services are developed based on Schlumberger cloud security standards that form a comprehensive body of cloud security standards and guidelines. It includes the cloud security framework, standards for encryption, penetration testing, secure deployment, authentication and access control, and compliance among others. Cloud security guidelines are published to provide guidance on secrets management, network security, secure deployment practices, and threat modeling. Agora leverages these standards and best practices to build a secure cloud service.

SECURELY DELIVER DATA WHERE YOU NEED IT

Agora can connect to Google cloud, Azure cloud, or a customer's private cloud.

To protect customer data, the Agora cloud utilizes encryption using AES-256 with secure key management. Multi-factor authentication is enforced, and identity federation is supported to allow customers to authenticate using their native credentials. Authorization is managed via role-based access control (RBAC). A strong tenant isolation model is used to keep data and applications segregated for each customer. All these features work together to secure customer's data and applications in the cloud. Security related events are logged and monitored to ensure security incidents are detected. These incidents are sent a dedicated 24/7 security supervision and management center where any detected incident is responded using a cloud incident process.

Establishing a secure development lifecycle

Agora software development follows secure software development practices to ensure that security has been included in every stage of the software lifecycle. Security requirements, threat modeling, and secure design are included in the early stages of development, whereas static and dynamic code analysis are performed during the implementation and testing phases. Static, dynamic, and open source code analysis is integrated into the automated software deployment platform to ensure it is consistently performed during each development cycle. Finally, penetration testing will be performed by engaging a third-party vendor to perform offensive security testing in the deployment staging environment.

Security qualification processes

Implementing a standard process for security validation that checks the readiness of an application for deployment against the security standard. Compliance is maintained throughout development and audited at certain development stages. For Agora, two security qualification processes were undertaken, namely the Security Application Qualification Process (SAQP) and Cloud Security Qualification Process (CSQP).

The SAQP process looks at the security risks in the system architecture and requires the development organization to perform security testing against the application. It looks at various aspects of the endpoint or application communications channels and performs security testing on all those channels. Either recommendations for retesting or acceptance of the application are provided.

Similar testing is performed for any cloud hosted application as part of the CSQP process. In this case, special emphasis is put on the security of publicly exposed services or endpoints to ensure proper communications security and network security are in place. Additionally, compliance with Schlumberger cloud security standards are performed. Threat modeling is performed to ensure that the application architecture follows the best practices and to adequately address any threat that is discovered during the analysis process.

Isolating tenant resources

In cloud multi-tenancy provides a shared common infrastructure across multiple customers leading to economies of scale. Each customer's instance is called a tenant. Isolating these tenants is critical to ensure that the confidentiality, integrity, and availability of each customer's data and applications can be ensured. The Agora cloud environment achieves this by implementing logical isolation at the application layer, network layer, or data layer. Tenant isolation ensures that the data is not accessible across tenants. Tenant isolation in Agora is integrated with access control system to ensure it works in sync with RBAC. The RBAC system then limits their access to resources like applications, data, or control functions within their tenant.

Apart from the application layer isolation, tenants can also be attacked by adversarial virtual machines (VMs) that are deployed on the same physical server in the cloud data center. Each cloud service provider implements specific controls to address this threat. For example, Microsoft Azure Hypervisor enforces memory and process separation between virtual machines and it securely routes network traffic to guest OS tenants. This eliminates possibility of and side channel attack at VM level. The hypervisor and the host OS provide network packet filters to help assure that untrusted virtual machines cannot generate spoofed traffic or receive traffic not addressed to them, direct traffic to protected infrastructure endpoints, or send/receive inappropriate broadcast traffic.

Deploying a secure gateway

The AgoraGateway is based on Linux Debian 9. System hardening is performed to ensure that the gateway and operating system attack surface is minimized. All unnecessary ports, services, and communication links are blocked. Industry-standard benchmarks like CIS-CAT have been deployed to reduce the attack surface qualitatively and quantitatively. Endpoint security assessment tools are commonly utilized to map the attack surface and then analyze their recommendations to further reduce the residual attack surface.

Securely updating and managing edge devices

Software deployed on IoT systems tend to be unpatched for long periods of time. This creates publicly known vulnerabilities. Patching IoT systems can be challenging because cloud-based updates require secure connectivity to the cloud where local updates require manpower and opens avenues for malware infections. The AgoraGateway leverages its continuous and secure connection to the cloud to update software on the device from the cloud. It does not provide any local update functionality, which—in combination with secure boot—protects against any potential malware infections. Cloud-based software updates ensure that software on IoT systems is always running the latest versions, and hot patches for security can be deployed on demand in a fast and smooth way.

> In today's IT environment, each IT asset is monitored continuously and any attack is detected in near real time.

Security monitoring and incident response

Alerts are generated and corrective actions are taken for incident response. Typically, organizations have no visibility into the IoT environment. If an attacker tries to attack an IoT device, they will receive no alerts. To address this, Agora has partnered with major technology vendors to provide security monitoring for their IoT environments. The monitoring solutions collects security related events continuously and send them to the cloud monitoring service for detection. The cloud service correlates the events with known attack patterns and threat intelligence. Once it is confirmed that the events are due to a security incident, the security incident is sent to the automation platform in the Schlumberger Security Operations Center. After initials alerts are sent, an analyst is assigned to the incident. Schlumberger IT group and the Agora Edge Operations Center (EOC) resolve the incident and initiate incident response actions.

Fostering a security culture

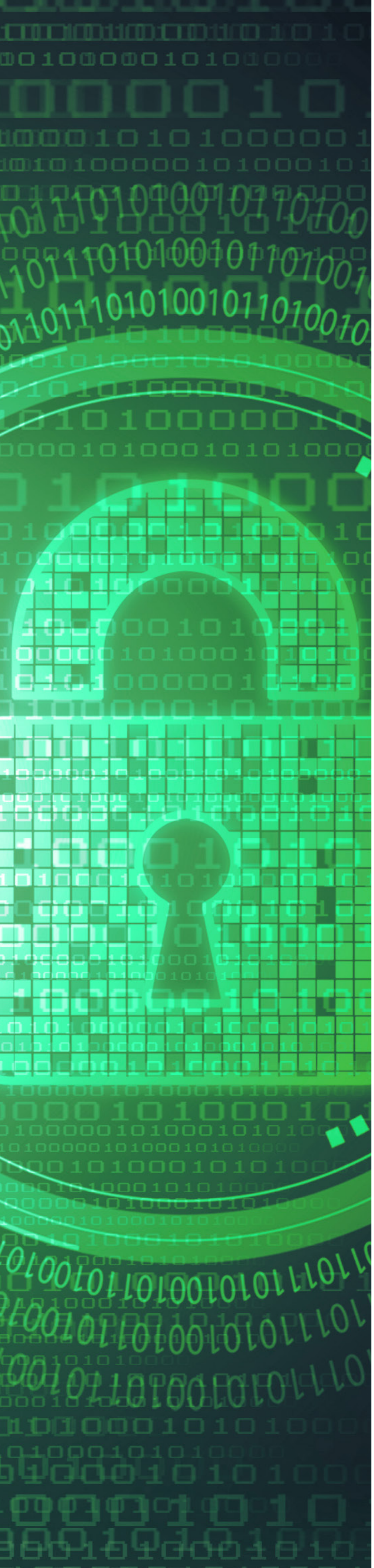
Agora's strong security culture aligns with Schlumberger's global security culture and strategy. The security culture focuses heavily on security awareness and training. Security is a core attribute of the Agora environment and the Schlumberger organizational culture. Security begins at the pre-employment stage with a comprehensive background check for all employees. Upon hiring, new employees can only get access to IT resources upon completing an IT security training and passing an exam. All Schlumberger employees are required to complete an annual training certification on IT security and customer data handling. This is a mandatory part of the Schlumberger performance management process encompasses quarterly performance reviews, including a review of security trainings and reminders for compliance.

Security tests and certifications

Ongoing assessment for industry-standard Service Organization Controls 2 (SOC 2) accreditation for security and availability ensures that the Agora platform is secure, and all best practices are adhered to for high-quality service delivery and management. The certificate would attest Agora security controls that ensure superior security and availability in the Agora environment to meet operational demands.

Security assessments

Agora cloud is compliant with Schlumberger Cloud Application Security Qualification Process (CSQP). CSQP is an umbrella of multiple qualification processes to ensure that all aspects of cloud security are tested and qualified. It includes Security Application Qualification Process (SAQP), Network Analysis Qualification Process (NAQP), Trade Controls Compliance (TCC), Data Residency, Data Privacy Qualification Process (DPQP), and legal. A brief overview of these processes is provided next:



Data Privacy Qualification Process (DPQP): DPQP applies to personal data like Personally Identifiable Information (PII), Personal Health Information (PHI), and Payment Card Industry (PCI). It also ensures compliance with GDPR, if personal data is involved.

Trade Controls Compliance (TCC): TCC ensures application compliance against trade and customs requirements. The intent is to keep up to date with latest restrictions applied to regions/countries.

Data residency: Many countries and customers have a legal or compliance requirement to ensure that their data resides in a specific geography. The intent of this qualification process is to ensure that these data residency requirements are complied with by the cloud platform.

Legal: Legal compliance checks are performed to ensure that data ownership, disclosure and lifecycle management clauses, limitation of liability are well understood and complied by.

Security Application Qualification Process (SAQP): SAQP is the most involved qualification process in the group. It includes understanding the model of deployment, evaluating architecture of the solution, performing threat modeling, evaluate OS vulnerability for IaaS, evaluate application vulnerability (web headers, certificate), performing and validating Identity and Access Management, performing penetration tests against the site (web, rest API), and to validate encryption in transit and at rest.

Network Analysis Qualification Process (NAQP): The intent of NAQP is to evaluate network performance of the application. NAQP perform analysis to evaluate the impact the application can have on the network bandwidth. If an application is consuming excessive bandwidth, it impacts the performance of other applications as well. NAQP ensures that each application uses reasonable network resources.

Achieving SOC 2 certification

Agora engaged an independent accredited auditing firm for SOC 2 certification. The audit follows the security and availability trust services categories set forth by the AICPA (American Institute of Certified Public Accountants). It ensures that all industry-standard practices are followed relative to the design suitability and operational effectiveness of the controls—giving customers increased confidence in the security and availability of the Agora environment. The accreditation is renewed as new services move to general commercial availability. For more information, read the Trust Services Criteria published by the AICPA SOC for cyber security, which assesses an organization's cyber security risk management program and the controls based on cyber security objectives defined by entity management. The audit has five areas: security, availability, processing integrity, confidentiality, and privacy. Agora's audit is comprised of security, availability, processing integrity, and confidentiality.

SOC 2 security principal refers to protection against unauthorized access and use. It covers components like network and web application firewalls (WAFs), two-factor authentication and intrusion detection. Availability ensures that systems are available for use as per a defined service level agreement. Monitoring network performance and availability, site failover and security incident handling are critical in this context. Process integrity ensures data processing must be complete, valid, accurate, timely and authorized. Finally, confidentiality of all data in terms of access and disclosure must be maintained. Access can be controlled by network and application firewalls, access control lists, and authorization systems, whereas disclosure should be compliant with organization policies.

SECURING DIGITAL PERFORMANCE

Security is a foundational pillar of digital transformation..

An edge computing and IIoT platform is only as effective as it is secure.

For more information about edge computing and IIoT security, contact Apurva Mohan at AMohan5@slb.com.

To learn more about Agora, visit AgoraIoT.com.