AYYEKA CYBER-SECURITY & COMMUNICATION PROTOCOLS

OVERVIEW

Ayyeka provides end-to-end remote monitoring solutions consisting of a Wavelet data acquisition device, one or more sensors, wireless connectivity, and data and device management software. Ayyeka's Wavelet device and software (IoT Platform) provide input for decision makers with continuous data on the state of their infrastructure and dispersed assets. The Ayyeka solution is intended and engineered for passive monitoring, and is not intended for control of critical assets and processes.

Fundamental cyber-security considerations for telemetry device manufacturers and service providers include encryption, DXWKHQWLFDWLRQUHPRWHGHYLFH4UPZDUHXGDWHFDSDELOLWLHVDQGSKLFDODFFHVVUHVWULFWLRQV7KVGRFXPHQWGHWDLOVW
YULRXVPXOWLODHUHGFEHUVHFXULWFRQVLGHUDWLRQVRIWHQGGWHQGHNDHULQFOXGLQJWWKHUGZDUHZLUHOHVV
communication, data hosting, and data delivery layers of the technology stack.

WAVELET (AYYEKA INDUSTRIAL IoT EDGE DEVICE)

The Wavelet device is an ultra-low power, fully autonomous wireless telemetry device. The Wavelet collects data from a connected sensor(s) using industry-standard protocols, including analog (4-20mA and 0-10V), serial (RS485, RS232, and 6ĐQGGLVFUHWHSXVHFRQWLQGL1WDO26HQVRUGDWDFROOHFWLRQEWH:DHOHWRFFXVDWFRQ4XDEOHVDPSOLQJ
frequencies.

The data obtained from the sensors is logged locally on the device with a timestamp and stored in industrial-grade internal memory in a proprietary binary format. This locally stored data is then transmitted to a Wavelet server (Ayyeka Private &ORXGRUFXWRPHURQSUHPLVHVVHUHUDWDFRQ4XDEOHWUDQVPLVVLRQIUHTKQFRUEHFHSWLRQIRFRQ4XDEOHWKHVROGV

WAVELET COMMUNICATION INTERFACES

All Wavelet devices are equipped with the following three communication interfaces:

1. Cellular Modem (4G, 3G, 2G)

2. Bluetooth Low-Energy for information on device status during installation and maintenance

3. USB for cabled console access and out-of-band configuration and trace-level debugging

Wireless Communication

Cellular Modem

The Wavelet communicates via cellular modem over industry-standard, encrypted, and secured protocols. Communication from the Wavelet to the server is in a binary, proprietary format. This communication is encapsulated in HTTPS or MQTTS using TLS 1.2, leveraging public key cryptography as well as pre-shared keys (unique username and password) for MQTT device authentication. Secure communication from the Wavelet supports the following cipher suites:

- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA
- ECDHE-RSA-AES128-SHA
- ECDHE-RSA-AES256-SHA
- ECDHE-ECDSA-AES128-SHA
- ECDHE-ECDSA-AES256-SHA
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA256
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA256

The Wavelet uses dynamic, NAT'ed, and firewalled IP addresses offered by Ayyeka's tier 1 cellular providers, which offer Verizon, AT&T, and T-Mobile network coverage in the US and coverage with several hundred other carriers around the globe via their own APNs.

There are no listening TCP/UDP communication ports to the Wavelet. More specifically, the device can initiate sessions with a server, but all incoming connections to the device are automatically rejected. Direct access to the Wavelet is theoretical rather than practical, as scanning Wavelet devices would first require penetrating the tier 1 cellular providers' firewalls and traversing NAT.

Communication sessions are limited in duration (typically 2 minutes or less) and allocated random IP addresses from a secured pool per session.

Security updates, firmware upgrades of the Wavelet device and embedded cellular modem*, can be pushed through cellular communication only.

* Over-the-air security update capabilities of the modem are prerequisites that were demonstrated as part of the device certification and acceptance criteria by Verizon Wireless for access to the Verizon LTE network.

Bluetooth Low-Energy

Ayyeka has developed multiple layers of security and authentication to enable a communication session with a Wavelet over Bluetooth via an embedded Bluetooth Low-Energy (BLE) module in the Wavelet and an iOS or Android device using the AyyekaGo mobile application. These layers of security and authentication include:

1. Pre-shared unique pairing key per Wavelet device

2. Communication encryption using Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) encryption
   a. The first phase is key establishment, which is done through ECDH and HDKF. Salt exchange for each message is utilized to prevent reply attacks. The encryption is done with AES CBC, and data integrity is done using HMAC-SHA256.
   b. This method provides the following benefits: eavesdropping on the connection does not reveal anything to the snooper, replay attacks are impossible, man-in-the-middle attacks do not reveal anything to the attacker.

3. Until the AyyekaGo mobile app, over BLE connection authentication is performed, the Wavelet does not answer any other messages. Moreover, in a case a non-authentication message (or a wrong authentication message) is sent, the Wavelet slams the connection. This is a general principle, related to all security aspects: both the Wavelet and the mobile app, in case an unexpected message with a bad data, not decrypted correctly, with a wrong length and etc. is received, the first side who is aware of the problem slams the connection.

USB Interface

It is important to note that sensitive information and operations are NOT available via the USB interface.

1. Firmware modification, upload, and download

2. Access or modification of stored data

3. Ability to upload any data to the server via the device

The USB interface is NOT physically exposed. It can only be accessed by removing a secured back cover plate of the Wavelet enclosure.

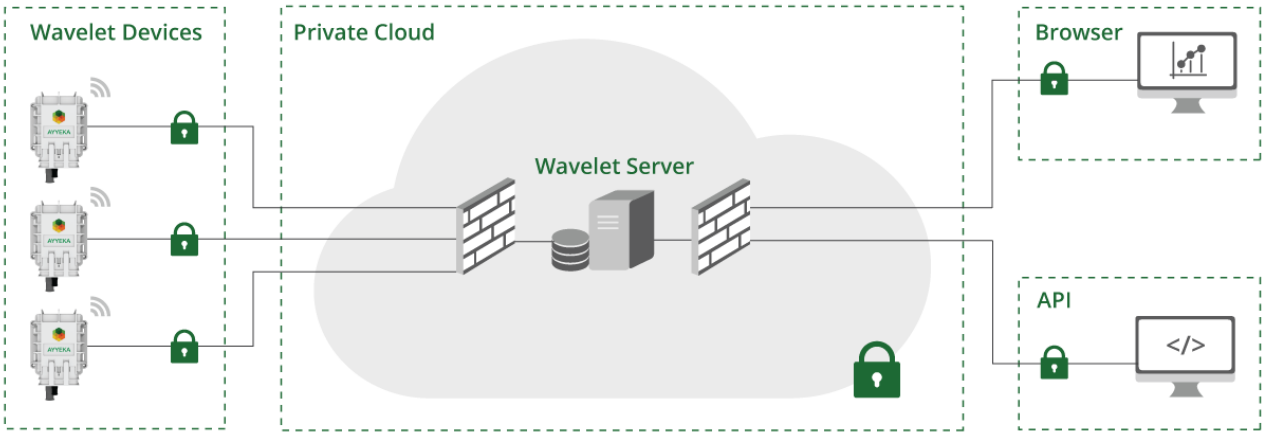
The USB interface has functionality that is limited to the following operations:

1. Provide trace output, which includes real-time information only (not historical information) that is limited in scope to operational and health status (e.g. battery voltage, device internal humidity, cellular signal strength, and health indicators)

2. Sending local Wavelet configuration commands and retrieving device diagnostics through Ayyeka proprietary command language only that is protected from injections, such as changing the device APN, device reboot, and updating serial sensor communication parameters such as baud rate

3. Access to modem AT command interface for cellular troubleshooting

AYYEKA CLOUD HOSTING



Data Packet and Routing Security

Data is transmitted by Wavelets to the Ayyeka Private Cloud services hosted on Amazon Web Services (AWS) in multiple, physically separated and isolated Availability Zones which are connected with low latency, high throughput, and highly redundant networking. All Ayyeka services are built on fully-redundant software stacks monitored and managed by a NOC 24/7/365. The redundant software stacks include the following security components:

- Stateful Packet Inspection (SPI) Firewall, which includes Advanced Threat Protection (ATP) at the L2 and L3 level
- Ayyeka web application server, which authenticates and decrypts message payloads sent by the Wavelets
- All servers have properly signed SSL certificates issued by a trusted certificate authority

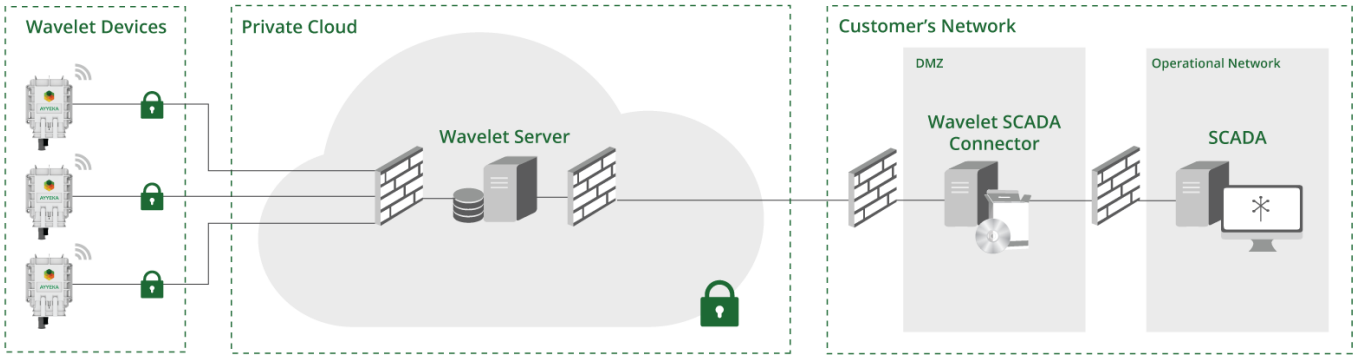
Data Storage Security

Ayyeka utilizes data hosting provided by AWS in secured and redundant facilities. The services used by Ayyeka include:

- S3 for configuration and binary archiving of transmitted payloads
- RDS for fully-scalable and redundant database storage

For further information on S3 and RDS security and retention, please refer to AWS Whitepaper at the following link:
https://docs.aws.amazon.com/aws-technical-content/latest/aws-overview/aws-overview.pdf

API AND AGENTS



Ayyeka employs two industry-standard API methods (REST API and SOAP API) for data retrieval from the Ayyeka Private Cloud. In addition, Ayyeka provides three data retrieval Agents, which include DNP3, OPC-UA, and CSV, which are traditionally used for SCADA integration.

The SOAP API is being deprecated in favor of the more modern REST API implementation.

The REST API utilizes secure 64-bit OAuth 2.0 encoded security tokens, which can be revoked by the user who issues the token. Tokens enable software programs and Ayyeka Agents to use non-transparent application authentication.

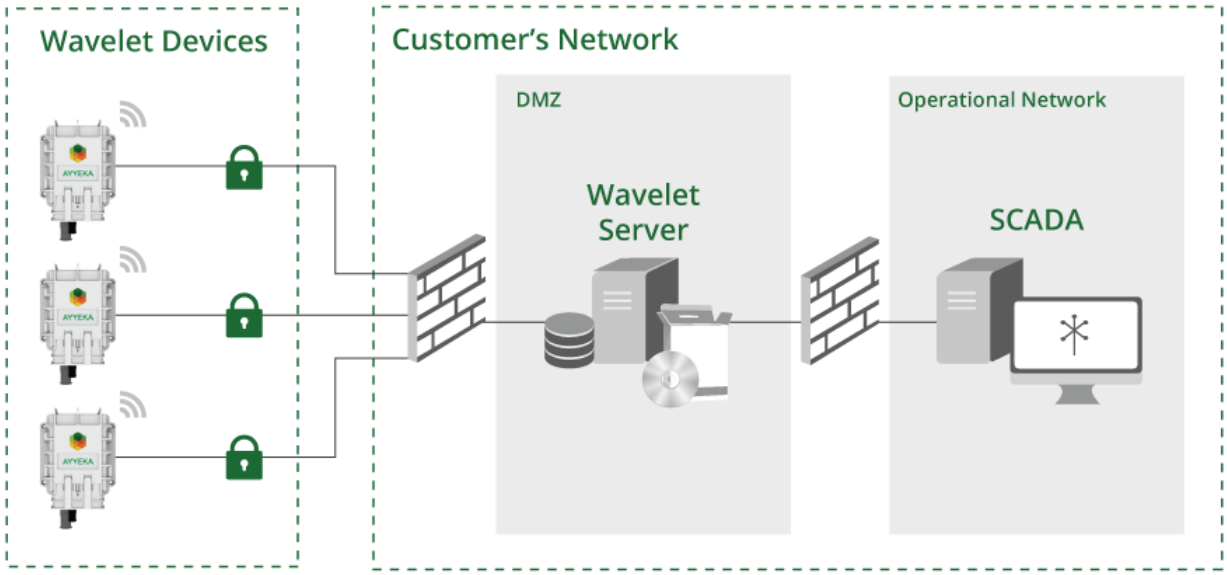
The APIs and Agents pull information via a single, secured HTTPS communication port utilizing TLS 1.2 (SSL) by initiating a session and polling at regular intervals as defined by the API and Agents' configuration scripts. The agents are limited with a maximum polling frequency to prevent an intentional or an unintentional Denial of Service attack. Ayyeka Agents only use a single outbound TCP port over an encrypted connection to a specific host address, which enables simplified firewall administration and monitoring.

In the case of the DNP3 Agent, collected and cached data is pushed unsolicited via DNP3 protocol.

In the case of the OPC-UA Agent, collected and cached data is presented to the services to the local LAN via a local OPC-UA server.

In the case of the CSV Agent, collected and cached data is landed to named files in a designated directory and formatted according to the Agent's configuration files.

ON-PREMISES HOSTING



In the Ayyeka On-Premises offering, customers can opt to host the application side on their own cloud services or local network. In this scenario, no information is stored by Ayyeka and all Wavelets are pointed to servers sitting on an IP address of the customer's choosing. All aforementioned application-level communication security is applicable to the Ayyeka On-Premises offering. It is the responsibility of the customer to provide redundancy and packet-level security for any on-premises deployment.

CONCLUSION

This document is current as of November 19, 2018 and will be updated on an as-needed basis to reflect future enhancements of the Ayyeka cyber-security and communication protocols.

For additional details, please contact:

Simeon Gelband
simeon.gelband@ayyeka.com

Yair Poleg, PhD
yair.poleg@ayyeka.com