Document Status

Document Status

- Document title: Communication and Security Overview
- Author: T. Heijnen
- Version: 2.0
- Date: 14 Jun 2022

Revision History

Table 1 Revision History

Version	Date	By	Reason
1.0	20190201	T. Heijnen	Initial version
2.0	20220614	T. Heijnen	• Textual changes • Document in new corporate identity

Wireless Communication

- SenseAnywhere data loggers wirelessly communicate with a SenseAnywhere AccessPoint using the SenseAnywhere protocol
- 868 / 915 MHz ISM (Industrial, Scientific, Medical) band
- SenseAnywhere Short Message Protocol
- Automatic service discovery
- Encryption of payload
- Easy to install
  - Large wireless range
  - No limitations of number of sensors used
  - Automatic service discovery
  - Seamless roaming
  - No security keys, no pairing
- Easy to maintain
  - No maintenance
  - Lifetime battery (10 years battery life)

Wired Communication

- HTTP communication using port 80
- SenseAnywhere data encrypted as payload using SenseAnywhere's proprietary encryption algorithm
- Most used internet protocol
- Only outgoing traffic on port 80 needed
- No incoming ports need to be opened
- Routes easily through all kind of equipment / internet connections
- Easy to install
  - Only outgoing traffic on port 80 needs to be allowed
  - No incoming ports need to be opened
- Easy to maintain
  - Traffic can be easily monitored as the connection is not encrypted, the payload is.

How it Works

No incoming ports need to be opened
Only outgoing HTTP traffic via port 80
Firewall only need to be reconfigured if outgoing traffic on port 80 is blocked.

Wireless
868/915 MHz ISM band
SenseAnywhere protocol
Encrypted data

Wired 10-base T
HTTP Get protocol
Port 80 outgoing traffic only
Encrypted payload

Wired / Wireless / Cellular
HTTPS protocol
Encrypted connection

Penetration Tested

- Cyber Security Tested by ProCheckUp along IoT Security Foundation framework (https://www.iotsecurityfoundation.org)
  - Hardware testing:
  - Embedded device – Hardware analysis
  - External network, USB and wireless interfaces tests
  - Cellular, Wi-Fi, Bluetooth low energy, Zigbee, Z-Wave and more
  - Internal interfaces, USB, Serial, JTAG SPI
  - Embedded device – Gaining shell access
  - Ethernet Exploitation, Wireless Exploitation, USB exploitation, UART exploitation, I2C/SPI exploitation, JTAG exploitation
  - Embedded device – Firmware analysis, Trying backdooring the firmware
    - From a security perspective firmware is the most critical component of an embedded device. Firmware resides on the non-volatile section of the device, allowing and enabling the device to perform different tasks required for the functioning of the device.
    - Backdooring the firmware is one of the main security issues which devices faces, if it has no secure integrity checks and signature validation.
  - Firmware, software and applications - Auditing the file system and programs in use
    - Operating system audit,
  - User Interface audit – Web and thick client /iOS/Android/API client, Key management, Ownership transfer audit
  - Cloud and support network audit, Data store audit

Penetration Tested (cont'd)

- Cyber Security Tested by ProCheckUp along IoT Security Foundation framework (https://www.iotsecurityfoundation.org)
  - API and application testing:
  - Encryption
  - Server Configuration
  - Session management
  - Authentication
  - Input validation and data sanitisation
  - Authorisation
  - Information leakage

  - No Critical, severe or high risk vulnerabilities found
  - Some medium and low risk vulnerabilities found, most of them mitigated

AccessPoint

- Likely the safest device on your network
  - Does not have 2.4GHz radios so cannot listen to Wi-Fi, Bluetooth communications
  - Does not interfere with 2.4GHz communications
  - The company's switched twisted pair network makes sure that no data is available on the device's port that is not addressed to it. Meaning the AP cannot listen to wired communication going back and forth in your organisation
  - Does not feature a web interface for local configuration to allow settings that you do not want
  - Does not feature an operating system that can be upgraded or replaced. We can upgrade the firmware though.
  - Does not feature installation options for pieces of code (DLLs, apps, plugins)
  - Does not have a USB interface for local management / upgrading

Any other device in your network, like PC's, Notebooks, WiFi AccessPoints, Routers, Servers, Managed switches, Scanners, Printers, Smartphones and Tablets cause a bigger threat to your data and infrastructure

Contact Details

SenseAnywhere B.V.

Bergrand 218
4707 AT Roosendaal
The Netherlands

info@senseanywhere.com

+31 165560088

senseanywhere

@senseanywhere

www.senseanywhere.com

SIMPLY SMARTER

SenseAnywhere