ATLONA
a PANDUIT company

# WAVE™

## Security White Paper

AT-WAVE-101

Atlona Manuals
**Presentation**

# Version Information

| Version | Release Date | Notes |
|---|---|---|
| 1 | Nov 2021 | Initial release |

# Table of Contents

# The Importance of Security in the Enterprise Environment

When an email is sent, or a password is entered on a website, the data is transferred point-to-point through a series of third-party channels, where the data could be intercepted and read, unless the data is encrypted. The same threat can exist within an enterprise LAN with hundreds or thousands of users, where client communications, trade secrets, and other private information is shared: unauthorized users can install packet sniffing software on client devices, compromising the security of both the wired and wireless LAN. In such environments, this is where it is important to implement client-based authentication methods.

The attack surface of any enterprise has expanded significantly in recent years. Typically, organizations would be responsible for securing data in on-premises servers, using state-of-the-art security solutions to protect against cyber-attacks. However, in today's world organizations globally connect with vendors, allowing a distributed workforce on a vast geographical scale. This vastly increases the risk of leaving the corporate environment exposed and vulnerable to malicious intent.

However, vulnerability is not limited to corporate environments and consumers. Many organizations' IT infrastructure is modular and cloud-based. Therefore, private data, company assets, and brand reputation can suffer due to the negative impact of a cybersecurity breach. As a result, many enterprises have implemented large data environments to store collected information that further increase the surface area of a potential cyberattack.

As the landscape of digital environments grows to include more opportunities for data collection, cloud computing, and the Internet of Things (IoT), the potential for security threats also grows. A comprehensive enterprise security strategy is paramount in effective risk management.

In this whitepaper we will cover the security methods Atlona has implemented into the WAVE-101 to maintain a secure system.

# The Atlona Security Testing Process

The Atlona standard practice is to follow the Secure Development Lifecycle: Web-based applications follow the Open Web Application Security Project (OWASP) process. For each standard firmware release, Atlona implements a wide range of industry-standard security assessment tools to ensure all firmware is secure prior to release. The security assessment tools are constantly being updated and current and new firmware is constantly being re-evaluated.

As part of a secure ecosystem, Atlona firmware works to comply with the latest industry security standards, such as the implementation of HTTPS, SSH, 802.1x, secure boot (where applicable), code signing, and strong password policies.

# OS Hardware Security

## Trusted Platform Module (TPM)

Trusted Platform Security (TPM) is an on-board secure microprocessor that performs cryptographic operations. Since the chip is designed for security in mind, it includes several mechanisms which make a tamper-resistant boot environment, even from malicious software attacks. As a matter of fact, the TPM microprocessor's keys are encrypted on the bus and will automatically zeroize if any probing or scanning is performed.

The most common TPM functions are used for system integrity measurements and for key creation and use. During the boot process of a system, the boot code that is loaded can be measured and recorded in the TPM. The integrity measurements can be used as evidence for how a system started and to make sure that a TPM-based key was used only when the correct software was used to boot the system.

## Secure Boot

Secure boot is a security standard that makes sure that when a device boots, the device uses only the software that is trusted by the Original Equipment Manufacturer (OEM). When the PC starts, the firmware checks the signature of each piece of boot software, including UEFI (Unified Extensible Firmware Interface) firmware drivers, EFI applications, and the operating system. If the signatures are valid, the PC boots, and the firmware gives control to the operating system.

The OEM can use instructions from the firmware manufacturer to create Secure boot keys and to store them in the PC firmware.

## Yocto OS Security

Yocto is a customized distribution of the Linux operating system, allowing the manufacturer to select which services are included (or excluded from) with the operating system. This makes it very secure and desirable for embedded systems. For example, some services may contain security exploits causing the OS, itself, to become a security risk. However, any service that might contain a security risk will not reside on the Yocto distribution so the system would not be exposed to the vulnerability.

## Firewalls

firewalls are security systems (hardware or software) that monitor inbound and outbound traffic, based on rules defined by the IT administrator. The operation of a firewall is similar to a router with ACL entries - allowing only specific traffic to pass through. A typical use of a firewall is to provide a barrier between trusted and untrusted networks – for example, the LAN and the Internet. The Atlona AT-WAVE-101 have built-in software-based firewalls between the Wireless and Ethernet interfaces. This allows guests to have access to the features of the WAVE-101 without exposing the corporate network.

## Encrypted Firmware

In a very general sense, firmware is defined as software that is targeted at the hardware-based technology of a computer or embedded system. Examples include the Basic Input-Output System (BIOS), device drivers, and other low-level functionality.

Although no code is 100% secure, measures can be taken to increase the effort required to break or disassemble the code. By using code obfuscation and firmware encryption technologies, images can be “hidden” before pushing to client devices.

Additionally, the firmware must be decrypted with a known trusted key prior to installation. If the firmware has not been properly encrypted, the AT-WAVE-101 will reject the firmware and the upgrade process will fail.

# Security Features

When securing a Wireless Local Area Network (WLAN), a variety of methods are available. However, it is important to implement the most secure features, based on the compatibility between wireless devices.

The Wi-Fi Alliance (http://wi-fi.org) provides the following industry certifications: WPA, WPA2, and WPA3. Although there are different versions, the collective term is WPA.

## Wireless Protected Access (WPA)

Wireless Protected Access (WPA) was designed to replace Wireless Equivalent Piracy (WEP) and is based on the 802.11i standard. The WPA protocol uses the Temporal Key Integrity Protocol (TKIP) which employs a per-packet key. This means that TKIP dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP authentication. Unfortunately, WPA has a security flaw which was exposed and is no longer used and has been replaced by WPA2.

## Wireless Protected Access Version 2 (WPA2)

Wireless Protected Access Version 2 (WPA2) was designed to replace WPA. WPA2 provides additional essential features from the 802.11i standard. In particular, the Counter/CBC-MAC Protocol (CCMP) was implemented, which consists of two algorithms: 1) AES counter mode encryption and 2) Cipher Block Chaining Message Authentication Code (CBC-MAC). This makes CCMP more secure than TKIP. CCMP only functions on devices with the WPA2 designation. All Atlona wireless devices support WPA2.

## Wireless Protected Access Version 3 (WPA3)

Wireless Protected Access Version 3 (WPA3) is the latest iteration and is designed as a future replacement for WPA2. WPA3 was announced in 2018 and leverages a stronger Advanced Encryption Standard (AES) using the Galois/Counter Mode Protocol (GCMP). In addition, WPA3 also uses Protected Management Frames (PMF) to secure 802.11 management frames between access points and clients. This prevents any malicious activity that might spoof or tamper with Basic Service Set (BSS) operation.

## Private Shared Key (PSK)

PSK is a protection mechanism used for Small Office Home Office (SOHO) networks, which usually only include a wireless router and/or modem, which provide an access point, router, switch, and firewall services. All three versions of WPA support PSK. The PSK is typically entered as part of the WLC configuration and entered as a string of 64 hexadecimal digits or as an ASCII passphrase. However, with Atlona devices, the PSK is entered within the built-in web server of the product. Each wireless network device then uses this key to encrypt network traffic, preventing unauthorized users from accessing the WLAN. WPA-PSK is not recommended for WPA-Enterprise networks where an authentication server should be used.

## 802.1X (coming soon)

802.1X is commonly used in WPA-Enterprise environments and provides a challenge, response, and decision algorithm to grant access to the LAN. 802.1X is a server-based port authentication protocol which restricts unauthorized clients from connecting to a Local Area Network (LAN or WLAN) through a public port. In its simplest form, 802.1X usually involves three parties: supplicant (client device), authenticator (Ethernet switch or Wireless Access Point), and an authentication server (usually a RADIUS server). Before the device is permitted to access the network, port communication is restricted to Extensible Authentication Protocol over LAN (EAPOL) traffic. If the device passes the authentication process, then the authentication server notifies the switch, allowing the client to access the LAN.

## Protocol Encryption

### Miracast

Miracast is a wireless casting standard using a Wi-Fi direct connection and relies on a Wi-Fi network using 2.4 GHz and 5 GHz bands and has two modes: 1) Peer-to-Peer (P2P), where the casting device establishes a virtual network connection directly to the receiving device. 2) Infrastructure, where the PC sends wireless traffic to the receiving device using the existing infrastructure network connection. The receiver then decodes the A/V signal and passes it to the output device. Miracast supports WPA2/WPA3-PSK encryption.

### AirPlay

AirPlay is a proprietary wireless protocol developed by Apple Incorporated and allows streaming between audio, video, device screens, and photos, along with any related metadata. AirPlay supports the Advanced Encryption Standard (AES), providing content protection when mirroring or streaming from an iPhone, iPad, or Mac to a display.

### Google Cast

Google Cast is a proprietary protocol developed by Google for playing Internet-streamed audio/video content to consumer devices such as phones, tablets, and other compatible consumer devices, in addition to mirroring desktops. Google Cast uses Transport Layer Security (TLS) inspection, which runs at the Application Layer of the OSI model.

### Instructor and Admin Password Support

The AT-WAVE-101 includes both Instructor and Admin password support. This protects administrative access to the AT-WAVE-101 settings, while permitting end users the ability to use the WAVE-101.

### PIN code support for AirPlay and Miracast P2P/Infrastructure

Atlona wireless devices can be configured to prompt for a PIN code before a BYOD device connects with either AirPlay or Miracast P2P / Infrastructure. When this option is enabled, a PIN code will be displayed on the connected display when an AirPlay or Miracast device attempts to connect to the Atlona device. This ensures that the user is in the correct room and that unauthorized users are unable to share their screen.

# Copyright, Trademark, and Registration