Nest Audio ioXt Security Review

Google

June 4, 2021 – Version 1.0

Prepared for

Ankur Chakraborty
Doug Steedman

Prepared by

NCC Group ioXt Certification Lab

Executive Summary

Overview and Scope

NCC Group was contracted by Google to conduct a security assessment of the Nest Audio device. This assessment was specifically focused on determining whether the device complies with the ioXt Security Pledge.[1] This assessment was performed in May of 2020, spanning 10-person days, and was authorized by Google. The final day of the assessment was postponed until November 2020 to allow for some additional requirements to be tested pertaining to the ioXt Smart Speaker Profile and the publication of the device's security expiration information.

The device being assessed allows a Google account owner to exercise its functionality with the Google Home Android application connected on the same local network and with voice commands. The hardware model numbers and firmware versions within the scope of this test are listed below:

```
"system_build_number": "208279"
"cast_build_revision": "1.47.208279"
Hardware Board ID: G651-04079-04 Rev02
```

At the time of the initial assessment, NCC Group performed the tests associated with the currently defined ioXt Base Profile, and also the then in-draft Smart Speaker Profile that is available to both Google and NCC Group as ioXt members. The final day of the assessment in November allowed for tests against the finalized Smart Speaker Profile.

Limitations

The Smart Speaker profile draft includes a set of tests for a higher, optional security level 3. Some tests at this level were not performed for a few reasons, either because the test was still in draft and not well defined, or NCC Group did not have access to the required information. In the latter case, the most notable examples are the interface between the network and application SoCs, and the proprietary method by which the exposed USB port allows the Synaptics AS370 SoC to boot from an external image.

All assessments performed as part of the ioXt pledge certification program are intended to be time-limited black box audits. These reviews are simply focused on determining the basic security hygiene of the product and the compliance with the eight pledge principles. Therefore, NCC Group performed this shallow review in a limited time-frame, and did not explore deeply any portion of the device. In particular, NCC Group did not review the kernel, or look for remotely-exploitable memory corruption issues in network-listening services. This type of work is best suited for a white-box audit where product source code is available.

Additionally, a number of services and applications were out of scope for the purposes of this assessment. In particular, NCC Group did not assess the back-end Google microservices, interaction with other smart devices, or perform an assessment of the Google Home Android mobile companion applications.

Software updates are performed over a TLS connection with which NCC Group could not tamper to effectively test the signing of software as prescribed in the VS3 test case. NCC Group interpreted this requirement as being met given the TLS connection, but acknowledges that it does not exercise the underlying code-signing scheme. NCC Group learned in the second week of the assessment that a USB port on the device allows it to boot from an external USB-provided image, strictly used for development and RMA, and is still subject to the same boot time signature verification that over-the-air updates are. NCC Group suggests that to apply additional rigor to the VS3 test case and to pass the optional VS5 test case, it would be ideal to attempt to boot tampered binaries loaded via this method, acknowledging that Synaptics' proprietary development tools and documents would be needed.

Key Findings

While the ioXt pledge includes eight principles, many of the base test cases focus on a couple of key technical requirements: the security of all network interfaces, and the implementation of effective software integrity verification. The device is robust in this capacity, as far as NCC Group was able to test. TLS1.2 verifying the server or client (mTLS) as appropriate is broadly used. Software is verified at boot time, anchored by a secure ROM and root public key.

[1] https://www.ioxtalliance.org/the-pledge

The ioXt pledge compliance summaries for the Nest Audio device can be found in the following section of this document.

ioXt Pledge Compliance Summary

This section serves to summarize the device's compliance with the ioXt Smart Speaker Profile[2] version 1.0, which has been defined by the ioXt Alliance.

Principle	Level	Justification
No universal passwords	2 / 2	While the device itself does not require authentication for a user to interact with it physically, Google account credentials are required to remotely interact with the device, and these credentials, along with WLAN connectivity, are required to render the device operable. Note also that Google account authentication can be backed by two-factor authentication. NCC Group determined the requirements associated with this pledge item to be met based on these details.
Secured interfaces	2 / 4	A remote port scan was performed. No ports were directly exposed remotely by design of the device. Security levels 3 and 4 were determined to not be met. The microphone is not optically shielded (SI102), and therefore theoretically vulnerable to lightcommands attacks. It is important to note however that the device does meet most of the test cases required to meet security levels 3 and 4. Aside from those described above, physical interfaces were determined to be disabled (SI3.1). Data persisted to the flash filesystem, including device private keys, is secured by a hardware-backed trusted application and trusted execution environment (SI104). The microphone mute switch and LED indicator are implemented in hardware, protecting them from influence by misbehaving or compromised software (SI108).
Proven cryptography	1 / 1	Google provided a description of the cryptography used for software updates, hardware-backed data storage security, the security of all data transmitted and received, and device provisioning. NCC Group further reviewed the device private key metadata to confirm that they conformed to recognized standards.
Signed software updates	3 / 3	Google provided detail on the method by which software updates are received and verified, including detail pertaining the Secure Boot functionality of the bootloader, using appropriate cryptographic verification at boot time, chained to a root public-key hash burned into one-time programmable storage. NCC Group was unable to intercept and modify an update due to the TLS-secured channel by which the device receives updates, but in review of the documentation and observation of the live update, NCC Group determined these requirements to be met.
Automatically applied updates	2 / 2	Google provided a security maintenance plan, indicated that updates were applied to connected devices regularly and automatically, notifying the end user. NCC Group observed one such update.
Vulnerability reporting program	1 / 1	Google described the vulnerability reporting program applicable to this and many other devices.[3] NCC Group has confirmed that this program meets the ioXt requirements, including ISO29147[4] compliance.

[2] https://www.ioxtalliance.org/s/ioXt_Smart_Speaker_Profile.pdf
[3] https://www.google.com/about/appsecurity/reward-program/
[4] https://www.iso.org/standard/72311.html

Principle	Level	Justification
Security expiration date	1 / 1	Google shared internal documentation regarding the EOL support of various devices including this one, meeting the requirements of this pledge item. Google indicated that this information will be publicly available at https://support.google.com/product-documentation/answer/10231940 by July 30, 2021.
Security by default	2 / 2	The requirements in this pledge item pertain to the implementation of factory reset and voice recognition. Upon performing a factory reset, network and account credentials were removed from the device. Google further described this functionality in documentation. A subset of voice commands pertaining to users' private data such as calendar and contact information was found to be inaccessible by an unrecognized (computer-generated) voice.

This section describes the criteria used by NCC Group when testing a product for alignment with the ioXt Security Pledge. While many of the questions posed below are answered manually by reviewing and testing the product, in the interest of time, some may be answered based on the *ioXt Pledge Questionnaire* that the OEM fills out to provide NCC Group with a detailed technical understanding of the product and its security controls.

The set of tests that were explicitly performed are detailed in the ioXt Test Case Library.[5] This summary provides a broader perspective of the considerations that NCC Group reviewed in alignment with the overall ioXt pledge.

The ioXt Security Pledge is composed of eight clear principles:

1 No universal passwords

The pledge states:

> *The product shall not have a universal password; unique security credentials will be required for operation.*

In order to test this best-practice, NCC Group has reviewed the following aspects of the device:

- All device passwords are unique at the earliest opportunity (out-of-box experience or manufacturing) and not resettable to any universal default value.
- The minimum strength and verification method of the password render brute force attacks difficult even at scale.
- The device does not use any hard-coded credentials or identity.

With respect to any methods by which the device authenticates to remote endpoints and functionality, NCC Group further reviewed the following:

- Establish the set of identifiers that uniquely identify a device and consider the use and sensitivity of each.
- Establish that each device must prove its unique identity and authenticate to exercise any remote functionality using a proven secure mechanism.

2 Secured interfaces

The pledge states:

> *All product interfaces shall be appropriately secured by the manufacturer.*

In order to test this best-practice, NCC Group has reviewed the following aspects of the device:

- JTAG/SWD and debug interfaces are disabled on release products.
- All sensitive interfaces, including device-internal interfaces, are encrypted and authenticated.
- Authorization is performed for any privileged access to device functionality.
- Sufficient input validation is performed on all external interfaces.

3 Proven cryptography

The pledge states:

> *Product security shall use strong, proven, updatable cryptography using open, peer-reviewed methods and algorithms.*

In order to test this best-practice, NCC Group has reviewed the following aspects of the device:

- Establish where the product uses cryptography.
- Establish that wherever cryptography is used, it is considered standard and best-practice.
- Establish that wherever TLS is used, it is version 1.2 or greater.

4 Security by default

The pledge states:

[5] https://ioxtalliancemembers.org/wg/Compliance_wg/document/134

> *Product security shall be appropriately enabled by default by the manufacturer.*

In order to test this best-practice, NCC Group has reviewed the following aspects of the device:

- There are no RMA/debug modes enabled in release firmware.
- There are appropriately implemented privacy modes/buttons.
- There is no means to trivially bypass user authentication.
- All device keys are managed securely.
- There are no unnecessary network-facing services, and those that are necessary restrict access accordingly.
- The manufacturer provides consumers with clear and transparent information about how their personal data is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers. The manufacturer
- Where personal data is processed on the basis of consumers' consent, this consent is obtained in a valid way, and that consent is revocable by the consumers at any time, allowing the consumers to permanently delete all previously collected data and prevent future collection.
- Logging on the device does not expose personal private information of the user.

5 Signed software updates

The pledge states:

> *The product shall only support signed software updates.*

In order to test this best-practice, NCC Group has reviewed the following aspects of the device:

- Firmware updates are downloaded over TLS, and the certificate of the firmware host that the device verifies should be pinned.
- The firmware images are encrypted until installation.
- The firmware images are signed, and they are verified on the device prior to installation.
- The device supports secure boot.
- The device supports downgrade prevention.

6 Automatically applied updates

The pledge states:

> *The manufacturer shall act quickly to apply timely security updates.*

In order to test this best-practice, NCC Group has reviewed the following aspects of the manufacturer:

- The device supports a secure firmware over-the-air update mechanism.
- The manufacturer is able to distribute firmware updates remotely using this mechanism.
- The consumer can be informed in a timely manner that an update is required or available. The urgency of each update is communicated to the consumer.
- Where possible, the device will continue to provide a basic level of functionality during an update.
- The manufacturer maintains awareness of both internally developed and externally sourced firmware running on the device and is responsive in distributing updates to both in the presence of a discovered vulnerability.

7 Vulnerability reporting program

The pledge states:

> *The manufacturer shall implement a vulnerability reporting program, which will be addressed in a timely manner.*

In order to test this best-practice, NCC Group engaged the manufacturer to answer the following questions:

- Have you ever had to deal with an external security vulnerability report?

- Have you defined patching criteria which guarantee that vulnerabilities must be patched within a reasonable time frame from initial disclosure?
- When a security update is published, how are vulnerability details disclosed publicly to stakeholders including customers?

Furthermore, NCC Group has reviewed the following aspects of the manufacturer:

- Security contact information and vulnerability reporting guidelines are published on the manufacturer's website.
- The contact information is easily discoverable.
- Any documentation provided by the company related to the their vulnerability disclosure program and its parameters.
- The company participates in a bug bounty program, and the details thereof.

8 Security expiration date

The pledge states:

> *The manufacturer shall be transparent about the period of time that security updates will be provided.*

In order to test this best-practice, NCC Group engaged the manufacturer to answer the following questions:

- After the product is released, what is the earliest possible date that it will no longer be supported via security patches before *End Of Life*?
- How is this information communicated to stakeholders including customers?