Updates to Device Security Requirements for Alexa Built-in Products

Amit Agrawal Jan 30, 2020

Alexa Built-in SDK Device Makers AVS Device SDK

Patrick McCanna also contributed to this article.

With the Alexa Voice Service (AVS), device makers can build Alexa Built-in products including smart speakers, smart TVs, hearables, and more. As the Alexa Built-in product selection grows and customers spend more time interacting with Alexa, we continue to look for opportunities to help device makers enhance security of their devices. Today, we released updated minimum security requirements for new AVS devices. You must have at least one AVS product created in the console to access this page. The list consolidates requirements for devices based on any of the available AVS SDKs, including the Alexa Smart Screen SDK and Alexa Auto SDK, to help device makers understand what steps they can take to improve the security of their products. The first set of requirements will go into effect August 1, 2020, and the next set will go into effect on August 1, 2021.

Overview of the Security Requirements

Hardware, Software, and Device Security Requirements

Securing devices requires a multifaceted approach in every step of the development process from product initiation to launch. Even after launch, device makers must release security fixes when the need arises. Required capabilities include:

- **Secure Boot** can be used to reduce the risk that a hacker can tamper with and gain a persistent foothold on their device.
- **Secure Key Storage** can be used to limit the exposure of authentication tokens and sensitive operations for attackers who've gained temporary access to a device.
- **Hardware-Based Cryptographic Engines** can be used to reduce the risk of an attacker disrupting

- **Up-to-Date and Operating Systems with Long-Term Support (LTS)** can reduce the risk of an attacker using old platform exploits to compromise a device.
- **Host Hardening** can constrain the capabilities of an attacker targeting a device. You can consider using solutions like SELinux or AppArmor to reduce the blast radius of a successful compromise.
- **Separation of Account Privileges** can reduce the risk of a successful exploit of a service or process leading to catastrophic compromise of the device.
- **Threat Surface Reduction (e.g. removing unnecessary network services)** can help simplify the hardening process and reduce the risk of an unneeded service being used to exploit a device.

Company Processes

Connected devices rely on complex embedded operating systems and multiple layers of application software. Any time you add new features to an existing fleet of devices, you risk introducing new vulnerabilities to the device. Therefore, it is important that you develop a mature software maintenance strategy where you periodically patch vulnerabilities in software on your devices.

Start by evaluating potential threat scenarios by performing threat modeling for all features and use cases for your device. Your software development life cycle must include checks to evaluate if adequate authorization, authentication, and input sanitization mechanisms are being implemented for high-risk operations. Pick secure hardware and software components that are actively maintained and supported by your suppliers. Lastly, make sure to invest in the vulnerability discovery and management, bug bounty, and incident response mechanisms.

Independent Security Assessments

It is important to have both the right security expert within your company to establish secure design practices and an independent expert who can perform regular security assessments on production devices. We require device makers to submit a security assessment report before launch and every time there is a major change in the device software/firmware that triggers re-certification of your device. To help you with this, we have authorized security laboratories across the globe to assist and provide independent security assessments. You can reach out to the following security labs to get an assessment: Bishop Fox, NCC Group, Onward Security, Dekra, and Underwriters Laboratories.

Review the Security Requirements for your New Devices

We encourage you to review the updated security requirements on the developer portal. If you need to get in touch with any of the above laboratories or have any questions about security requirements for designing devices with Alexa Built-in, you can reach out to avs-security@amazon.com.

Back to Top