Security Overview

Table of Contents

System Security

The Roku Streaming Player is designed to play a variety of streaming content directly from the Internet. We understand that this content is valuable to the content owners and must be protected from unauthorized access to prevent both casual and professional copying and distribution. Multiple types of security provisions are available if needed.

The system has been designed to be hardened against unauthorized attack. This process starts at the Roku factory as each system is individualized and uniquely keyed as a foundation for robust security. The platform supports a secure key store and hardware encryption engine. The core set of system software has been encrypted and is protected by a secure boot process and the use of signed binaries.

SSL is the primary method provided for developers to implement content and/or communications security for their application. The device supports both client and server authentication via SSL to provide a secure communications channel between trusted end-points.

Application Security

Applications which run on the player must be encrypted and signed using the developer's unique developer specific set of keys generated by the Roku Streaming Player in developer mode. Code signing is done automatically as part of generating a package and ensures the integrity of code. Application packages are also encrypted to ensure confidentiality of the source code. Packaging tools are available on the Developer web page of Roku Streaming Players. By default, the Developer page is not enabled. You must enter the remote code **Home 3x, Up 2x, Right, Left, Right, Left, Right** to enable it. A walkthrough of the packaging process is detailed later in this document.

The packaging process is designed to be lightweight and focuses on ensuring that an application originates from a known source and is protected against tampering. It is the responsibility of the developer to ensure that the application is properly tested, high quality, and provides a good user experience.

Protected Environment

BrightScript applications are run within a unique context in the BrightScript Virtual Machine. Applications are "sand-boxed" and run protected from other areas of the system. Scripts have limited access to platform resources and can only access functionality specifically exposed through the scripting layer as BrightScript components. This ensures the overall integrity of the platform and prevents unauthorized access to the operating system or any third party content. Applications are restricted from interacting with other applications on the system or accessing their private data. Applications store their data separately and securely in a unique area of the system registry. Suites of applications can share registry data by creating each application's package with the same developer ID keys.