Hardware Analysis of the Amazon Fire TV Stick

Nasser and Melanie

UAT

NTW233: IoT Architecture and Security Course

Mr. Becote

08-18-2024

Overview

Visual Inspection

- External Ports: By viewing various images and disassembly's online, the Amazon Fire TV Stick includes an HDMI connector for connecting to a TV and a micro-USB port for power. It does not have any exposed USB, UART, JTAG, or other debug interfaces that could be used for unauthorized access or debugging.
- Exposed Test Points or Headers: There are no exposed test points or headers on the exterior of the device that would allow access to sensitive data or functionality without disassembly.
- Physically Accessible Storage Media: The device does not contain any slots for SD cards or removable flash memory, reducing the risk of physical data extraction.

Image source: https://www.pcmag.com/reviews/amazon-fire-tv-stick-lite

Disassembly

- Tamper-Evident Seals: When disassembling the Fire TV Stick, you won't encounter tamper-evident seals or stickers, however the box that it comes in does, which can indicate attempts to sabotage the device.
- Main Components: As we can see from the image below, inside the device, you will find components such as the processor, memory chips, and wireless modules. These components are crucial for the device's operation, and their make and model can be identified upon disassembly.

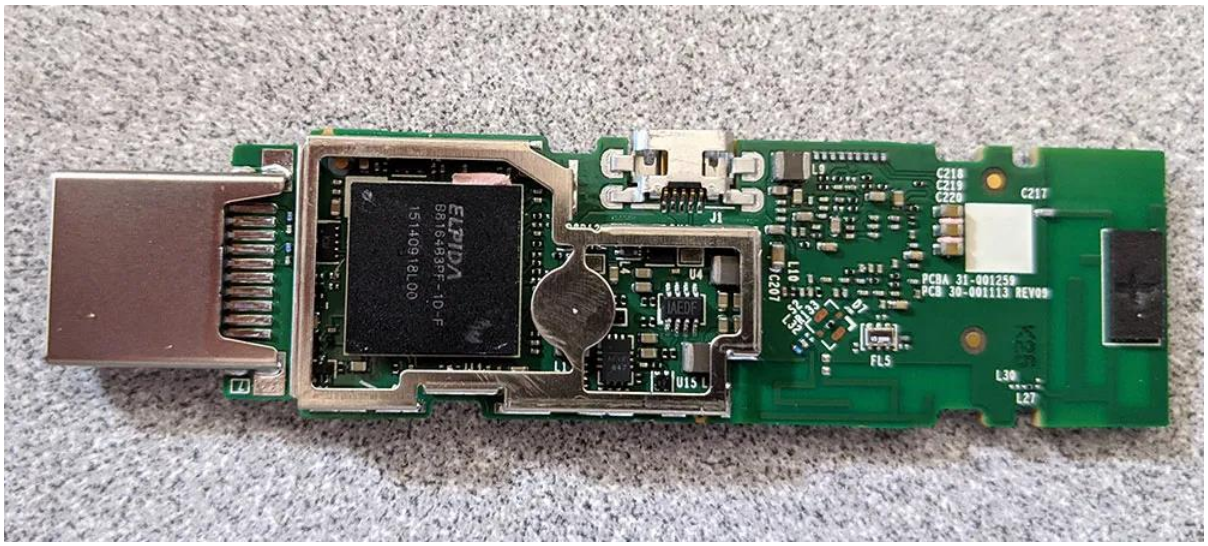

Image source: https://www.edn.com/teardown-what-makes-the-amazon-fire-tv-stick-tick/#comments

Hardware Interfaces

- Exposed Interfaces: As seen from the image below that shows a complete teardown, Internally, the Fire TV Stick contains interfaces like UART or SPI, but these are not accessible without disassembly. The JTAG interface, when present, is also internal.
- Firmware Update Mechanisms: Firmware updates are managed through the device's software interface, with security measures such as digital signatures and encryption in place to prevent unauthorized updates.
- Risks Associated with Interfaces: If accessible, internal interfaces could potentially be used to extract firmware, modify configurations, or bypass security controls. However, the device employs secure boot processes and encrypted firmware to mitigate these risks.

Image source: https://www.edn.com/teardown-what-makes-the-amazon-fire-tv-stick-tick/#comments

Executive Summary

The Amazon Fire TV Stick is a secure IoT device designed for seamless streaming of media content while prioritizing user security. A visual inspection reveals that it features an HDMI connector and a micro-USB port for power, with no exposed debug interfaces such as USB, UART, or JTAG. Additionally, the absence of slots for SD cards or removable flash memory significantly reduces the risk of physical data extraction, making unauthorized access more challenging.

Upon disassembly, the device may exhibit tamper-evident seals, indicating attempts to access its internals. Inside, key components such as the processor, memory chips, and wireless modules are present, which are essential for its functionality. The Fire TV Stick employs secure firmware update mechanisms, including digital signatures and encryption, to safeguard against unauthorized modifications. Overall, the device's design effectively mitigates potential risks associated with internal interfaces, ensuring that user data remains protected and secure against tampering and unauthorized

Wireless Communications

For wireless connections we will be discussing the wireless interfaces within the device which mostly consists of Bluetooth and Wi-Fi, the security of the wireless communications and the device's behavior to common wireless attacks.

When opening and looking at the hardware of the device you will find a PCB-embedded Bluetooth and Wi-Fi antenna structure that turns out to be Cypress Semiconductors (which used to be Broadcom's BCM43242) which deals with all the dual-band Wi-Fi and Bluetooth duties (Dipert, 2020).

Bluetooth is one of the major wireless interfaces on the device. Features like Bluetooth Low Energy (BLE), Bluetooth Baseband Core (BBC) which is a high-performance operation that manages the buffering, routing of data for connections, segmentation, etc (Cypress Semiconductor Corporation, 2018).

When it comes to the devices behavior to replay attacks some actions that are put into action are using timestamps or nonces in each transmission and session-specific tokens that are invalid after each use. These actions help keep the device secure allowing no unauthorized actions or access to be granted (OpenAI, 2024).

MitM attacks results in the device to behave in a way that use mutual authentication, certificate validation for devices using PKI, and encryption integrity checks to result in a secure device that i able to detect inconsistencies or incomplete a secure connection to avoid an MitM attack (OpenAI, 2024).

Lastly for unauthorized pairing attempts the device will behave in a way to require a pin by using NFC or confirm a code displayed on both devices, this leaves unauthorized pairing

attempts to be blocked if the correct information is provided. User Conformation is another way to confirm an authorized user by having the user press a button before pairing. Some devices will also store data of previously paired devices and ignore pairing requests from any unknown or unauthorized devices (OpenAI, 2024).

Hardware Security Features

In this section I will be listing the hardware features in the device, how they are utilized and if they are properly working and maintained.

The hardware includes a security engine accelerator that decreases the time to perform typical security operations such as the ones listed below, significantly:

- PKA cryptography
- AES-CTR/CBC-MAC/CCM acceleration
- SHA2 message hash and HMAC acceleration
- RSA encryption and decryption
- Elliptic curve Diffe-Hellan in prime field
- Generic math functions
    - (Cypress Semiconductor Corporation, 2018)

PKA cryptography is used within the device to secure connections and authenticate devices and plays an important role in initial pairing and ongoing communication and ensuring only authorized devices can communicate.

CCM is an authenticate-and-encrypt block cipher mode that is defined with 128-bit block ciphers such as AES. Therefore AES-CTR/CBC-MAC/CCM Acceleration is a combination of authentication, encryption, and restrictions all working together to encrypt and send data to an authenticated device (Housley et al., n.d.). This prevents replay attacks, eavesdropping, and tampering all while impacting on the battery life with little use.

SHA2 message hash is used to generate cryptographic hashes to ensure data and integrity and to verify the integrity of commands sent from the remote. HMAC acceleration is used to verify messages between the remote and Firestick, ensuring that they have not been altered by an attacker. Both features are always conducting checks and are performed quickly (OpenAI,2024).

RSA encryption and decryption would be used for key exchange during pairing process for secure updates without exposing the keys to any potential attackers. RSA is well established method for secure communications and is used throughout many devices. It provides a high level of security especially when it comes to key exchanges.

Elliptic Curve Diffe-Hellman (ECDH) is an agreement protocol that allows two parties who both have an elliptic-curve public and private key pair to establish a shared secret over an insecure channel which can be used as a key or to retrieve another key. It can then be used to encrypt commnications using a symmetric-key cipher (Wikipedia contributors, 2024). Related to the device it allows the remote and the Firestick to agree without exposing the key to potential eavesdroppers. Using this method allows a strong security while also using small key sizes which is best suited for the device.

All these security features ensure secure paring, data integrity, and encrypted and properly configured communications which is a big part of the security pillars when everything is maintained.

Mitigation and Recommendations

In this section we will be identifying potential threats and weaknesses in the device, strategies to mitigate issues and recommendations for updates secure configuration and best practices.

When it comes to hardware some threats can include:

- physical tampering
- modifications that are malicious to the hardware
- side-channel attacks.

When threat modeling is applied there are a couple things to identify for our IoT device. Identifying and ways that the Fire Stick Lite can be tampered with physically can include assets like ports, connectors, or micro-controller.

Some threats can include anyone who has unauthorized access by being able to physically tamper with it, insert malicious hardware components, and exploitation of side-channeling.

To prevent this from happening to our device it is crucial that we follow recommended intended protections such as using an updated TLS protocol version, using an Amazon account with 2-step verification, having strong passwords that are not reused anywhere else especially when it comes to Wi-Fi connections, and adjusting the default settings. This can also include using a remote case that can show if it has been tampered with, using a secure location to keep it physically safe, implement hardware encryption, and disabling unused ports. All these steps can help prevent an attacker while also keeping our information safe while analyzing the device.

Lastly for firmware updates, some potential threats can be:

- Malicious firmware
- Update hijacking
- Integrity attacks

The assets this involves would be the firmware running on the Fire Stick Lite, which would be the Fire OS 7. The entry points to this can be through update servers and firmware update mechanisms.

The threats that can expose this would be related to malicious firmware being distributed, integrity attacks on firmware updates, and the hijacking of update processes. To counteract these, you can do signed hardware which allows a secure firmware update mechanism, verifying update integrity, and restricting firmware updates with trusted sources only.

References

- *Device Specifications: Fire TV Streaming Media Player | Amazon Fire TV*. (n.d.). https://developer.amazon.com/docs/fire-tv/device-specifications-fire-tv-streaming-media-player.html?v=ftvsticklite
- *Safety and Compliance Information*. (n.d.). amazon.com. Retrieved August 15, 2024, from https://www.amazon.com/gp/help/customer/display.html?nodeId=GW67H2WCNMB5K475
- *Can an Amazon Fire Stick be Hacked? | Black Hat Ethical Hacking*. (2024, March 19). Black Hat Ethical Hacking. https://www.blackhatethicalhacking.com/articles/can-an-amazon-fire-stick-be-hacked/
- *Amazon Fire TV Quick Start Guides and User Manuals*. (n.d.). amazon.com. Retrieved August 15, 2024, from https://www.amazon.com/gp/help/customer/display.html?nodeId=201348270
- Cypress Semiconductor Corporation. (2018). CYW20735B1 Single-Chip Bluetooth Transceiver for Wireless Input Devices. In *Cypress* (Dataset No. 002-14881 Rev. *I; Version 002-14881 Rev. *I). https://www.mouser.com/datasheet/2/100/002-14881_CYW20735B1_Single-Chip_Bluetooth_Transce-961637.pdf
- Dipert, B. D. (2020, May 11). *Teardown: What makes the Amazon Fire TV Stick tick?* EDN. https://www.edn.com/teardown-what-makes-the-amazon-fire-tv-stick-tick/#comments

- Housley, R. H., Whiting, D. W., Housley, R. H., & Ferguson, N. F. (n.d.). Counter with CBC-MAC (CCM) AES Mode of Operation. In *NIST*. Retrieved August 16, 2024, from https://csrc.nist.rip/groups/ST/toolkit/BCM/documents/proposedmodes/ccm/ccm.pdf
- Som Tips. (2021, February 13). *Amazon Fire TV Stick Lite Teardown 🔥 Disassemble of Fire Stick Lite & Alexa Remote Lite ✅ | Som tips* [Video]. YouTube. https://www.youtube.com/watch?v=m76Uxtt4K-0
- Wikipedia contributors. (2024, May 27). *Elliptic-Curve Diffie–Hellman*. Wikipedia. https://en.wikipedia.org/wiki/Elliptic-curve_Diffie%E2%80%93Hellman
- Greenwald, W. (2024, July 3). *Amazon Fire TV Stick Lite Review*. Pcmag. Retrieved August 17, 2024, from https://www.pcmag.com/reviews/amazon-fire-tv-stick-lite

For additional information on APA Style formatting, please consult the APA Style Manual, 7th Edition.