SUIT Working Group
Internet-Draft
Intended status: Standards Track
Expires: May 1, 2021

J. Lee
Sejong University
J. Park
ETRI

October 28, 2020

Distributed SUIT Architecture Model
draft-lee-suit-distarch-00

Abstract

The management of data is entirely centralized on servers in a server client model which leads the servers to be high-value targets for adversaries. Also, firmware consumers fail to download the latest firmware image if the author is disappeared in the server client model. The distribution of network for managing the manifest and firmware image files thus required. This draft introduces a distributed SUIT architecture model, which utilizes blockchains to resolve the issues of the server client model for SUIT.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL","SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 1, 2021.

Table of Contents

1. Introduction

In the existing SUIT architecture, firmware images and manifest files are stored in the firmware servers, which deploy the firmware images based on the traditional server-client model. However, in the server-client model, servers may endure excessive network traffic and overload because of the centralized architecture. As the number of IoT devices is rapidly increasing, the servers will be overwhelming to handle the requests from the IoT devices all around the world. Also, a server is a high-value target for adversaries since the server takes charge of data management.

In the server-client model, the firmware consumers are unable to download the latest firmware image if the authors disappeared. In this draft, we propose a distributed firmware update architecture by applying blockchain to the existing SUIT architecture. The proposed distributed SUIT architecture decentralizes the requests from the IoT devices, prevents targeting attacks, and provides sustainable updates even after an author disappears.

2. Motivations

The existing SUIT update architecture is as follows:

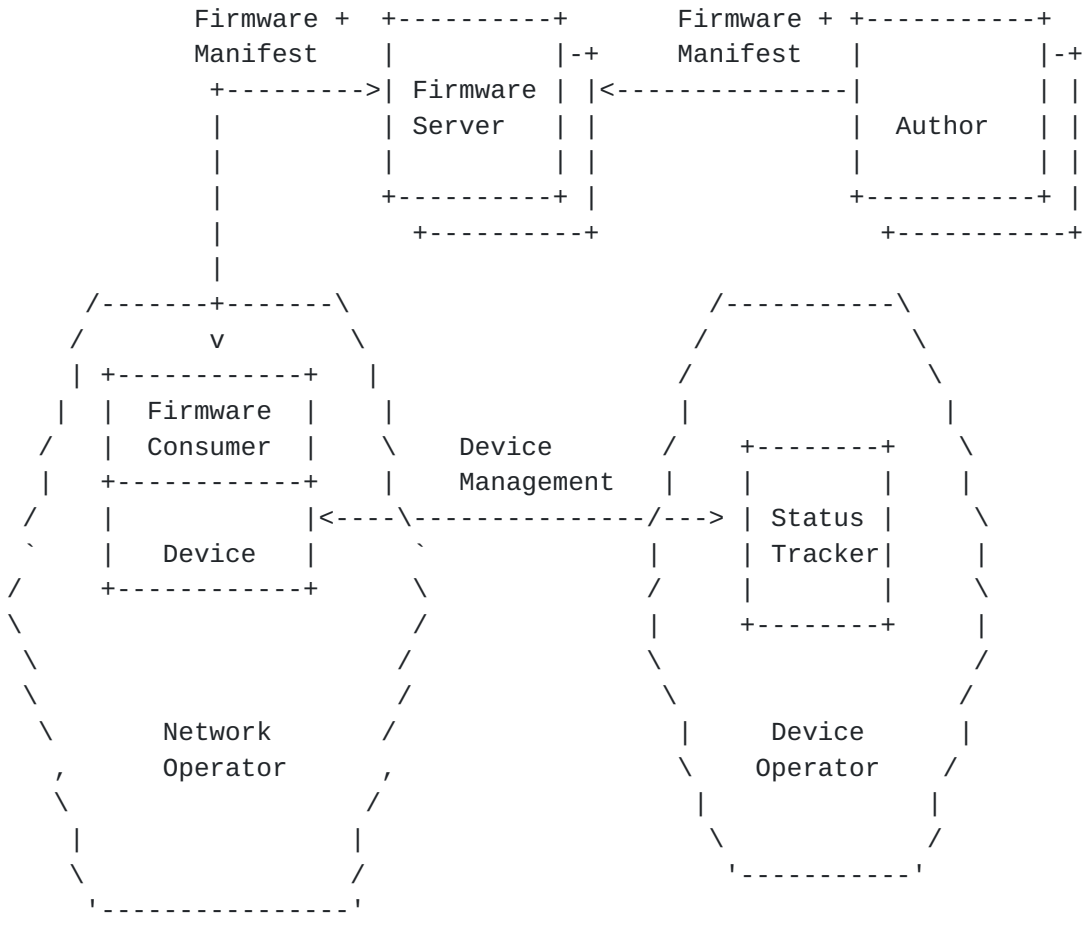

Figure 1: Existing SUIT Architecture

The existing SUIT architecture can cause failures and targeting attacks due to the centralized server-client model.

The author's continued service offer is not guaranteed. The company and its servers may disappear due to an attacker's cyber-attack or funding problems. In the worst case, all author nodes managed by the author may not function properly. At this point, devices that have not been updated with the latest firmware before the author disappears can no longer update the firmware. The existing SUIT architecture cannot solve author disappearing issues.

If the firmware update does not complete properly, the client may not be able to use the newly provided service or the security patch and be exposed to the cyber-attack easily.

3. Distributed SUIT Architecture

In the firmware update architecture based on server-client model, the firmware consumers request the firmware server to download the latest version of the firmware. However, the traditional server-client method adopted in the existing SUIT architecture can cause several problems in network traffic, data security and firmware update persistence.

In the server-client model, data is dependently managed by the server in a centralized structure. Since many clients request one server, this centralized structure causes excessive overhead when excessive network traffic occurs and may cause a situation in which requests are not properly processed. In addition, when an attacker attacks a server, it is impossible to use all data managed by the server, so an attack targeting the server may occur.

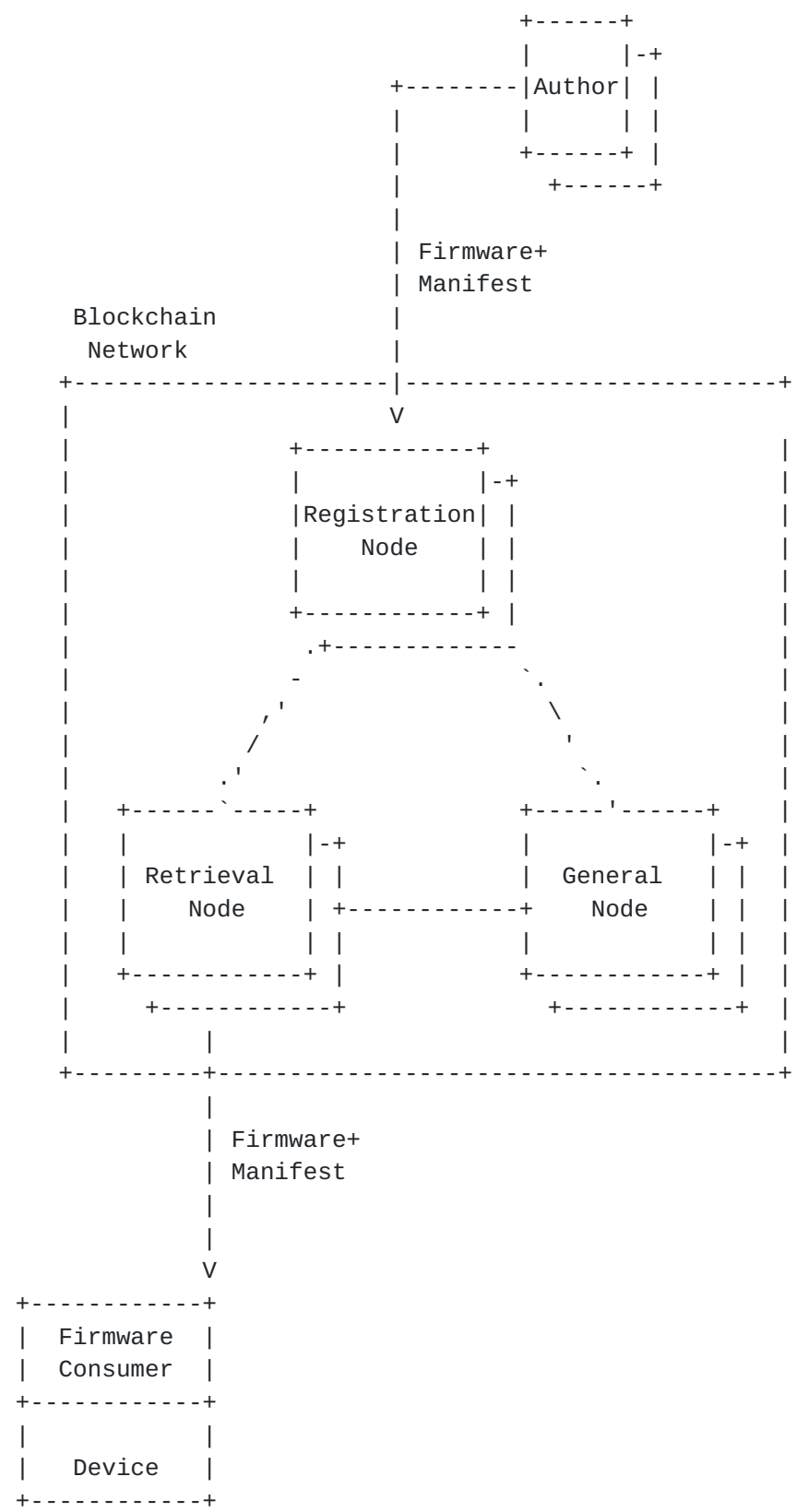

Figure 2: Distributed SUIT Architecture

As shown in Figure 2, the authors upload the manifest files and firmware images to the blockchain network in the proposed firmware update architecture. The IoT devices download the manifest files and firmware images through the blockchain network. When an IoT device requests upload, the retrieval nodes retrieve the firmware images that were stored as chunks in a distributed file system and deliver the manifest file and firmware image after the device verified.

4. Example Procedure

TBA.

5. Conclusion

TBA.

6. Security Considerations

TBA.

7. IANA Considerations

This document presents no IANA considerations.

8. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

Authors' Addresses

Jong-Hyouk Lee
Sejong University
209, Neungdong-ro, Gwangjin-gu
Seoul 05006
Republic of Korea

EMail: jonghyouk@sejong.ac.kr

Jungsoo Park
ETRI
218, Gajeong-ro, Yuseong-gu
Deajeon 34129
Republic of Korea

EMail: pjs@etri.re.kr