        Solution Requirements - Secure Firmware Upgrade (SecFU)
              draft-nandakumar-suit-secfu-requirements-00

Abstract

   The IETF SUIT effort has been forming to define a secure firmware
   upgrade solution for Internet of Things (IOT). Recent
   vulnerabilities and the need to upgrade firmware on the IoT devices
   for security updates in a standardized, secure, and automated fashion
   has been the driving force behind this work.

   This specification is a requirements document to aid in developing a
   solution for Secure Firmware upgrade of the IoT devices.

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 http://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 3, 2018.

Table of Contents

1. Introduction

This draft outlines a set of requirements around firmware download
for IoT devices. A sketch of a proposed solution can be found in .

2. Solution Requirements

Informally, a secure firmware upgrade solution might need to address
following components:

o Secure firmware description container format, in the form of
   Manifest

o Locating a server to download the firmware from

o Downloading the manifest and the firmware image(s)

o Cryptographic validation of the manifest and signed code images

o Complete the installation

Given above tasks, this specification breaks down the secure firmware
upgrade solution into following requirements:

1. Solution must allow devices that delete the old firmware before
    installing the new firmware. Thus implying a solution that can
    easily be implementable on a minimal boot-loader

2. Solution must enable devices that have enough memory to have the
    new firmware image of the firmware simultaneously loaded with
    the existing image.

3. The manifest format should be self describing.

   4.   Allow a given device to decide which manifest format is
        appropriate for it choosing from JSON, CBOR, or perhaps ASN.1 if
        there is a a device vendor that plans to use this

   5.   Manifest must allow metadata about the firmware sourced by a
        single manufacturer

   6.   Optionally, the solution may allow the manifest to describe
        metadata about firmwares from different providers

   7.   The solution should enable firmware that is delivered as a
        single image

   8.   Optionally, the solution may enable firmware to be split into
        multiple images.

   9.   The charter should recommend a solution agnostic to the format
        of the firmware image and inter dependencies. Dependency
        management is complicated and is by nature proprietary and
        should not be in the initial scope.

   10. The proposed solution must provide mechanism to discover where
        to download the firmware where that mechanism includes the
        ability for a local cache.

   11. The proposed solution should allow flexibility to choose the
        underlying transport protocol as defined by the deployment
        scenarios. The WG should define a MTI set of protocols that
        firmware servers need to implement and clients can choose which
        one to use

   12. The proposed solution must require a device to validate
        signatures on the manifest and firmware image(s)

   13. Optionally, the solution might want to support encrypted
        manifest and firmware

   14. The proposed solution should enable crypto agility and prevent
        roll-back attacks.

   15. Solution should allow for secure transition between the
        generations of the keying material

   16. Charter should not invent new crypto or transports and use
        existing techniques

[3]. IANA Consideration

   Not Applicable

[4]. Security Considerations

   Not Applicable

[5]. Acknowledgements

   Thanks IOTSU workshop.

Authors' Addresses

   Suhas Nandakumar
   Cisco

   Email: snandaku@cisco.com

   Cullen Jennings
   Cisco

   Email: fluffy@iii.ca

   Shaun Cooley
   Cisco

   Email: scooley@cisco.com