

Securing Software Updates for IoT Devices with TUF and Uptane

Ricardo Salveti ricardo@foundries.io
Principal Engineer



Foundries.io

Foundries.io

- Established October, 2017
 - Spin-out from, and funded by, Linaro Ltd.
 - Team formerly known as Linaro Technologies Division
- Backgrounds in
 - Embedded Systems, (Linux, RTOS, PC BIOS, Windows, Android)
 - Linux Distributions
 - Consumer, Commercial, Military, Commercial Aviation Product Development
 - Web Frameworks
 - Advanced CI (LAVA, [KernelCI.org](https://kernelci.org))
- Offers secure, over-the-air updatable software platforms for connected products
 - Linux microPlatform
 - Zephyr microPlatform

Why are updates
critical for IoT?

Mirai botnet adds three new attacks to target IoT devices

This new version of the botnet uses exploits instead of brute force attacks to gain control of unpatched devices.



By [Danny Palmer](#) | May 18, 2018 -- 13:29 GMT (06:29 PDT) | Topic: [Security](#)

Someone is Using Mirai Botnet to Shut Down Internet for an Entire Country

 November 03, 2016  Swati Khandelwal

Hajime Botnet Makes a Comeback With Massive Scan for MikroTik Routers

By [Catalin Cimpanu](#)



March 28, 2018



05:02 AM



0

Need for Updates with IoT

- Connected devices exposing a substantial attack surface
- Common to see poor development practices
 - Common to have poor default user/password
 - Ship and forget
- Transmitted data not always encrypted (e.g. TLS)
- Bugs and vulnerabilities will happen
 - Issues can happen at any piece of the stack, including hardware
 - Updates are critical for reacting and fixing issues as they arise

"Just use traditional
update systems!"

Linux distro hacked on GitHub, “all code considered compromised”

ANDY GREENBERG SECURITY 07.07.17 10:00 AM

THE PETYA PLAGUE EXPOSES THE THREAT OF EVIL SOFTWARE UPDATES

INDUSTRY NEWS

Vault 7: CIA used fake software update to spy on NSA, DHS, FBI

Somebody Tried to Hide a Backdoor in a Popular JavaScript npm Package

KIM ZETTER SECURITY 06.04.12 04:44 PM

FLAME HIJACKS MICROSOFT UPDATE TO SPREAD MALWARE DISGUISED AS LEGIT CODE

By [Catalin Cimpanu](#)

 May 3, 2018  06:15 AM  0

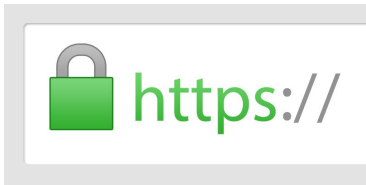
Common Update Threats

- Arbitrary installation attacks
- Endless data attacks
- Extraneous dependencies attacks
- Fast-forward attacks
- Indefinite freeze attacks
- Malicious mirrors preventing updates
- Mix-and-match attacks
- Rollback attacks
- Slow retrieval attacks
- Vulnerability to key compromises
- Wrong software installation

Problems with traditional Update Systems

- TLS

- Only secures the communication
- Doesn't say anything about the server
- Online Key
- Single point of failure



- GPG

- Offline key, but need for frequent updates makes it online
- Trust for anything usually implies trust for everything
- Key compromise can compromise the entire system



The Update Framework - TUF

The Update Framework



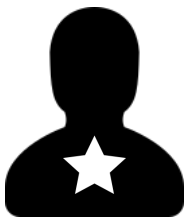
- Framework for securing software update systems
- Created and maintained by Justin Cappos (assistant professor at NYU)
- Largely based on Thandy, Tor's application updater
- Designed to be **compromise resilient**
- Provides **multiple roles** and **signed metadata** (JSON)

“A software update system is secure if it can be sure that it knows about the latest available updates in a timely manner, any files it downloads are the correct files, and no harm results from checking or downloading files.”

TUF: Design Principles

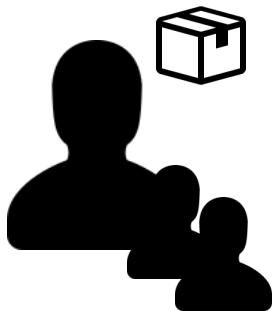
- Multiple Roles
- Responsibility Separation
 - Allows Roles Delegation
- Multi-signature Trust
 - Threshold Signatures
- Minimize Individual Key and Role Risk
- Explicit and Implicit Key Revocation

TUF: Roles Overview



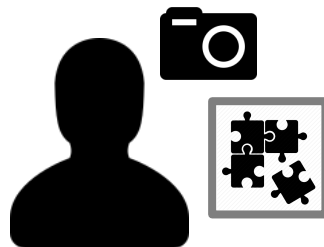
Root

(root of trust)



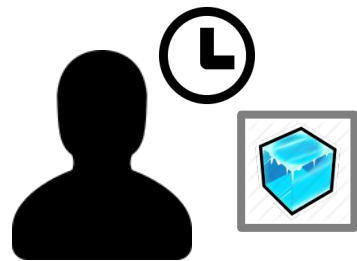
Targets

(integrity)



Snapshot

(consistency)



Timestamp

(freshness)

TUF: Roles Overview



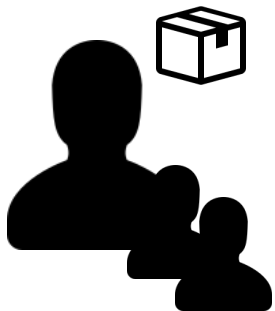
Root

/root.json

(root of trust)

```
{ "_type" : "root",  
  "spec_version" : SPEC_VERSION,  
  "version" : VERSION,  
  "expires" : EXPIRES,  
  "keys" : {  
    KEYID : KEY ,  
    ... },  
  "roles" : {  
    ROLE : {  
      "keyids" : [ KEYID, ... ] ,  
      "threshold" : THRESHOLD }  
    , ... }  
}
```

TUF: Roles Overview



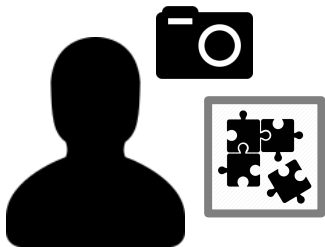
Targets

/targets.json

(integrity)

```
{ "_type" : "targets",  
  "spec_version" : SPEC_VERSION,  
  "version" : VERSION,  
  "expires" : EXPIRES,  
  "targets" : {  
    TARGETPATH : {  
      "length" : LENGTH,  
      "hashes" : HASHES,  
    },  
    ("delegations" : DELEGATIONS)  
  }
```


TUF: Roles Overview



Snapshot

/snapshot.json

(consistency)

```
{ "_type" : "snapshot",  
  "spec_version" : SPEC_VERSION,  
  "version" : VERSION,  
  "expires" : EXPIRES,  
  "meta" : {  
    "root.json": { "version": 1 },  
    "targets.json": { "version": 1 },  
  },  
}
```

TUF: Roles Overview



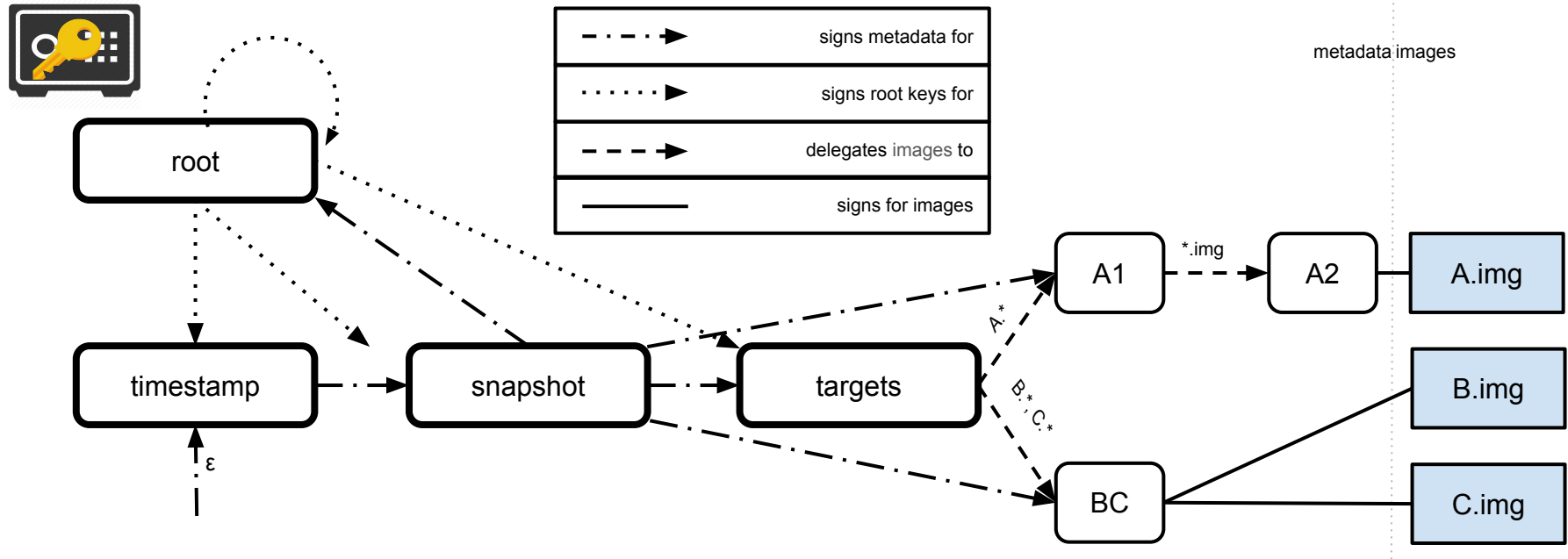
Timestamp

/timestamp.json

(freshness)

```
{ "_type" : "timestamp",  
  "spec_version" : SPEC_VERSION,  
  "version" : VERSION,  
  "expires" : EXPIRES,  
  "meta" : {  
    "snapshot.json": {  
      "hashes": { "sha256": "..."} ,  
      "length": LENGTH,  
      "version": 1 }  
    },  
  },  
}
```

TUF: Design Principles for a Repository

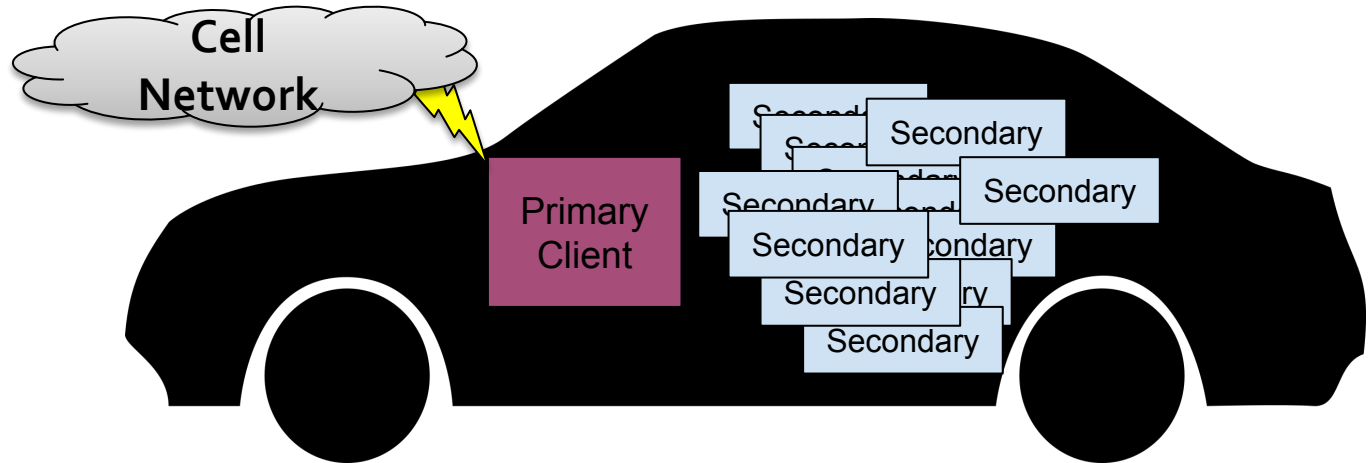


A dark blue horizontal bar with a 3D arrow pointing to the right, set against a background of vertical blue stripes of varying shades.

Uptane

Difficulties applying TUF to IoT and Automotive

- TUF only offers one secure view to a repository
- No way to provide a customized view based on the client needs
- How to manage devices composed by multiple computing units (ECUs)?



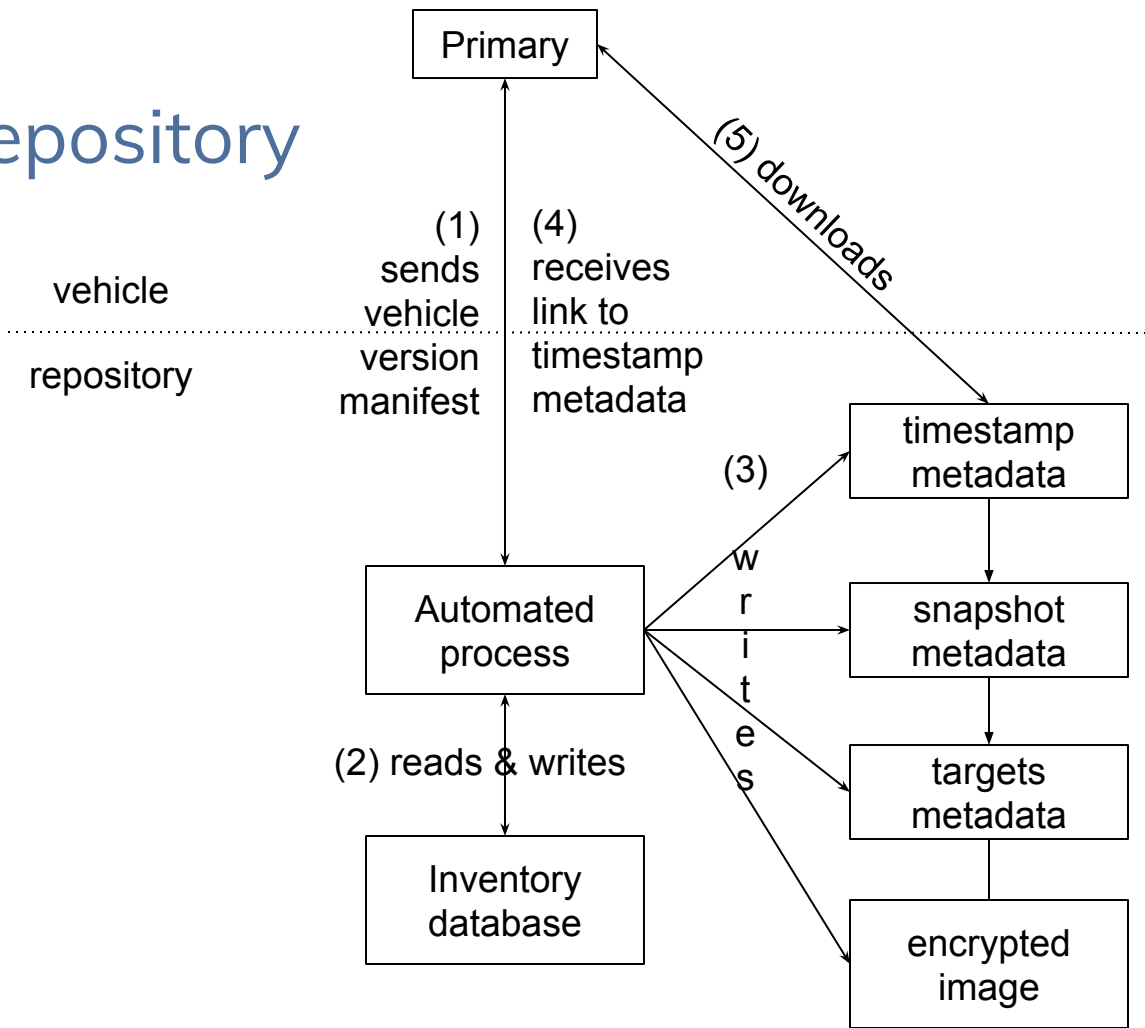
Uptane: TUF Extended for Automotive

- Software update security system developed by New York University, University of Michigan and Southwest Research Institute
- Multiple Repositories: Director and Image Repository
- Primary and Secondary Clients
- Timeserver
- Full and Partial Verification

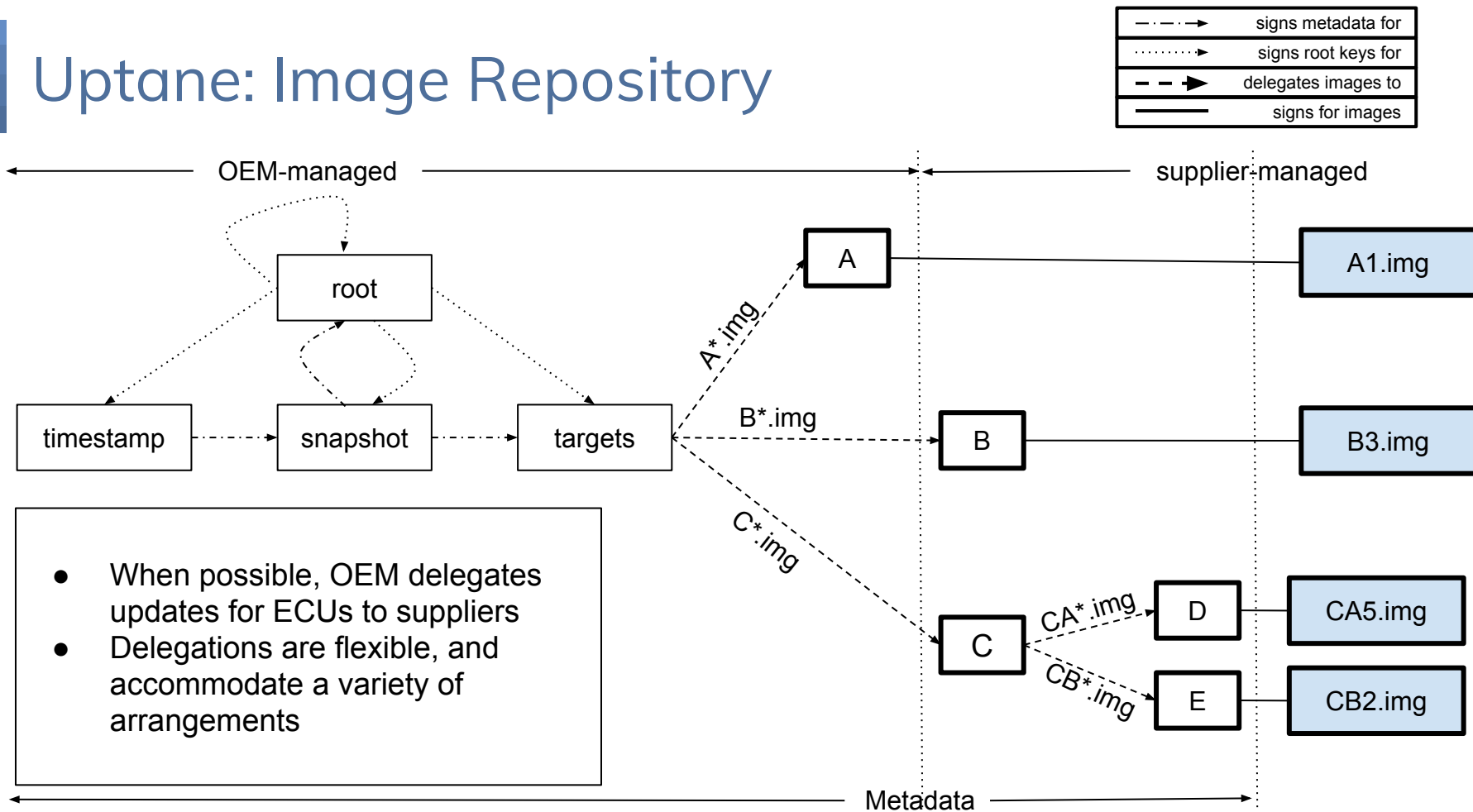
Uptane

Uptane: Director Repository

- Records vehicle version manifests
- Determines which ECUs install which images
- Produces different metadata for different vehicles
- May encrypt images per ECU
- Has access to an inventory database



Uptane: Image Repository



Integrating TUF / Uptane

OpenEmbedded / Yocto

- Meta-Updater Layer
 - <https://github.com/advancedtelematic/meta-updater>
 - Enables TUF / Uptane over-the-air updates with OSTree and Aktualizr
 - Used by Linux microPlatform by default
- Aktualizr
 - Implements Uptane specification
 - Controls the actual device update process
 - OSTree supported by default
 - Additional packaging / image targets can be implemented

OTA Community Edition

- Open-source server software to allow over-the-air updates
- Implements the server side of the Uptane specification
- Microservice based
 - Components can be easily replaced if needed
 - Foundries.io provides a customized UI
- Implements OSTree-compatible repository
- Aktualizr as default client
 - REST API exposed, additional clients can be easily supported
- <https://github.com/advancedtelematic/ota-community-edition>
- <https://foundries.io/insights/2018/07/12/ota-part-4/>



Devices

Name	Stream	Image	Status	Last Seen	Registered	Actions	
beagle-1	premerge	405	Up to date	2018-08-11T10:59:59Z	2018-08-10T21:45:00Z		
beagle-release-1	premerge	391	UpToDate	2018-07-31T20:39:01Z	2018-07-31T20:17:57Z		
colibri-release-1	premerge	391	Up to date	2018-08-07T19:43:48Z	2018-07-31T23:16:22Z		
cubox-i-release	premerge	391	UpToDate	2018-07-31T22:59:28Z	2018-07-31T22:21:49Z		
db410c-release-1	premerge	415	Up to date	2018-08-17T23:42:54Z	2018-08-15T22:38:16Z		
intel-4	premerge	405	UpToDate	2018-08-11T01:45:26Z	2018-08-11T01:44:19Z		
intel-5	premerge	406	Up to date	2018-08-11T01:51:31Z	2018-08-11T01:47:51Z		
minnow-release-1	premerge	391	UpToDate	2018-07-31T22:16:38Z	2018-07-31T21:44:03Z		
rpi3-64-release-1	premerge	411	Up to date	2018-08-14T00:11:31Z	2018-08-13T23:30:32Z		
rpi3-64-release-2	premerge	410	UpToDate	2018-08-14T01:46:35Z	2018-08-14T00:19:03Z		



Devices → «rpi3-64-release-1»

Name rpi3-64-release-1
Stream premerge
OTA+ UUID 876e67f3-b16e-4938-9c6a-1a922f198ce6
Product Raspberry Pi 3 Model B Plus Rev 1.3
Serial 000000007aca937d

Status Up to date
Last Seen 2018-08-14T00:11:31Z
Registered 2018-08-13T23:30:32Z

IP address 192.168.1.64
Hostname raspberrypi3-64
MAC address b8:27:eb:ca:93:7d

Auto update ☒

Image Info

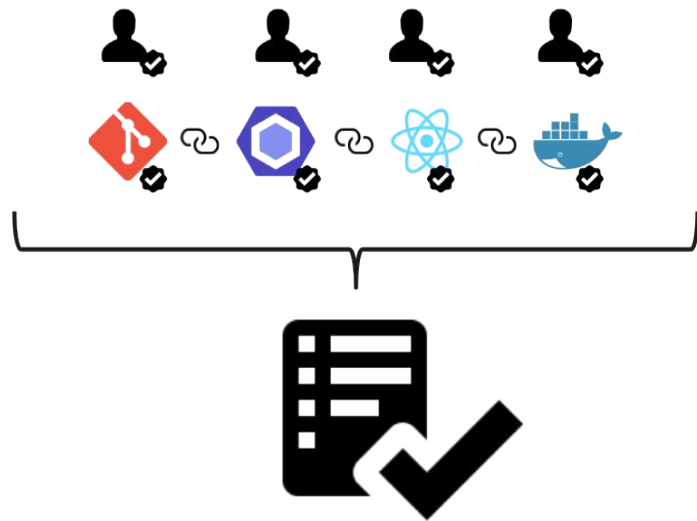
Name 411
Hardware Id raspberrypi3-64
Hash 3fed7d185ec9508985dbf3477b5705130782c40bb4798d62545dae75a31ba332

Available Images

Name	Update Time	Hash	Action
418	2018-08-22T20:46:51Z	a646ab68a87b17e60d6c94720e014238d106f1c9814a328f8664ac459da11d36	Apply
417	2018-08-22T17:49:29Z	9bd67674b3099345ec3d24c150998f98c5dcbb857b6145b72b95d1489a586783	Apply

Related Projects

- In-toto
 - Framework to protect supply chain integrity





Thank You!

ricardo@foundries.io



FOUNDRIES.IO



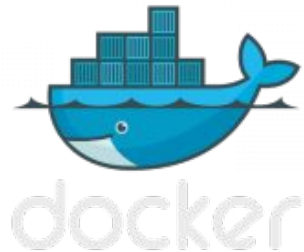
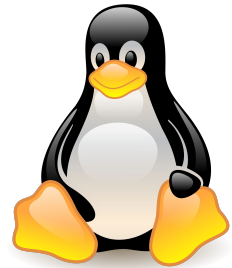
Backup Slides



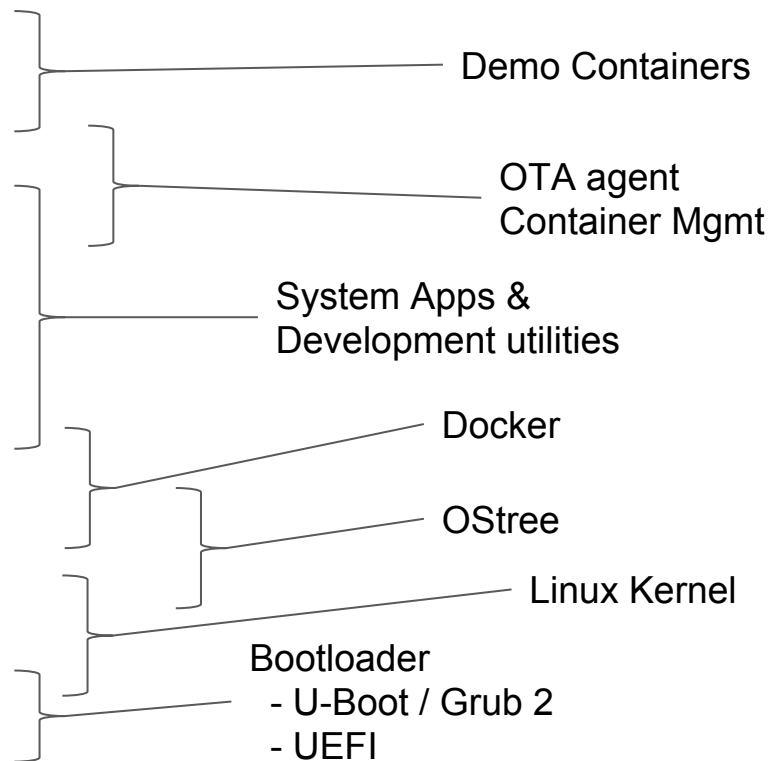
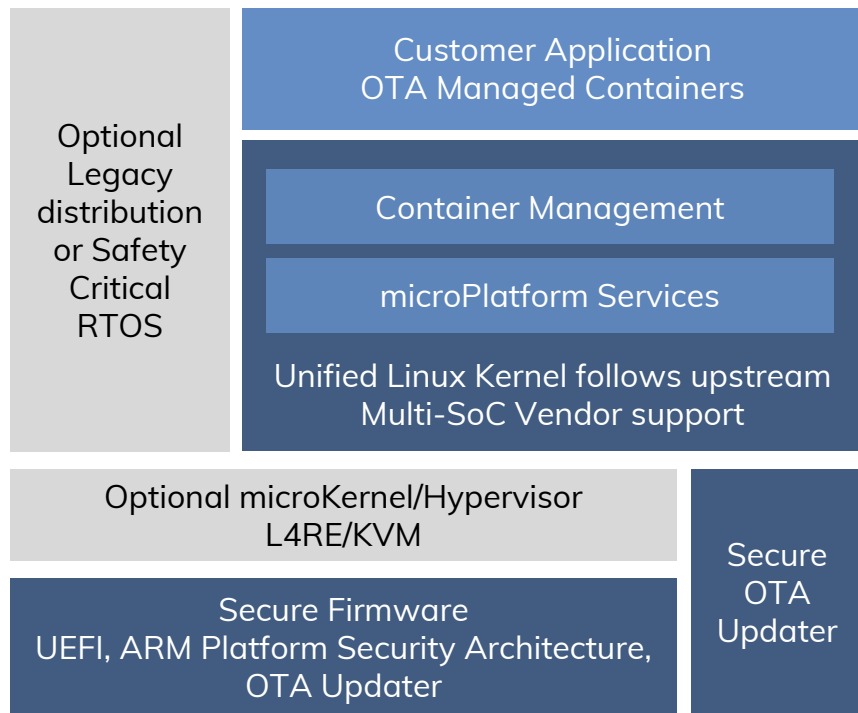
microPlatforms

microPlatforms - OS / Distributions

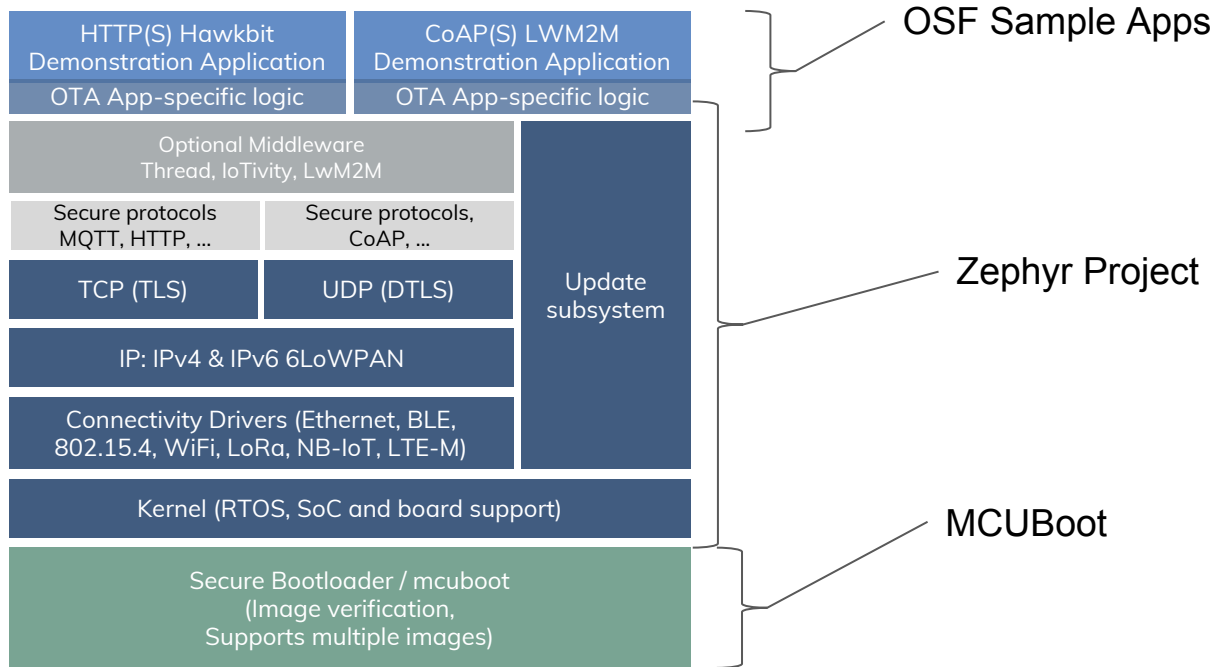
- Upstream, open source software
- microPlatforms are built directly from upstream open source projects
 - As close to tip as possible
 - Little or no non-upstream code
- Stabilized and tested for connected IoT use-case
- Continuous updates (integrated & fully tested)
 - Continuous merge-ups
- We believe that the most secure and stable software is upstream software
- It's open source, there is No proprietary Lock-in



Linux microPlatform - the 'OS' for embedded systems



Zephyr microPlatform - OS for microcontrollers



OSTree basics: sysroot

/boot/

/loader/uEnv.txt

/ostree

/deploy/os/deploy/da3045...

/deploy/os/deploy/4eda05...

/deploy/os/var

/ostree/repo/objects/4eda...4.commit

/ostree/repo/objects/c4b5...5.dirtree

/ostree/repo/objects/805d...a.file

/ostree/repo/objects/7d11...0.file

bootargs=ostree=/ostree/deploy/
os/deploy/4eda...4/

Deployment sysroot

/bin -> /usr/bin

/lib -> /usr/lib

/var

/usr

/lib

/libostree-1.so.1