Software and Firmware Updates for Internet of Things

SIMON CARLSON

Master in Information Technology
Date: January 29, 2019
Supervisor: Farhad Abtahi
Examiner: Elena Dubrova
Swedish title: Mjukvaru- och Firmwareuppdateringar för Internet of Things
School of Computer Science and Communication

Abstract

IoT devices are used in a variety of use cases and the use of IoT is expected to grow significantly the coming years. Unsecured devices have the past years led to IoT devices being leveraged in attacks or attacked themselves, which is in the face of growth unacceptable. In order to secure devices, they need to be updated to patch existing and future vulnerabilities. However, update mechanisms for remote and constrained IoT devices are most often proprietary and closed source. In order to develop an open and interoperable, the IETF has created a working group called SUIT. SUIT has developed a standard for IoT updates, which forms the basis of this work. The thesis explains the state of the art and SUIT standard, from which it develops a software and firmware update mechanism for constrained IoT devices. The mechanism fulfills X and Y from the standard, while showing G and H reliability and power requirements on the nodes.

Sammanfattning

Svensk sammanfattning här.

Contents

Chapter 1

Introduction

1.1 Background

Internet of Things, or IoT, is the notion of connecting physical objects to the world-spanning Internet in order to facilitate services and communication both machine-to-human and machine-to-machine. By having everything connected from everyday appliances to vehicles to critical parts of infrastructure, computing will be ubiquitous and the Internet of Things realized. The benefits from the IoT can range from quality of life services, such as controlling lights and thermostats from afar, to data gathering through wireless sensor networks, to enabling life critical operations such as monitoring a pacemaker or traffic system. IoT is a broad definition and fits many different devices in many different environments, what they all have in common is that they are physical and connected devices.

The Internet of Things is expected to grow massively in the following years as devices get cheaper and more capable. Ericsson expects the amount of IoT connections to reach 22.3 billion devices in 2024, of which the majority is short-range IoT devices [1]. However, cellular IoT connections are expected to have the highest compound annual growth rate as 4G and new 5G networks enable even more use cases for IoT devices.

In recent years the general public has become increasingly aware of digital attacks and intrustions affecting their day to day lives. In 2016 the DNS provider Dyn was attacked by a botnet consisting of heterogeneous IoT devices infected by the Mirai malware. Devices such as printers and baby monitors were leveraged to launch an attack on

Dyn's services which affected sites like Airbnb, Amazon, and CNN [2]. Cardiac devices implanted in patients were also discovered to be unsafe, with hackers being able to deplete the batteries of pacemakers prematurely [3]. These cases and many others make it clear that security in IoT is a big deal, and as IoT is expected to grow rapidly insecure devices can cause even more problems in the future.

Security in IoT is also closely related to its business potential. According to Bain & Company, the largest barrier for Internet of Things adoptation is security concerns, and customers would buy an average of 70% more IoT devices if they were secured [4]. Despite security being lacking today in IoT, the field is expected to grow rapidly and an increase in unsecured devices could spell disaster. Securing IoT equipment such as printers, baby monitors, and pacemakers is imperative to prevent future attacks. But what about the devices currently employed without security, or devices in which security vulnerabilities are discovered after deployment? They need to be updated and patched in order to fix these vulnerabilities, but sending a technician to each and every of the predicted 22.3 billion devices is not feasible. They need secure and remote updates which is a non-trivial task.

1.2 Problem Statement

There is a need for secure software and firmware updates for IoT devices as vulnerabilities must be patched. For many IoT devices this mean patches must be applied over long distances and possibly unreliable communication channels as sending a technician to each and every device is unfeasible. There are non-open, proprietary solutions developed for specific devices but no open and interoperable standard. The IETF SUIT working group aims to define an architecture for such a mechanism without defining new transport or discovery mechanisms [5]. By expanding upon the work of the SUIT group, a standardized update mechanism suitable for battery powered, constrained, and remote IoT devices can be developed.

1.2.1 Problem

The thesis project will examine the architecture and information model proposed by SUIT in order to create and evaluate an updating mechanism for battery powered, constrained, and remote IoT devices with

a life span exceeding five years. The update mechanism can be considered in three parts, communication, upgrading, and device management. Communication will happen over unreliable channels and the payloads must arrive intact and untampered with. The upgrade mechanism itself must ensure integrity of the target image and safely perform the upgrade with a limited amount of memory. Device management concers managing devices in a network and seeing which devices are in need of updates. Device management will not be considered in this thesis.

The thesis will examine the update mechanism from the viewpoint of IoT devices running the Contiki-NG operating system on 32-bit ARM Cortex M3 processors. A suitable public key infrastructure developed by RISE will also be an underlying assumption for the work. The thesis aims to investigate the problem "How can the SUIT architecture be used to provide secure software and firmware update for the Internet of Things?".

1.2.2 Purpose

The purpose of the thesis project is to provide an open and interoperable update mechanism that complies with the standards suggested by the IETF SUIT working group. This will aid other projects trying to secure their IoT devices following accepted standards.

1.2.3 Goal

The goals of the thesis are to study current solutions and technologies and then propose lightweight end-to-end protocols that can be used when updating IoT devices. The degree project shall deliver specifications and prototypes of the protocols in an IoT testbed, as well as a thesis report.

1.3 Methodologies

The thesis will follow a mix of qualitative and quantitative methodologies. The SUIT group defines some goals or constraints a suitable updating mechanism should follow, but as their proposed architecture is agnostic of any particular technology these goals cannot be easily quantified. It is better to regard them as qualitative properties the

mechanism should have. In addition to this there are some relevant measurements, such as reliability of the communication and memory and power requirements of the updates, that can be used in an evaluation. The quantitative part of the evaluation will follow an objective, experimental approach, while the qualitative part will follow a interpretative approach.

1.4 Risks, Consequences, and Ethics

As IoT devices become more commonplace their security becomes more important. Incorrect or faulty firmware or software can lead to incorrect sensor readings, a common application of IoT devices, which in turn can lead to incorrect conclusions. This could have a large effect on businesses such as agriculture and healthcare.

As these devices are typically connected on networks with other computers such as laptops, a compromised IoT device can cause an attack to proliferate throughout an entire network. This can affect other IoT devices as well as traditional computers, putting every connected device at risk. Furthermore hacked devices can leak data to attackers and cause service distruptions. All of these risks and more have to be accounted for as IoT is expected to boom.

1.5 Scope

The updating mechanism can be roughly split into three parts: the actual updating or flipping of images on the device, the transportation of the new image, and managing a heterogeneous network of devices needing different updates at different times. This thesis will only look at the first two parts, updating a firmware image on the device and transportation of the image. The thesis will not be concerned with device management. Furthermore the thesis will focus on the use case of applying an entire update to one single device. Other use cases such as broadcasting updates or applying differential updates will only be considered with respect to time.

1.6 Outline

Chapter two describes the theoretical background needed to understand the results of the thesis. This includes the network protocols and operating system being used in the thesis as well as the SUIT standard. Chapter three describes the design of the communication protocols used in the update mechanism. Chapter four describes how the local update mechanism works and how devices can upgrade their images. Chapter five evaluates the developed updating mechanism and presents the results. Chapter six ends the report with a discussion about the update mechanism and its results.

Chapter 2

Theoretic Background

This chapter presents the theoretical background needed to understand the thesis. Section 2.1 introduces the networks protocols used and motivates their use over other protocols in an IoT context. The following section, Section 2.2 presents and explains the SUIT architecture and information model and their respective requirements as formulated by the IETF. Finally, Section 2.3 presents the Contiki-NG operating system which the updating mechanism will be developed for as well as the target hardware.

2.1 IoT Network Stack

Network protocols in IoT networks operate under different circumstances compared to traditional computer networks. Networks in IoT are defined by their low power requirements, low reliability, and low computational performance on edge devices whereas traditional networks enjoy high reliability, high throughput, and high computational performance. This posts some constraints on the protocols used in IoT as they must properly handle these characteristics.

One of the most widely used network protocol stacks today in traditional networks is the TCP/IP stack. It uses TCP as a transportation protocol, usually with TLS for security, and a common application layer protocol is HTTP. TCP is however poorly suited for IoT networks as it is a connection based, stateful protocol which tries to ensure the guaranteed delivery of packets in the correct order. There is also advanced congestion control mechanisms in TCP which are hard to apply on low-bandwitch, unreliable networks. IoT networks on the other

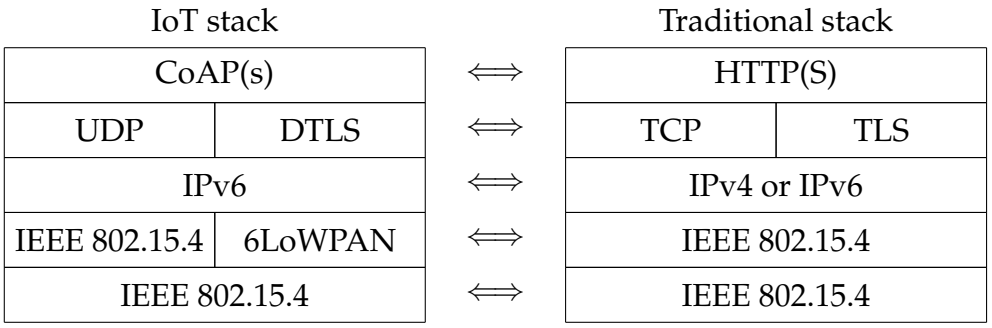

Figure 2.1: Comparison of network stacks between IoT networks and traditional networks.

hand often utilize UDP for transport. UDP is also an IP-based protocol but it connectionless and less reliable than TCP, performing on a best-effort level instead. Despite being less reliable, UDP often performs better in IoT contexts. As TLS is based on the same assumptions TCP it is unsuitable for UDP networks.

UDP networks are instead secured by DTLS, which is a version of TLS enhanced for use in datagram oriented protocols. HTTP can be used over UDP for the application layer, but as HTTP is encoded in human readable plaintext it is unecessarily wordy and not optimal for constrained networks. Instead, CoAP is a common protocol for the application layer in IoT networks. Figure 2.1 shows the equivalent protocols for IoT network stacks versus traditional network stacks.

In this chapter, subsection 2.1.1 explains UDP and why it is the prefered transport protocol in IoT networks. Subsection 2.1.2 briefly explains TLS, why it is unsuitable for IoT networks, the differences between TLS and DTLS and why DTLS is used. Subsection 2.1.3 describes the CoAP protocol, and lastly subsection 2.1.4 briefly introduces the certificate enrollment protocol used in the thesis.

2.1.1 UDP

UDP is a stateless and asynchronous transfer protocol for IP [6]. It does not provide any reliability mechanisms but is instead a best-effort protocol. It also does not guarantee delivery of messages. For general purposes in unconstrained environments TCP is usually the favored transport protocol as it is robust and reliable, but in environments

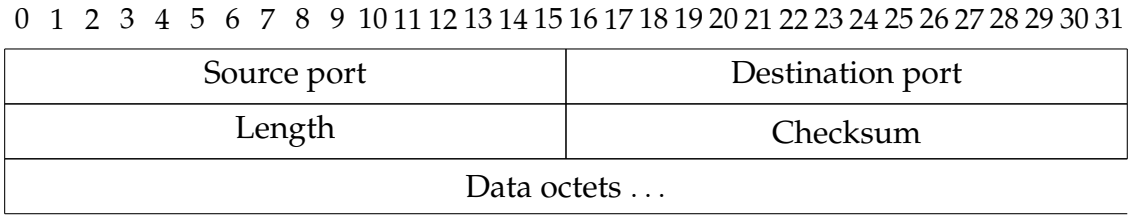

Figure 2.2: The UDP header format.

where resources are scarce and networks unreliable, a stateful protocol like TCP could face issues. Since TCP wants to ensure packet delivery, it will retransmit packages generating a lot of traffic and processing required for a receiver. Also, if the connection is too unstable TCP will not work at all since it can no longer guarantee the packets arrival. The best-effort approach of UDP is favorable in these situations, in addition to UDP being a lightweight protocol.

Figure 2.2 shows the UDP header format. The source port is optional, the length denotes the length of the datagram (including the header), and the checksum is calculated on a pseudo-header constructed from both the IP header, UDP header, and data.

2.1.2 DTLS

DTLS is a protocol which adds privacy to datagram protocols like UDP [7]. The protocol is designed to prevent eavesdropping, tampering, or message forgery. DTLS is based on TLS, a similar protocol for stateful transport protocols such as TCP, which would not work well on unreliable networks as previously discussed. The main issues with using TLS over unreliable networks is that TLS decryption is dependant on previous packets, meaning the decryption of a packet would fail if the previous packet was not received. In addition, the TLS handshake procedure assumes all handshake messages are delivered reliably which is not the case in IoT networks.

DTLS solves this by banning stream ciphers, effectively making decryption an independent operation between packets, as well as adding explicit sequence numbers. Furthermore, DTLS supports packet retransmission, reordering, as well as fragmenting DTLS handshake messages into several DTLS records. These mechanisms makes the handshake process feasible over unreliable networks. By splitting messages into different DTLS records, fragmentation at the IP level can

be avoided since a DTLS record is guaranteed to fit an IP datagram. IP fragmentation is problematic is low-performing networks since if a single fragment of an IP packet is dropped all fragments of that packet must be retransmitted and should thus be avoided. Since DTLS is designed to correctly handle reordering and retransmission in lossy networks, splitting messages into several DTLS records is no problem, and if one record is lost only that record needs to be retransmitted

Listing 2.1 shows the DTLS record structure. It contains a TLS 1.2 type field, a version field which for DTLS 1.2 is 254.253, an epoch counter that is incremented for each cipher state change, an increasing sequence number (unique to each epoch), a length field and a fragment field containing the application data [8]. These fields, with the exception of the epoch and sequence number, are the same as in TLS 1.2 [7].

Listing 2.1: The DTLS plaintext record structure.

```
struct {
    ContentType type;
    ProtocolVersion version;
    uint16 epoch;
    uint48 sequence_number;
    uint16 length;
    opaque fragment[DTLSPlaintext.length];
} DTLSPlaintext;
```

Listing 2.2: The DTLS ciphertext record structure.

```
struct {
    ContentType type;
    ProtocolVersion version;
    uint16 epoch;
    uint48 sequence_number;
    uint16 length;
    select (CipherSpec.cipher_type) {
        case block: GenericBlockCipher;
        case aead: GenericAEADCipher;
    } fragment;
} DTLSCiphertext;
```

TLS records are compressed and then encrypted, the same holds for DTLS. When initating contact, a compression algorithm is cho-

sen. The DTLSPlaintext is then compressed into a DTLSCompressed record, with similar structure to Listing 2.1.The compressed record is encrypted into a DTLSCiphertext record whose structure is shown in Listing 2.2. Note that since DTLS disallows stream ciphers they are not an option in the encrypted fragment, whereas in TLS they are.

In order to communicate via TLS and DTLS, a handshake has to be carried out. The handshake establishes parameters such as protocol version, cryptographic algorithms, and shared secrets. The TLS handshake involves hello messages for establishing algorithms, exchanging random values, and checking for earlier sessions. Then cryptographic parameters are shared in order to agree on a shared premaster secret. The parties authenticate each other via public key encryption, generate a shared master secret based on the premaster secret, and finally verifies that their peer has the correct security parameters. The DTLS handshake adds to this a stateless cookie exchange to prevent DoS attacks, some modifications to the handshake header to make communication over UDP possible, and retransmission timers since the communication is unreliable. Otherwise the DTLS handshake is as the TLS handshake.

2.1.3 CoAP

CoAP is an application layer protocol designed to be used by constrained devices over networks with low throughput and possibly high unreliability for machine-to-machine communication [9]. While designed for constrained networks, a design feature of CoAP is how it is easily interfaced with HTTP so that communication over traditional networks can be proxied. CoAP uses a request/response model similar to HTTP with method codes and request methods that are easily mapped to HTTP. Furthermore CoAP is a RESTful protocol utilizing concepts such as endpoints, resources, and URIs. Additionally CoAP offers features such as multicast support, asynchronous messages, low header overhead, and UDP and DTLS bindings which are all suitable for constrained environments.

As CoAP is usually implemented on top of UDP, communication is stateless and asynchronous. For this reason CoAP defines four message types: Confirmable, Non-confirmable, Acknowledgement, and Reset. Confirmable messages must be answered with a corresponding Acknowledgement, this provides one form of reliability over an other-

wise unreliable channel. Non-confirmable messages do not require an Acknowledgement and thus act asynchronously. Reset messages are used when a recipient is unable to process a Non-confirmable message. Confirmable, Non-confirmable, and Acknowledgement messages all use Message IDs in order to detect duplicate messages in case of retransmission.

Since CoAP is based on unreliable means of transport, there are some lightweight reliability and congestion control mechanics in CoAP. Message IDs allows for detection of duplicate messages and tokens allow asynchronous requests and responses be paired correctly. There is also a retransmission mechanic with an exponential back-off timer for Confirmable messages so that lost Acknowledgements does not cause a flood of retransmissions. Additionally, CoAP features piggybacked responses, meaning a response can be sent in the Acknowledgement of a Confirmable or Non-Confirmable request if the response fits and is available right away. This also reduces the amount of messages sent by the protocol.

Figure 2.3 shows the CoAP message format. The 2-bit version (Ver) field indicates the CoAP version, which at time of writing is 1 (01 in binary). The 2-bit type (T) field determines the type of message (Confirmable, Non-confirmable, Acknowledgement, Reset). Token length (TKL) indicates the length of the Token field which can vary between zero to eight bytes. The 8-bit code field carries which method code the message carries and can be further broken into a 3-bit class and 5-bit detail. The class can indicate a request (0), a success response (2), a client error response (4), or a server error response (5), with the detail further specifying the status of the message. The message ID is a 16-bit integer used to detect duplicate message and to match Acknowledgement or Resets with their initiating requests.

Following the header is the zero to eight bit Token value, which in turn is follow by zero or more Options. One of the options offered is the observe options, which allows a client to notified by the server when a particular resource changes. Lastly comes the optional payload, which if present is prefixed by a payload marker (0xFF). The length of the payload is dependant on the carrying protocol, which in this thesis will be DTLS. The length of the payload is calculated depending on the size of the CoAP header, token, and options as well as maximum DTLS record size.

Since firmware images can be relatively large their size needs to

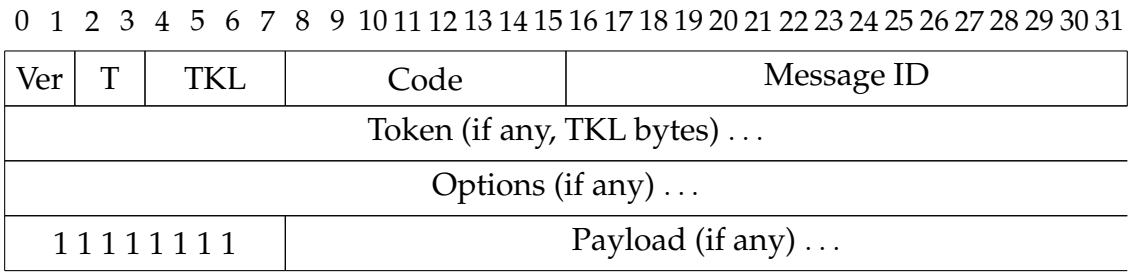

Figure 2.3: The CoAP message format.

be handled during transportation, which can be done via block-wise transfers [10]. A Block option allows stateless transfer of a large file separated in different blocks. Each block can be individually retransmitted and by using monotonically increasing block numbers, the blocks can be reassembled. The size of blocks can also be negotiated between server and client meaning they can always find a suitable block size, making the mechanism quite flexible.

2.1.4 EST-coaps

EST-coaps is a protocol for certificate enrollment in constrained environments using CoAP. [11]. By allowing IoT devices to enroll for certificates, assymetric encryption can be used even in a constrained environment. EST-coaps is heavily based on EST which was developed for traditional, less constrained networks and is thus unsuitable to be used with the SUIT standard [12]. EST-coaps retains much of the functionality and structure of EST but modifies it slightly to work over CoAP, DTLS, and UDP instead of HTTP, TLS, and TCP, for instance by making use of CoAPs block requests and responses to remedy the relatively large sizes of certificates.

2.2 SUIT

The IETF SUIT (Software Updates for Internet of Things) working group aims to define a firmware update solution for IoT devices that is interoperable and non-proprietary [5]. The working group does not however try to define new transport or discovery mechanism, making their proposal angostic of any particular technology. The solution shall be usable on Class 1 devices, defined by 10 KiB RAM and 100 KiB code size [13]. The solution may be applied to more powerful devices.

Subsection 2.2.1 presents the SUIT architecture and subsection 2.2.2 presents the SUIT information model.

2.2.1 Architecture

There is an Internet Draft by the SUIT group focusing on the firmware update architecture [14]. This draft describes the goals and requirements of the architecture, although makes no mention of any particular technology. The overarching goals of the update process is to thwart any attempts to flash unauthorized, possibly malicious firmware images as well as protecting the firmware image's confidentiality. These goals reduces the possibility of an attacker either getting control over a device or reverse engineering a malicious but valid firmware image as an attempt to mount an attack.

In order to accept an image and update itself, a device must be presented with certain information. Several decisions must be made before updating and the information comes in form of a manifest. The next section will describe the requirements posted upon this manifest in more detail. The manifest helps the device make important decisions such as if it trusts the author of the new image, if the image is intact, if the image is applicable, where the image should be stored and so on. This in turns means the device also has to trust the manifest itself, and that both manifest and update image must be distributed in a safe and trusted architecture. The draft [14] presents ten qualitative requirements this architecture should have:

- Agnostic to how firmware images are distributed:
  As this thesis aims to implement a prototype of an update mechanism, some choices about technology has to be done. This will realistically mean only a subset of the SUIT standard will be implemented as certain parts of the standard is not applicable. The proposed network stack uses UDP, DTLS, and CoAP for transportation and the target devices are Firefly devices running the Contiki-NG operating system.

- Friendly to broadcast delivery:
  Broadcasting will not be of main concern in this thesis, it will be considered with respect to time.

- Use state-of-the-art security mechanisms:
  The SUIT standard assumes a PKI is in place. RISE has previ-

ously developed a PKI suitable for IoT, this PKI is an underlying assumption for the thesis. The PKI will allow for signing of the update manifest and firmware image.

- Rollback attacks must be prevented:
  The manifest will contain metadata such as monotonically increasing sequence numbers and best-before timestamps to avoid rollback attacks.

- High reliability:
  This is an implementation requirement and depends heavily on the hardware of the target device.

- Operate with a small bootloader:
  This is also an implementation requirement.

- Small parser:
  It must be easy to parse the fields of the update manifest as large parser can get quite complex. Validation of the manifest will happen on the constrained devices which further motivates a small parser and thus less complex manifests.

- Minimal impact on existing firmware formats:
  The update mechanism itself must not make assumptions of the current format of firmware images, but be able to support different types of firmware image formats.

- Robust permissions:
  This requirement is directed towards the administration of firmware updates and how different roles interact with the devices. The thesis will not consider any infrastructure outside of transporting manifest and image and applying the update, such as device management, but will consider authorisation of parties through techniques like signing.

- Operating modes:
  The draft presents three broad modes of updates: client-initiated updates, server-initiated updates, and hybrid updates, where hybrids are mechanisms that require interaction between the device and firmware provider before updating. The thesis will look into all three of these broad classes. Some classes may be preferred over others based on the technologies chosen in the thesis.

The distribution of manifest and firmware image is also discussed, with a couple of options being possible. The manifest and image can be distributed together to a firmware server. The device then recieves the manifest either via pulling or pushing and can subsequently download the image. Alternatively, the manifest itself can be directly sent to the device without a need of a firmware server, while the firmware image is put on the firmware server. After the device has receieved the lone manifest through some method, the firmware can be downloaded from the firmware server. The SUIT architecture does not enforce a specific method to be used when delivering the manifest and firmware, but states that an update mechanism must support both types.

2.2.2 Information Model

The corresponding Internet Draft for the SUIT information model presents the information needed in the manifest to secure a firmware update mechanism [15]. A manifest is needed for a device to make a decision about whether or not to update itself, and if the image related to the manifest is valid and untampered with.

The draft also presents threats, classifies them according to the STRIDE model, and presents security requirements that map to the threats [16]. Finally it presents use cases and maps usability requirements to the use cases in order to motivate the presence of the manifest elements. Since the thesis makes a choice about specific technologies to use, not all use cases, usability requirements, and manifest elements are deemed necessary. The threats and security requirements however are. Note that the information model does not discuss threats outside of transporting the updates, such as physical attacks.

The proposed manifest elements and their brief motivations can be seen in Table 2.1. For more detailed motivations and requirements, refer to [15].

Table 2.1: The proposed manifest elements of the SUIT information model.

Manifest Element	Status	Motivation/Notes
Version identifier	Mandatory	Describes the iteration of the manifest format

Table 2.1: The proposed manifest elements of the SUIT information model.

Manifest Element	Status	Motivation/Notes
Monotonic Sequence Number	Mandatory	Prevents rollbacks to older images
Payload Format	Mandatory	Describes the format of the payload
Storage Location	Mandatory	Tells the device which component is being updated, can be used to establish physical location of update
Payload Digest	Mandatory	The digest of the payload to ensure authenticity. Must be possible to specify more than one payload digest indexed by XIP Address
XIP Address	-	Used to specify which address the payload is for in systems with several potential images
Size	Mandatory	The size of the payload in bytes
Signature	Mandatory	The manifest is to be wrapped in an authentication container (not a manifest element itself)
Dependencies	Mandatory	A list of digest/URI pairs linking manifests that are needed to form a complete update
Precursor Image Digest Condition	Mandatory (for differential updates)	If a precursor image is required, the digest condition of that image is needed
Content Key Distribution Method	Mandatory (for encrypted payloads)	Tells how keys for encryption/decryption are distributed
Vendor ID Condition	Recommended	Helps distinguish products from different vendors
Class ID Condition	Recommended	Helps distinguish incompatible devices in a vendors infrastructure

Table 2.1: The proposed manifest elements of the SUIT information model.

Manifest Element	Status	Motivation/Notes
Required Image Version List	Optional	A list of versions that must be present to apply an update which applies to multiple versions of a firmware
Best-Before Timestamp Condition	Optional	Tells the last application time
Component Identifier	Optional	For heterogeneous storages, identifies which part is to store the payload
URIs	Optional	A list of weighted URIs used to obtain the payload
Directives	Optional	A list of instructions on processing the manifest. Applies to the entire manifest, unlike "Processing Steps"
Aliases	Optional	A list of digest/URI pairs
Processing Steps	-	A list of payload processors needed to process a nested format

Certain elements of the manifest are dependant on certain use cases. Examples of this are storage location (assumes there are more than one components on the device) and precursor image digest condition (assumes differential updates). As the thesis will implement a subset of the SUIT standard, mentioned in Section 2.2.1, not all elements would be mandatory for the particular use cases of the thesis. This will have to be taken into consideration when designing the manifest transport protocol.

To summarize, the SUIT information model proposes to use a signed manifest that is distributed to each device in need of an update. The device then processes the manifest in order to determine if the update is trusted, suitable, up to date, with many other optional elements such as if special processing steps or new URIs to fetch the images are needed. The model does not make assumptions about technology which is one of the reasons there are optional elements, not all of them are applicable to all solutions. Nevertheless, the architecture and information model together provides a solid base on which to design a

secure update mechanism for IoT.

2.3 Contiki-NG

Contiki-NG is an open-source operating system for resource constrained IoT devices based on the Contiki operating system [17], [18]. Contiki-NG focuses on low-power communication and standard protocols and comes with IPv6/LoWPAN, DTLS, and CoAP implementations which makes it a suitable operating system for this thesis. Furthermore Contiki-NG is open source and licensed under the permissive BSD 3-Clause license and targets a wide variety of boards which makes it align with SUITs goal of creating an open standard for updating IoT devices.

Subsection 2.3.1 explains processes, events, and memory management in Contiki-NG. These internals are heavily based on the previous Contiki operating system and much of the information is gathered from there. Subsection 2.3.2 presents the different timers available in Contiki-NG. Subsection 2.3.3 presents part of the network protocol stack that is implemented in standard Contiki-NG. Finally, subsection 2.3.4 presents the target hardware Contiki-NG will run on.

2.3.1 Processes, Events, and Memory Management

Contiki-NG has a process abstraction which is built on lightweight protothreads [19]. Protothreads can be seen as a combination of threads and event-driven programming, keeping the yield semantics of threads and stacklessness of event-driven programming. By providing a conditional blocking wait statement, protothreads can execute cooperatively. All protothreads in a system are run on the same stack, meaning each protothread has a very low memory overhead. A process is declared through a `PROCESS` macro and can be automatically started after system boot or when a specific module is loaded.

Contiki-NGs execution model is event based, meaning processes often yield execution until they are informed a certain event has taken place, upon which they can act. Figure 2.3.1 shows the states of the processes and their transitions. User-space processes are run in a cooperative manner while kernel-space processes can preempt user-space processes. Examples of events are timers expiring, a process being polled, or a network packet arriving.

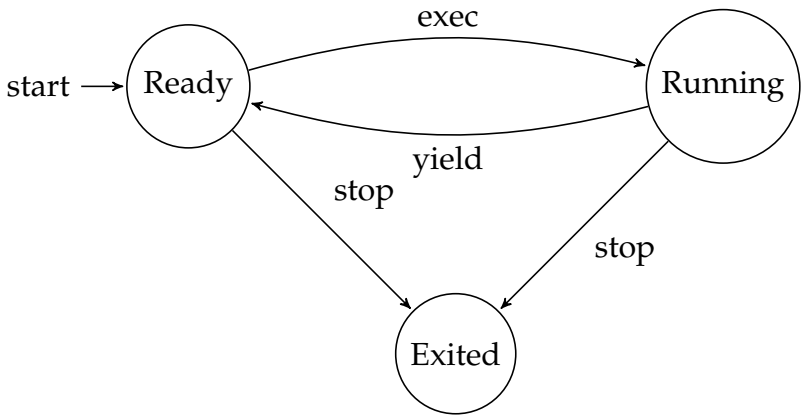

Figure 2.4: The state machine of Contiki threads. Adapted from [20].

Contiki-NG provides two memory allocators in addition to using static memory. They are called `MEMB` and `HeapMem` and are semi-dynamic and dynamic, respectively. `MEMB` provides ways to manage memory blocks. The memory blocks are allocated on static memory as arrays of constant sized objects. After a memory block has been declared, it is initialized after which objects can be allocated memory from the block. All objects allocated through the same block have the same size. Blocks can be freed, and it is possible to check whether a pointer resides within a certain memory block or not.

`HeapMem` solves the issue of dynamically allocating objects of varying sizes during runtime in Contiki-NG. It can be used on a variety of hardware platforms, something a standard C `malloc` implementation could struggle with. To allocate memory on the heap, the number of bytes to allocate must be provided and a pointer to a contiguous piece of memory is returned (if there is enough contiguous memory). Memory can be reallocated and deallocated such as using a normal `malloc`.

2.3.2 Timers

Contiki-NG provides different timers used by both the kernel and user-space applications. The timers are based on the clock module which is responsible for handling system time. The definition of system time is platform dependent.

The different timers and their usages are:

- `timer`: a simple timer without built-in notification.

- `stimer`: counts in seconds and has a long wrapping period.
- `etimer`: schedules events to processes. Since events in Contiki-NG can put yielding processes in the execution state, `etimer` can be used to periodically schedule code by setting up an `etimer` to signal a specific event when it expires then waiting on that event
- `ctimer`: schedules calls to a callback function. `ctimer` works in similar ways to `etimer` but with callbacks to callback functions instead of events.
- `rtimer`: schedules real-time tasks. Since real-time tasks face different requirements than normal tasks, rtimer uses a higher resolution clock. Real-time tasks preempt normal execution so that the real-time task can execute immediately. This mean there are constraints on what can be done in real-time tasks as many functions cannot handle preemption.

`timer`, `stimer`, and `rtimer` are stated to be safe from interrupts while `etimer` and `ctimer` are unsafe. All timers are declared using a timer struct, which is also how the timer is interacted with.

2.3.3 Networking in Contiki-NG

Contiki-NG features an IPv6 network stack designed for unreliable, low-power IoT networks. There are many protocols implemented in the stack, this thesis will look at UDP and CoAP secured by DTLS. Beneath IPv6 Contiki-NG supports IEEE 802.15.4 with Time Slotted Channel Hopping [21].

The CoAP implementation in Contiki-NG is based on Erbium by Mattias Kovatsch but has become part of core modules in the operating system itself [22]. The default implementation supports both unsecured (CoAP) and secured (CoAPs) communication. CoAPs uses a DTLS implementation called TinyDTLS which handles encryption and decryption of messages [23]. The CoAP implementation consists of [24]:

- a CoAP engine which registers CoAP resources
- a CoAP handler API that allows for implementations of resource handlers. The handlers act upon incoming messages to their corresponding resource

- a CoAP endpoint API allowing handling of different kinds of CoAP endpoints.
- a CoAP transport API which hands CoAP data from the CoAP stack to the transport protocol.
- CoAP messages functions for parsing and creating messages
- a CoAP timer API providing timers for retransmission mechanisms.

2.3.4 Firefly

Zolertia Firefly is a supported hardware platform in Contiki-NG and the targeted board for this thesis. It is a breakout board designed for IoT application development sporting an ARM Cortex-M3 with 512 KB flash and 32 KB RAM, making it more powerful than the Class 1 devices the SUIT standard specifies as a lower bound. This is not an issue but should be kept in mind as less capable devices are supposed to be able to use an update mechanism complying with SUIT. Furthermore the board supports IEEE 802.15.4 communication in the 2.4 GHz band and SHA2 and RSA hardware acceleration [25].

Chapter 3

Transportation of Firmware Images

3.1 Manifest Format

As the target devices of the update mechanism are constrained IoT devices, the manifest format must be designed with careful consideration. The format must be easy to parse in order to reduce power consumption on devices and be small so that transportation of the manifest is done as quickly as possible, but still contain all necessary information to perform secure updates. This section will present the manifest format which is based on the SUIT specification. It consists of mandatory, always present elements as well as optional elements. The reasoning for splitting it into mandatory and optional elements is to reduce the size of the common case, a singular update for a single MCU, while still allowing more complex updates (such as differential updates or specifying components). The manifest format can be created or generated by some party in JSON, encoded in CBOR for efficient compression, then signed and sent over the network. Preferably the base manifest should fit in a single CoAP message, but the CoAP block option can be used if the manifest adds many options and thus grows.

Subsection 3.1.1 explains the structure of the manifest. Optional elements and their structure are explained in subsection 3.1.2.

3.1.1 Mandatory Elements

The mandatory elements of the manifest should facilitate singular updates for a homogenous device supporting one MCU as this is the simplest use case for secure updates. This use case updates the entire image at once, OS and code, and does not need to care for different storage locations or components. By restricting the mandatory elements to supporting these kinds of updates, the size of the always occuring elements can be reduced.

Different versions of manifests can feature different fields as an update mechanism evolves, therefore the device needs to know what to expect from the manifest. This can be encoded in a **manifest version ID**. Rollback attacks need to be prevented so that old, vulnerable images cannot be applied. They can be mitigated through a **sequence number**. Furthermore the **format** (ELF, binary, etc) and the **size** of the image must be included. **Vendor and class IDs**, possibly **device ID**, must also be included so that the device knows the image is applicable and will work. Lastly, a **digest** of the image must be included so the device can be sure the image has not been tampered with during transport. The **URI** from which the image can be fetched is bundled together with the digest. The manifest structure expressed as a C struct can be seen in Listing 3.1.

Listing 3.1: The mandatory manifest format.

```
struct Manifest {
    int version;
    int sequenceNumber;
    int format;
    int size;
    Condition* condition;
    URIDigest* digest;
    Option* option;
} Manifest;
```

These elements are deemed absolutely necessary and form the very minimum upon which an update mechanism can operate. A manifest containing these and only these elements can be used to perform a singular update for a device containing one MCU and one means of storage (no ambiguity about which components/locations are being updated).

The digests, conditions, and options are nested structures that can possibly be repeated depending on how many digests, conditions, and options are necessary. In order to implement this, each of these structures contain an element which is a pointer to another structure of the same type. This allows a parser to traverse the link of structures, and thus parse several URI/Digest pairs, conditions, or options. Their structures can be seen in Listing 3.2, Listing 3.3, and Listing 3.4 in the next section.

Listing 3.2: The format of URI/digest pairs.

```
struct URIDigest {
    int URILength;
    char* URI;
    char* digest;
    URIDigest* next;
} URIDigest;
```

Listing 3.3: The format of vendor, class, and device ID conditions.

```
struct Condition {
    int type;
    char* UUID;
    Condition* next
} Condition;
```

3.1.2 Options

The options provide additional value to the mechanism, but as the manifest aims to be as small as possible they are not accounted for in the base manifest. Instead they can be optionally included using the options field of the manifest. The included options must be sorted by their option code in ascending order to calculate a delta between the current and preceeding option. This is the way CoAP implements options, and it allows for a smaller amount of bits to encode the option code when the codes get larger. The options and their codes are presented in Table 3.1.

Table 3.1: The optional elements of the manifest and their option codes.

Option Code	Option Name
1	directives (Instruction struct)
2	processingSteps (Instruction struct)
3	URIs (mirrors)
4	component
5	dependencies (URIDigest struct)
6	precursors (URIDigest struct)
7	aliases (URIDigest struct)
8	storage
9	keyDist
10	best-before
11	payload (if small enough)

The option field in the manifest format will contain a list of option structures, each structure consisting of an option delta, option length, option value, and a pointer to the next option as seen in Listing 3.4. As with the mandatory elements, some options consist of nested structs. The dependencies and precursor options list digests of images or parts of images that must be acquired before applying the update, along with their URLs. Aliases lists alternative mirrors for each image that could be used instead. Directives and processingSteps both use a different kind of structure, an Instruction struct, that maps types of instructions to their values. Examples of directives could be whether to install the update right away or just cache the image and install at some later point, and examples of processingSteps could be which decompression algorithm to use. The Instruction struct can be seen in Listing 3.5.

Listing 3.4: The format of the option field.

```
struct Option {
    int delta;
    int length;
    char* value;
    Option* next;
} Option;
```

Listing 3.5: The format of directives or processing steps.

```
struct Instruction {
    int type;
    int value;
    Instruction* next;
} Instruction;
```

3.1.3 Example Manifest

JSON is a human readable and easily modified format. It is easy to convert JSON, which is quite verbose, into CBOR as a more efficient means of encoding the data. CBOR was designed around the same principles and elements as JSON, but is not very readable for humans. For these reasons, the thesis proposes to craft manifests in JSON, then convert into CBOR, and finally sign and send to the device requiring an update. An example manifest could look as in Listing 3.6.

Listing 3.6: An example manifest.

```
{
    "versionID": 1,
    "sequenceNumber": 1,
    "format": 0,
    "size": 512,        // Size of image in bytes
    "conditions": [
        {
            "type": 0,  // UUID5 vendor ID
            "UUID": "74738ff5-5367-5958-9aee-98fffdcd1876"
        },
        {
            "type": 1,  // UUID5 class ID
            "UUID": "74738ff5-5367-5958-9aee-98fffdcd1876"
        }
    ],
    "digests": [
        {
            "URI": "coap://fake.uri/image",
            // Digest of image found on that URI
            "digest": "b924842b4f4212d45ab7e0dc6f570cc9a69a20c925
        }
```

```
        ],
        "options": [
            {
                "delta": 4  // 0 + 4 = 4, option component
                "length": 1,
                "value": 0
            },
            {
                "delta": 6, // 6 + 4 = 10, option best-before
                "length": 10,
                "value": 1548683522
            }
        ]
    }
```

This manifest contains all the mandatory information and two options. There are two conditions telling the vendor and class ID so that the device knows the update is correctly targeted. There is only one URI/digest pair, giving the device the URI to download the image from and the digest to validate the image with. The two options specified are the component and best-before timestamp options. The component option value can for instance map integers to components to be updated, and the best-before timestamp prevents the device from applying the device if that moment in time has been exceeded. The manifest is easy to read but as it is JSON it is unnecessarily verbose. By encoding it in CBOR, which is a binary encoding, it will shrink in size and thus cost less to receive.

Listing 3.7: The first four elements of the example manifest in CBOR encoding.

```
A7                                      # map(7)
   69                                   # text(9)
      76657273696F6E4944                # "versionID"
   01                                   # unsigned(1)
   6E                                   # text(14)
      73657175656E63654E756D626572      # "sequenceNumber"
   01                                   # unsigned(1)
   66                                   # text(6)
      666F726D6174                      # "format"
   00                                   # unsigned(0)
```

```
64                                      # text(4)
   73697A65                             # "size"
19 0200                                 # unsigned(512)
```

Listing 3.7 shows the first four elements of the example manifest when encoded in CBOR. The structure of mapping keys to values is the same, but each element is preceeded by an indication of type and length. This allows for arbitrarily nested elements and indefinite length items. It also allows for a more efficient encoding of elements since if the size is known beforehand, only the required amount of bits can be used instead of preallocating bits and wasting them on shorter items.

The example manifest would be transmitted to a device and then parsed. The parser would divide the manifest into the structures shown in subsections 3.1.1 and 3.1.2. The parsed manifest structure would have an option struct referencing another option struct, meaning the chain is of length 2. The reason for having the nested structs carry a reference to its own type is to make memory allocation easier. While parsing, when the parser detects a new nested struct will be created it can simply allocate that memory and add it in the chain of structs. There is no need to preallocate a large enough block of memory to make sure the structs will fit. Finally, when the manifest is parsed and analyzed, the update itself can take place. This is a topic for the next chapter.

Chapter 4

Updating of Firmware Images

Chapter 5

Evaluation and Results

Chapter 6

Discussion

Bibliography

[1] Peter Jonsson et al. *Ericsson mobility report*. Nov. 2018. URL: https://www.ericsson.com/assets/local/mobility-report/documents/2018/ericsson-mobility-report-november-2018.pdf.

[2] Nicole Perlroth. *Hackers Used New Weapons to Disrupt Major Websites Across U.S.* Oct. 2016. URL: https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html (visited on 01/16/2019).

[3] Alex Hern. *Hacking risk leads to recall of 500,000 pacemakers due to patient death fears*. Aug. 2017. URL: https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update (visited on 01/16/2019).

[4] Syed Ali, Ann Bosche, and Frank Ford. *Cybersecurity Is the Key to Unlocking Demand in the Internet of Things*. Oct. 2018. URL: https://www.bain.com/insights/cybersecurity-is-the-key-to-unlocking-demand-in-the-internet-of-things/ (visited on 12/10/2018).

[5] *Software Updates for Internet of Things (suit)*. URL: https://datatracker.ietf.org/wg/suit/about/ (visited on 01/16/2019).

[6] Jon Postel. *User Datagram Protocol*. RFC 768. Aug. 1980. DOI: 10.17487/RFC0768. URL: https://rfc-editor.org/rfc/rfc768.txt.

[7] Eric Rescorla and Nagendra Modadugu. *Datagram Transport Layer Security Version 1.2*. RFC 6347. Jan. 2012. DOI: 10.17487/RFC6347. URL: https://rfc-editor.org/rfc/rfc6347.txt.

[8] Eric Rescorla and Tim Dierks. *The Transport Layer Security (TLS) Protocol Version 1.2*. RFC 5246. Aug. 2008. DOI: 10.17487/RFC5246. URL: https://rfc-editor.org/rfc/rfc5246.txt.

[9] Zach Shelby, Klaus Hartke, and Carsten Bormann. *The Constrained Application Protocol (CoAP)*. RFC 7252. June 2014. DOI: 10.17487/RFC7252. URL: https://rfc-editor.org/rfc/rfc7252.txt.

[10] Carsten Bormann and Zach Shelby. *Block-Wise Transfers in the Constrained Application Protocol (CoAP)*. RFC 7959. Aug. 2016. DOI: 10.17487/RFC7959. URL: https://rfc-editor.org/rfc/rfc7959.txt.

[11] Peter Van der Stok et al. *EST over secure CoAP (EST-coaps)*. Internet-Draft draft-ietf-ace-coap-est-07. Work in Progress. Internet Engineering Task Force, Jan. 2019. 46 pp. URL: https://datatracker.ietf.org/doc/html/draft-ietf-ace-coap-est-07.

[12] Max Pritikin, Peter E. Yee, and Dan Harkins. *Enrollment over Secure Transport*. RFC 7030. Oct. 2013. DOI: 10.17487/RFC7030. URL: https://rfc-editor.org/rfc/rfc7030.txt.

[13] Carsten Bormann, Mehmet Ersue, and Ari Keränen. *Terminology for Constrained-Node Networks*. RFC 7228. May 2014. DOI: 10.17487/RFC7228. URL: https://rfc-editor.org/rfc/rfc7228.txt.

[14] Brendan Moran et al. *A Firmware Update Architecture for Internet of Things Devices*. Internet-Draft draft-ietf-suit-architecture-02. Work in Progress. Internet Engineering Task Force, Jan. 2019. 22 pp. URL: https://datatracker.ietf.org/doc/html/draft-ietf-suit-architecture-02.

[15] Brendan Moran, Hannes Tschofenig, and Henk Birkholz. *Firmware Updates for Internet of Things Devices - An Information Model for Manifests*. Internet-Draft draft-ietf-suit-information-model-02. Work in Progress. Internet Engineering Task Force, Jan. 2019. 32 pp. URL: https://datatracker.ietf.org/doc/html/draft-ietf-suit-information-model-02.

[16] Microsoft. *The STRIDE Threat Model*. Nov. 2009. URL: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20) (visited on 01/17/2019).

[17] contiki-ng. *Contiki-NG*. 2019. URL: https://github.com/contiki-ng/contiki-ng (visited on 01/18/2019).

[18] contiki-os. *Contiki*. 2018. URL: https://github.com/contiki-os/contiki (visited on 01/18/2019).

[19] Adam Dunkels et al. "Protothreads: Simplifying Event-driven Programming of Memory-constrained Embedded Systems". In: *Proceedings of the 4th International Conference on Embedded Networked Sensor Systems*. SenSys '06. Boulder, Colorado, USA: ACM, 2006, pp. 29–42. ISBN: 1-59593-343-3. DOI: 10.1145/1182807.1182811. URL: http://doi.acm.org/10.1145/1182807.1182811.

[20] contiki-os. *Multithreading*. 2014. URL: https://github.com/contiki-os/contiki/wiki/Multithreading (visited on 01/23/2019).

[21] "IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)". In: *IEEE Std 802.15.4-2003* (2003). DOI: 10.1109/IEEESTD.2003.94389.

[22] M. Kovatsch, S. Duquennoy, and A. Dunkels. "A Low-Power CoAP for Contiki". In: *2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems*. Oct. 2011, pp. 855–860. DOI: 10.1109/MASS.2011.100.

[23] contiki-ng. *TinyDTLS*. 2018. URL: https://github.com/contiki-ng/tinydtls (visited on 01/18/2019).

[24] contiki-ng. *Documentation: CoAP*. 2018. URL: https://github.com/contiki-ng/contiki-ng/wiki/Documentation:-CoAP (visited on 01/23/2019).

[25] *Zolertia Firefly Revision A2 Internet of Things hardware development platform, for 2.4-GHz and 863-950MHz IEEE 802.15.4, 6LoWPAN and ZigBee® Applications*. ZOL-BO001-A2. Revision A2. Zolertia. Dec. 2017.

Appendix A

Appendix Title