OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG FACULTY OF COMPUTER SCIENCE

Communication and Networked Systems

DoRIoT RIOT

Concept for a Web-of-Trust-based certificate management in RIOT OS

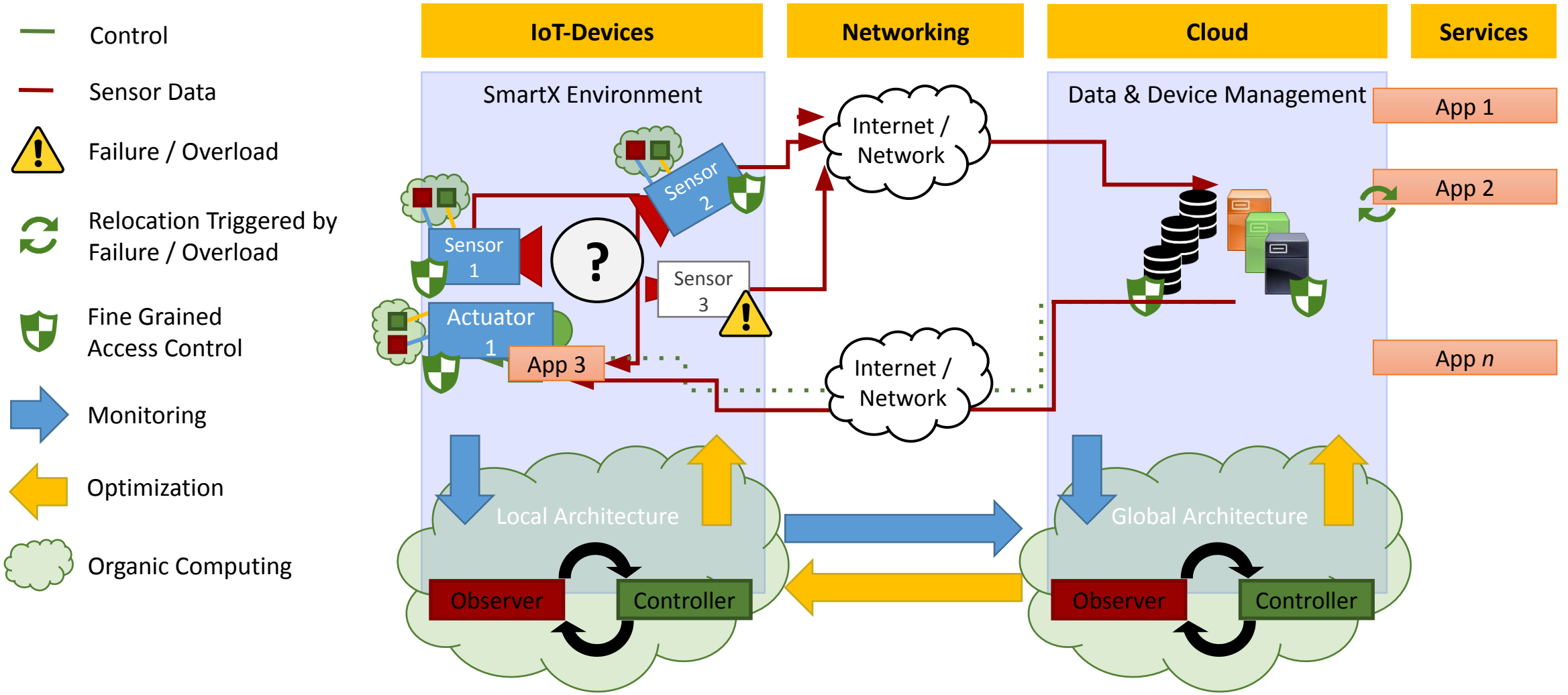
Master Thesis kick off

Presented by
Adarsh Raghoothaman

Contents

- DoRIoT Architecture
- Motivation
- Proposed solution and Scope of thesis
- Thesis plan
- Warm-up task

DoRIoT Architecture



Motivation

- Cloud dependency of IoT platforms
- Cloud interface provides registration and management of devices
- Central management of certificates for authentication can be single-point of failure
- Device management becomes difficult when number of devices are large

Proposed Solution and Scope of thesis

- Decentralized solutions for key management based on Web of Trust(WoT) approach
- Decentralized, hierarchical WoT-topologies are known to reduce the communication overhead in IoT scenarios[1]
- Key management infrastructure do not yet exist for the approach
- Thesis should propose a concept for certificate chain discovery protocol for encryption and authentication
- The implementation should run on RIOT Operating System[2]

Thesis Plan

- Literature review regarding Web of Trust solutions for IoT.
- Specification of a protocol for certificate chain discovery, supporting a hierarchical WoT topology as proposed in [1]. It should be CoAP-based and can make use of CoAP Resource Discovery, or CoAP Resource Directories, as stated in [1].
  Ex-changed certificates should be encoded according to the C509 standard [3]
- Implementation of certificate chain discovery protocol within RIOT.
- Evaluation of solution in terms of communication overhead.
- Discussion of the approach and comparison to Public Key Infrastructure (PKI)

Warm-up Task

Program a tool which converts x509 certificates to c509 standard

- Assumptions
  - encryption is ECDSA
  - extensions are omitted
- Implementation
  - wolfssl library[4] is used to decode x509 certificates in .pem format
  - tiny-cbor[5] is used to encode the certificates to cbor

Warm-up Task

x509 example

```
adarsh@adarsh-SVF15318SNW:~/RIOT/warmup/c509_encoder$ openssl x509 -in wolftest.pem -noout
-text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            08:1a:be:1b:2e:5a:c5:aa:2c:e5:6d:db:20:22:31:b5
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = US, ST = Montana, L = Bozeman, O = Sawtooth, OU = Consulting, CN = www.
wolfssl.com, emailAddress = info@wolfssl.com
        Validity
            Not Before: May  6 21:14:47 2020 GMT
            Not After : Sep 19 21:14:47 2021 GMT
        Subject: C = US, ST = MT, L = Bozeman, O = yourOrgNameHere, OU = yourUnitNameHere,
CN = www.yourDomain.com, emailAddress = yourEmail@yourDomain.com
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:8e:dc:b9:92:59:51:40:2e:3f:33:44:55:70:80:
                    16:bc:41:84:ab:47:3e:8b:93:6a:a0:16:78:0a:e9:
                    49:9a:d5:fe:08:cc:c3:23:2f:26:5a:14:cc:b1:8e:
                    db:94:8d:ad:3c:57:a4:3b:4f:e2:f0:7e:28:33:01:
                    40:57:f0:85:b5
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:localhost, DNS:example.com, DNS:127.0.0.1
    Signature Algorithm: ecdsa-with-SHA256
         30:44:02:20:36:08:d9:df:9e:7f:c2:1c:0c:db:06:26:3d:fe:
         8e:82:6e:64:07:6e:9b:fb:47:97:0a:d0:63:f6:6c:59:2a:82:
         02:20:37:5c:00:eb:0d:7d:95:51:5d:8e:e9:06:c7:a5:6f:7d:
         8b:1d:69:8d:8e:f8:5b:ba:13:0e:2a:5f:b4:86:1b:12
```

Warm-up Task

Field	Value
Version	CBOR int
Serial Number	CBOR byte array
Issuer	Issuer CN as CBOR text string
Validity	UTC time stamp as CBOR unsigned integer
Subject	Subject CN as CBOR text string
Public key	64 byte uncompressed ecPublicKey as CBOR byte string
Signature	ECDSA-Sig-Value ::= SEQUENCE {r INTEGER, s INTEGER} as CBOR byte string

```
adarsh@adarsh-SVF15318SNW:~/RIOT/warmup/c509_encoder$ openssl x509 -in wolftest.pem -noout
-text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            08:1a:be:1b:2e:5a:c5:aa:2c:e5:6d:db:20:22:31:b5
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: C = US, ST = Montana, L = Bozeman, O = Sawtooth, OU = Consulting, CN = www.
wolfssl.com, emailAddress = info@wolfssl.com
        Validity
            Not Before: May  6 21:14:47 2020 GMT
            Not After : Sep 19 21:14:47 2021 GMT
        Subject: C = US, ST = MT, L = Bozeman, O = yourOrgNameHere, OU = yourUnitNameHere,
CN = www.yourDomain.com, emailAddress = yourEmail@yourDomain.com
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:8e:dc:b9:92:59:51:40:2e:3f:33:44:55:70:80:
                    16:bc:41:84:ab:47:3e:8b:93:6a:a0:16:78:0a:e9:
                    49:9a:d5:fe:08:cc:c3:23:2f:26:5a:14:cc:b1:8e:
                    db:94:8d:ad:3c:57:a4:3b:4f:e2:f0:7e:28:33:01:
                    40:57:f0:85:b5
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                DNS:localhost, DNS:example.com, DNS:127.0.0.1
    Signature Algorithm: ecdsa-with-SHA256
         30:44:02:20:36:08:d9:df:9e:7f:c2:1c:0c:db:06:26:3d:fe:
         8e:82:6e:64:07:6e:9b:fb:47:97:0a:d0:63:f6:6c:59:2a:82:
         02:20:37:5c:00:eb:0d:7d:95:51:5d:8e:e9:06:c7:a5:6f:7d:
         8b:1d:69:8d:8e:f8:5b:ba:13:0e:2a:5f:b4:86:1b:12
adarsh@adarsh-SVF15318SNW:~/RIOT/warmup/c509_encoder$
```

```
adarsh@adarsh-SVF15318SNW:~/RIOT/warmup/c509_encoder$ sudo make BOARD=native term
/home/adarsh/RIOT/warmup/c509_encoder/bin/native/c509_encoder.elf /dev/ttyACM0
RIOT native interrupts/signals initialized.
LED_RED_OFF
LED_GREEN_ON
RIOT native board initialized.
RIOT native hardware initialization complete.

main(): This is RIOT! (Version: 2021.10)
x509 CBOR encoder
> cbor_encode wolftest.pem
cbor_encode wolftest.pem
version: 3

serial number: 08:1A:BE:1B:2E:5A:C5:AA:2C:E5:6D:DB:20:22:31:B5

issuer: /C=US/ST=Montana/L=Bozeman/O=Sawtooth/OU=Consulting/CN=www.wolfssl.com/emailAddress
=info@wolfssl.com

not before: 202005062114447Z

not after::202109192114447Z

subject: /C=US/ST=MT/L=Bozeman/O=yourOrgNameHere/OU=yourUnitNameHere/CN=www.yourDomain.com/
emailAddress=yourEmail@yourDomain.com

public key: 04:8E:DC:B9:92:59:51:40:2E:3F:33:44:55:70:80:16:BC:41:84:AB:47:3E:8B:93:6A:A0:1
6:78:0A:E9:49:9A:D5:FE:08:CC:C3:23:2F:26:5A:14:CC:B1:8E:DB:94:8D:AD:3C:57:A4:3B:4F:E2:F0:7E
:28:33:01:40:57:F0:85:B5

signature: 30:44:02:20:36:08:D9:DF:9E:7F:C2:1C:0C:DB:06:26:3D:FE:8E:82:6E:64:07:6E:9B:FB:47
:97:0A:D0:63:F6:6C:59:2A:82:02:20:37:5C:00:EB:0D:7D:95:51:5D:8E:E9:06:C7:A5:6F:7D:8B:1D:69:
8D:8E:F8:5B:BA:13:0E:2A:5F:B4:86:1B:12

c509 cert:880350081ABE1B2E5AC5AA2CE56DDB202231B56F7777772E776F6C6673736C2E636F6D1A5EB328C71
A6147A847727777772E796F7572446F6D61696E2E636F6D5841048EDCB9925951402E3F334455708016BC4184AB
473E8B936AA016780AE9499AD5FE08CCC3232F265A14CCB18EDB948DAD3C57A43B4FE2F07E2833014057F085B55
8403608D9DF9E7FC21C0CDB06263DFE8E826E64076E9BFB47970AD063F66C592A82375C00EB0D7D95515D8EE906
C7A56F7D8B1D698D8EF85BBA130E2A5FB4861B12
>
```

CBOR

Diagnostic → ☐ plain hex

```
[3, h'081ABE1B2E5AC5AA2CE56DDB202231B5', "www.wolfssl.com", 1588799687, 1632086087, "www.yourDomain.com",
h'048EDCB9925951402E3F334455708016BC4184AB473E8B936AA016780AE9499AD5FE08CCC3232F265A14CCB18EDB948DAD3C57A43B4FE2F07E2833014057F085B5',
h'3608D9DF9E7FC21C0CDB06263DFE8E826E64076E9BFB47970AD063F66C592A82375C00EB0D7D95515D8EE906C7A56F7D8B1D698D8EF85BBA130E2A5FB4861B12']
```

← 197 Bytes ☐ as text ☐ utf8 ☐ emb cbor ☐ cborseq

enter hex below or Browse... No file selected.

```
88                                      # array(8)
   03                                   # unsigned(3)
   50                                   # bytes(16)
      081ABE1B2E5AC5AA2CE56DDB202231B5  # "\b\x1A\xBE\e.Z\xC5\xAA,\xE5m\xDB \"1\xB5"
   6F                                   # text(15)
      7777772E776F6C6673736C2E636F6D    # "www.wolfssl.com"
   1A 5EB328C7                          # unsigned(1588799687)
   1A 6147A847                          # unsigned(1632086087)
   72                                   # text(18)
      7777772E796F7572446F6D61696E2E636F6D # "www.yourDomain.com"
   58 41                                # bytes(65)

048EDCB9925951402E3F334455708016BC4184AB473E8B936AA016780AE9499AD5FE08CCC3232F265A14C
CB18EDB948DAD3C57A43B4FE2F07E2833014057F085B5 # "\x04\x8E\xDC\xB9\x92YQ@.?3DUp
\x80\x16\xBCA\x84\xABG>\x8B\x93j\xA0\x16x\n\xE9I\x9A\xD5\xFE\b\xCC\xC3#/&Z\x14\xCC
\xB1\x8E\xDB\x94\x8D\xAD<W\xA4;O\xE2\xF0~(3\x01@W\xF0\x85\xB5"
   58 40                                # bytes(64)

3608D9DF9E7FC21C0CDB06263DFE8E826E64076E9BFB47970AD063F66C592A82375C00EB0D7D95515D8EE
906C7A56F7D8B1D698D8EF85BBA130E2A5FB4861B12 # "6\b\xD9\xDF\x9E\x7F\xC2\x1C\f
\xDB\x06&=\xFE\x8E\x82nd\an\x9B\xFBG\x97\n\xD0c\xF6lY*\x827\\\x00\xEB\r}\x95Q]
\x8E\xE9\x06\xC7\xA5o}\x8B\x1Di\x8D\x8E\xF8[\xBA\x13\x0E*_\xB4\x86\e\x12"
```

FACULTY OF
COMPUTER SCIENCE

Thank you for your attention !

References

1. F. Engelhardt and M. Güneş. Combined Certificate and Resource Discovery for Dynamically (Dis-)Aggregating IoT Processes. In R. H. Reussner, A. Koziolek, and R. Heinrich,editors, INFORMATIK 2020. Gesellschaft für Informatik, Bonn, 2021.
2. RIOT: The friendly Operating System for the Internet of Things. https://www.riot-os.org/
3. J. P. Mattsson, G. Selander, S. Raza, J. Höglund, and M. Furuhed. CBOR Encoded X.509 Certificates (C509 Certificates). Internet-Draft draft-ietf-cose-cbor-encoded-cert-02, Internet Engineering Task Force, July 2021. Work in Progress.
4. WolfSSL Embedded SSL/TLS library. https://doc.riot-os.org/group__pkg__wolfssl.html
5. TinyCBOR library. https://doc.riot-os.org/group__pkg__tinycbor.html
6. Lightweight X.509 Digital Certificates for the Internet of Things: Third International Conference, InterIoT 2017 Filip Forsby, Martin Furuhed, Panos Papadimitratos, and Shahid Raza