Evaluation of DNS over CoAP
Frankfurt a. M., RIOT Summit 2023, 2023-09-18
This Talk is Based on Our Paper

Accepted at CoNEXT’23, will be published in PACMNET:


ArXiv pre-print: https://arxiv.org/abs/2207.07486
Outline

Motivation

Design Guidance from IoT DNS Traffic

DNS over CoAP

DoC RIOT Integration

Evaluation

Conclusion & Next Steps
Motivation

Design Guidance from IoT DNS Traffic

DNS over CoAP

DoC RIOT Integration

Evaluation

Conclusion & Next Steps
Motivation

Attack Scenario

Countermeasure: Encrypt name resolution triggered by IoT devices
Possible Solutions

- DNS over HTTPS (RFC 8484)
- DNS over TLS (RFC 7858)

Our proposal: DNS over CoAP

- Encrypted communication based on DTLS or OSCORE
- Block-wise message transfer to overcome Path MTU problem
- Share system resources with CoAP applications
  - Same socket and buffers can be used
  - Re-use of the CoAP retransmission mechanism
Possible Solutions

- DNS over HTTPS (RFC 8484)
- DNS over TLS (RFC 7858)
- DNS over QUIC (RFC 9250)

Our proposal: DNS over CoAP (https://datatracker.ietf.org/doc/draft-ietf-core-dns-over-coap/)

• Encrypted communication based on DTLS or OSCORE
• Block-wise message transfer to overcome Path MTU problem
• Share system resources with CoAP applications – Same socket and buffers can be used – Re-use of the CoAP retransmission mechanism
Possible Solutions

- DNS over HTTPS (RFC 8484)
- DNS over TLS (RFC 7858)
- DNS over QUIC (RFC 9250)
- DNS over DTLS (RFC 8094)

TCP conflicts with resource constraints
TLS over UDP conflicts with resource constraints
Path MTU problem vs constrained link layer PDUs

Our proposal: DNS over CoAP
(https://datatracker.ietf.org/doc/draft-ietf-core-dns-over-coap/)

- Encrypted communication based on DTLS or OSCORE
- Block-wise message transfer to overcome Path MTU problem
- Share system resources with CoAP applications
  - Same socket and buffers can be used
  - Re-use of the CoAP retransmission mechanism
Possible Solutions

- DNS over HTTPS (RFC 8484)
- DNS over TLS (RFC 7858)
- DNS over QUIC (RFC 9250)
- DNS over DTLS (RFC 8094)

TCP conflicts with resource constraints

- Encrypted communication based on DTLS or OSCP
- Block-wise message transfer to overcome Path MTU problem
- Share system resources with CoAP applications
  - Same socket and buffers can be used
  - Re-use of the CoAP retransmission mechanism
Possible Solutions

- DNS over HTTPS (RFC 8484)
- DNS over TLS (RFC 7858)
- DNS over QUIC (RFC 9250)
- DNS over DTLS (RFC 8094)

TCP conflicts with resource constraints
TLS over UDP conflicts with resource constraints

Our proposal: DNS over CoAP
(https://datatracker.ietf.org/doc/draft-ietf-core-dns-over-coap/)

- Encrypted communication based on DTLS or OSCORE
- Block-wise message transfer to overcome Path MTU problem
- Share system resources with CoAP applications
  - Same socket and buffers can be used
  - Re-use of the CoAP retransmission mechanism
Possible Solutions

- **DNS over HTTPS** (RFC 8484)
- **DNS over TLS** (RFC 7858)
- **DNS over QUIC** (RFC 9250)
- **DNS over DTLS** (RFC 8094)

TCP conflicts with resource constraints

TLS over UDP conflicts with resource constraints

Path MTU problem vs constrained link layer PDUs

Our proposal: DNS over CoAP

- Encrypted communication based on DTLS or OSORE
- Block-wise message transfer to overcome Path MTU problem
- Share system resources with CoAP applications
  - Same socket and buffers can be used
  - Re-use of the CoAP retransmission mechanism
Possible Solutions

Our proposal: DNS over CoAP
(https://datatracker.ietf.org/doc/draft-ietf-core-dns-over-coap/)

- **Encrypted communication** based on DTLS or OSCORE
- **Block-wise message transfer** to overcome Path MTU problem
- **Share system resources** with CoAP applications
  - Same socket and buffers can be used
  - Re-use of the CoAP retransmission mechanism
Outline

Motivation

Design Guidance from IoT DNS Traffic

DNS over CoAP

DoC RIOT Integration

Evaluation

Conclusion & Next Steps
# Data Corpus for IoT DNS Traffic Analysis

## IoT data sets
- **YourThings**:
  - Collected throughout 2019
  - DNS & mDNS (DNS-SD) traffic
  - 90 consumer devices from 50 vendors
  - 0.2 million queries
  - 1.3 million responses
  - 2336 unique queried names
- **IoTFinder**:  
  - Collected throughout 2019
  - DNS & mDNS (DNS-SD) traffic
  - 90 consumer devices from 50 vendors
  - 0.2 million queries
  - 1.3 million responses
  - 2336 unique queried names
- **MonIoTr**:  
  - Collected throughout 2019
  - DNS & mDNS (DNS-SD) traffic
  - 90 consumer devices from 50 vendors
  - 0.2 million queries
  - 1.3 million responses
  - 2336 unique queried names

## IXP data set
- **Large Central European IXP**:  
  - Collected January 2022
  - DNS only
  - Sampling rate: 1/16000 pkts.
  - 1.6 million queries
  - 2.4 million responses
  - Names anonymized to lengths

---

DNS IoT Traffic: Name Lengths

Length of domain names [chars]

<table>
<thead>
<tr>
<th>Data set</th>
<th>min</th>
<th>max</th>
<th>mode</th>
<th>µ</th>
<th>σ</th>
<th>Q₁</th>
<th>Q₂</th>
<th>Q₃</th>
</tr>
</thead>
<tbody>
<tr>
<td>YourThings</td>
<td>2</td>
<td>83</td>
<td>31</td>
<td>24.5</td>
<td>9.7</td>
<td>18</td>
<td>24</td>
<td>30</td>
</tr>
<tr>
<td>IoTFinder</td>
<td>7</td>
<td>82</td>
<td>24</td>
<td>26.8</td>
<td>10.5</td>
<td>20</td>
<td>24</td>
<td>30</td>
</tr>
<tr>
<td>MonIoTr</td>
<td>9</td>
<td>83</td>
<td>18</td>
<td>27.1</td>
<td>14.7</td>
<td>18</td>
<td>23</td>
<td>30</td>
</tr>
<tr>
<td>IoT total</td>
<td>2</td>
<td>83</td>
<td>24</td>
<td>25.9</td>
<td>1.3</td>
<td>19</td>
<td>24</td>
<td>30</td>
</tr>
<tr>
<td>IXP</td>
<td>0</td>
<td>68</td>
<td>17</td>
<td>26.1</td>
<td>1.7</td>
<td>17</td>
<td>25</td>
<td>33</td>
</tr>
</tbody>
</table>
DNS IoT Traffic: Name Lengths

![Histograms of Name Lengths for IoT and IXP]

### Length of Domain Names [chars]

<table>
<thead>
<tr>
<th>Data set</th>
<th>min</th>
<th>max</th>
<th>mode</th>
<th>μ</th>
<th>σ</th>
<th>Q₁</th>
<th>Q₂</th>
<th>Q₃</th>
</tr>
</thead>
<tbody>
<tr>
<td>YourThings</td>
<td>2</td>
<td>83</td>
<td>31</td>
<td>24.5</td>
<td>9.7</td>
<td>18</td>
<td>24</td>
<td>30</td>
</tr>
<tr>
<td>IoTFinder</td>
<td>7</td>
<td>82</td>
<td>24</td>
<td>26.8</td>
<td>10.5</td>
<td>20</td>
<td>24</td>
<td>30</td>
</tr>
<tr>
<td>MonIoTr</td>
<td>9</td>
<td>83</td>
<td>18</td>
<td>27.1</td>
<td>14.7</td>
<td>18</td>
<td>23</td>
<td>30</td>
</tr>
<tr>
<td>IoT total</td>
<td>2</td>
<td>83</td>
<td>24</td>
<td>25.9</td>
<td>1.3</td>
<td>19</td>
<td>24</td>
<td>30</td>
</tr>
<tr>
<td>IXP</td>
<td>0</td>
<td>68</td>
<td>17</td>
<td>26.1</td>
<td>1.7</td>
<td>17</td>
<td>25</td>
<td>33</td>
</tr>
</tbody>
</table>
DNS IoT Traffic: Name Lengths

Length of domain names [chars]

<table>
<thead>
<tr>
<th>Data set</th>
<th>min</th>
<th>max</th>
<th>mode</th>
<th>μ</th>
<th>σ</th>
<th>Q₁</th>
<th>Q₂</th>
<th>Q₃</th>
</tr>
</thead>
<tbody>
<tr>
<td>YourThings</td>
<td>2</td>
<td>83</td>
<td>31</td>
<td>24.5</td>
<td>9.7</td>
<td>18</td>
<td>24</td>
<td>30</td>
</tr>
<tr>
<td>IoTFinder</td>
<td>7</td>
<td>82</td>
<td>24</td>
<td>26.8</td>
<td>10.5</td>
<td>20</td>
<td>24</td>
<td>30</td>
</tr>
<tr>
<td>MonIoTr</td>
<td>9</td>
<td>83</td>
<td>18</td>
<td>27.1</td>
<td>14.7</td>
<td>18</td>
<td>23</td>
<td>30</td>
</tr>
<tr>
<td>IoT total</td>
<td>2</td>
<td>83</td>
<td>24</td>
<td>25.9</td>
<td>1.3</td>
<td>19</td>
<td>24</td>
<td>30</td>
</tr>
<tr>
<td>IXP</td>
<td>0</td>
<td>68</td>
<td>17</td>
<td>26.1</td>
<td>1.7</td>
<td>17</td>
<td>25</td>
<td>33</td>
</tr>
</tbody>
</table>
DNS IoT Traffic: Name Lengths

Length of domain names [chars]

<table>
<thead>
<tr>
<th>Data set</th>
<th>min</th>
<th>max</th>
<th>mode</th>
<th>μ</th>
<th>σ</th>
<th>Q₁</th>
<th>Q₂</th>
<th>Q₃</th>
</tr>
</thead>
<tbody>
<tr>
<td>YourThings</td>
<td>2</td>
<td>83</td>
<td>31</td>
<td>24.5</td>
<td>9.7</td>
<td>18</td>
<td>24</td>
<td>30</td>
</tr>
<tr>
<td>IoTFinder</td>
<td>7</td>
<td>82</td>
<td>24</td>
<td>26.8</td>
<td>10.5</td>
<td>20</td>
<td>24</td>
<td>30</td>
</tr>
<tr>
<td>MonIoTr</td>
<td>9</td>
<td>83</td>
<td>18</td>
<td>27.1</td>
<td>14.7</td>
<td>18</td>
<td>23</td>
<td>30</td>
</tr>
<tr>
<td><strong>IoT total</strong></td>
<td><strong>2</strong></td>
<td><strong>83</strong></td>
<td><strong>24</strong></td>
<td><strong>25.9</strong></td>
<td><strong>1.3</strong></td>
<td><strong>19</strong></td>
<td><strong>24</strong></td>
<td><strong>30</strong></td>
</tr>
<tr>
<td><strong>IXP</strong></td>
<td><strong>0</strong></td>
<td><strong>68</strong></td>
<td><strong>17</strong></td>
<td><strong>26.1</strong></td>
<td><strong>1.7</strong></td>
<td><strong>17</strong></td>
<td><strong>25</strong></td>
<td><strong>33</strong></td>
</tr>
</tbody>
</table>
DNS IoT Traffic: Name Lengths

- IoT names similar to general Internet names
- Long names of \( \approx 24 \) characters typical
  - Cloud service/CDN names (e.g. `e123.abcd.akamaiedge.net`)
  - Compression needed for DoC (via Content-Format)
## DNS IoT Traffic: Record Type

<table>
<thead>
<tr>
<th>Record Type</th>
<th>Queried w/ mDNS</th>
<th>Queried w/o mDNS</th>
<th>Queried IXP</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>53.6%</td>
<td>75.8%</td>
<td>64.5%</td>
</tr>
<tr>
<td>AAAA</td>
<td>16.4%</td>
<td>23.5%</td>
<td>17.6%</td>
</tr>
<tr>
<td>ANY</td>
<td>8.2%</td>
<td>—</td>
<td>1.7%</td>
</tr>
<tr>
<td>HTTPS</td>
<td>—</td>
<td>—</td>
<td>9.1%</td>
</tr>
<tr>
<td>NS</td>
<td>—</td>
<td>—</td>
<td>0.7%</td>
</tr>
<tr>
<td>PTR</td>
<td>19.6%</td>
<td>0.3%</td>
<td>1.8%</td>
</tr>
<tr>
<td>SRV</td>
<td>1.0%</td>
<td>—</td>
<td>0.4%</td>
</tr>
<tr>
<td>TXT</td>
<td>1.2%</td>
<td>0.1%</td>
<td>0.7%</td>
</tr>
<tr>
<td>Other</td>
<td>&lt; 0.1%</td>
<td>0.3%</td>
<td>3.5%</td>
</tr>
</tbody>
</table>
## DNS IoT Traffic: Record Type

<table>
<thead>
<tr>
<th>Queried Record Type</th>
<th>IoT Devices w/ mDNS</th>
<th>IoT Devices w/o mDNS</th>
<th>IXP</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>53.6%</td>
<td>75.8%</td>
<td>64.5%</td>
</tr>
<tr>
<td>AAAA</td>
<td>16.4%</td>
<td>23.5%</td>
<td>17.6%</td>
</tr>
<tr>
<td>ANY</td>
<td>8.2%</td>
<td>—</td>
<td>1.7%</td>
</tr>
<tr>
<td>HTTPS</td>
<td>—</td>
<td>—</td>
<td>9.1%</td>
</tr>
<tr>
<td>NS</td>
<td>—</td>
<td>—</td>
<td>0.7%</td>
</tr>
<tr>
<td>PTR</td>
<td>19.6%</td>
<td>0.3%</td>
<td>1.8%</td>
</tr>
<tr>
<td>SRV</td>
<td>1.0%</td>
<td>—</td>
<td>0.4%</td>
</tr>
<tr>
<td>TXT</td>
<td>1.2%</td>
<td>0.1%</td>
<td>0.7%</td>
</tr>
<tr>
<td>Other &lt; 0.1%</td>
<td>&lt; 0.1%</td>
<td>0.3%</td>
<td>3.5%</td>
</tr>
</tbody>
</table>

Mainly address resolution
### DNS IoT Traffic: Record Type

<table>
<thead>
<tr>
<th>Record Type</th>
<th>Queried w/ mDNS</th>
<th>Queried w/o mDNS</th>
<th>Queried IXP</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>53.6%</td>
<td>75.8%</td>
<td>64.5%</td>
</tr>
<tr>
<td>AAAA</td>
<td>16.4%</td>
<td>23.5%</td>
<td>17.6%</td>
</tr>
<tr>
<td>ANY</td>
<td>8.2%</td>
<td>—</td>
<td>1.7%</td>
</tr>
<tr>
<td>HTTPS</td>
<td>—</td>
<td>—</td>
<td>9.1%</td>
</tr>
<tr>
<td>NS</td>
<td>—</td>
<td>—</td>
<td>0.7%</td>
</tr>
<tr>
<td>PTR</td>
<td>19.6%</td>
<td>0.3%</td>
<td>1.8%</td>
</tr>
<tr>
<td>SRV</td>
<td>1.0%</td>
<td>—</td>
<td>0.4%</td>
</tr>
<tr>
<td>TXT</td>
<td>1.2%</td>
<td>0.1%</td>
<td>0.7%</td>
</tr>
<tr>
<td>Other</td>
<td>&lt; 0.1%</td>
<td>0.3%</td>
<td>3.5%</td>
</tr>
</tbody>
</table>

Mainly address resolution

Also service discovery & information
DNS IoT Traffic: Record Type

<table>
<thead>
<tr>
<th>Record Type</th>
<th>w/ mDNS</th>
<th>w/o mDNS</th>
<th>IXP</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>53.6%</td>
<td>75.8%</td>
<td>64.5%</td>
</tr>
<tr>
<td>AAAA</td>
<td>16.4%</td>
<td>23.5%</td>
<td>17.6%</td>
</tr>
<tr>
<td>ANY</td>
<td>8.2%</td>
<td>—</td>
<td>1.7%</td>
</tr>
<tr>
<td>HTTPS</td>
<td>—</td>
<td>—</td>
<td>9.1%</td>
</tr>
<tr>
<td>NS</td>
<td>—</td>
<td>—</td>
<td>0.7%</td>
</tr>
<tr>
<td>PTR</td>
<td>19.6%</td>
<td>0.3%</td>
<td>1.8%</td>
</tr>
<tr>
<td>SRV</td>
<td>1.0%</td>
<td>—</td>
<td>0.4%</td>
</tr>
<tr>
<td>TXT</td>
<td>1.2%</td>
<td>0.1%</td>
<td>0.7%</td>
</tr>
<tr>
<td>Other</td>
<td>&lt; 0.1%</td>
<td>0.5%</td>
<td>3.5%</td>
</tr>
</tbody>
</table>

- Name resolution should be favored by DoC
- Group OSCORE may offer solution for encrypted DNS-SD
- Unsolicited NS records increase response size ⇒ Should be avoided with DoC
Outline

Motivation

Design Guidance from IoT DNS Traffic

DNS over CoAP

DoC RIOT Integration

Evaluation

Conclusion & Next Steps
DNS over CoAP (DoC)

• Just map the DoH methods **GET** and **POST**?
DNS over CoAP (DoC)

- Just map the DoH methods **GET** and **POST**?

<table>
<thead>
<tr>
<th>HTTP</th>
<th>GET</th>
<th>POST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cacheable</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Application data carried in body</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Block-wise transferable query</td>
<td>✗</td>
<td>✓</td>
</tr>
</tbody>
</table>
DNS over CoAP (DoC)

- Just map the DoH methods **GET** and **POST**?
- **FETCH** method in CoAP: best of both worlds (RFC 8132)

<table>
<thead>
<tr>
<th></th>
<th>HTTP</th>
<th>CoAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>POST</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>FETCH</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

- Cacheable
- Application data carried in body
- Block-wise transferable query
DNS over CoAP (DoC)

- Just map the DoH methods **GET** and **POST**?
- **FETCH** method in CoAP: best of both worlds (RFC 8132)

<table>
<thead>
<tr>
<th>CoAP</th>
<th>HTTP</th>
<th>GET</th>
<th>POST</th>
<th>FETCH</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Cacheable
Application data carried in body
Block-wise transferable query

---

**FETCH request**

**DoC Client**

**CoAP response**

**DoC Server**

**DNS Infrastructure**

**DNS over CoAP**

**DNS over UDP/HTTPS/QUIC/...**
Outline

Motivation

Design Guidance from IoT DNS Traffic

DNS over CoAP

DoC RIOT Integration

Evaluation

Conclusion & Next Steps
DoC RIOT Integration

Application / Library

- dns_query
- dns_msg / dns_cache

DNS over UDP
(sock_dns)

DNS over CoAP
(gcoap_dns)

- gcoap
- nanocoap

DNS over DTLS
(sock_dodtls)

sock (sync. / async.)

sock_dtls
sock_udp

netapi

GNRC

Alternative Network Stacks
DoC RIOT Integration

**Application / Library**
- dns_query
- DNS over UDP (sock_dns)
- DNS over CoAP (gcoap_dns)
- DNS over DTLS (sock_dodtls)
- dns_msg / dns_cache

**sock (sync. / async.)**
- sock_dtls
- sock_udp

**netapi**
- GNRC

**Alternative Network Stacks**
Outline

Motivation

Design Guidance from IoT DNS Traffic

DNS over CoAP

DoC RIOT Integration

Evaluation

Conclusion & Next Steps
Evaluation Setup: DNS Transport Comparison

Name properties: Based on empirically measured data from IoT devices

Testbed experiments:

- Clients query 50 A or AAAA records for names of length 24 chars via DNS over UDP / DTLSv1.2 / CoAP (unencrypted) / CoAPsv1.2 / OSCORE
- Poisson distribution: $\lambda = 5$ queries / sec (ignoring NSTART=1 requirements)
- 10 runs on IoT-nodes (incl. BR): Cortex-M3 with IEEE 802.15.4 radio
Experiment: Resolution Time

DNS Transports
- UDP
- DTLSv1.2
- OSCORE
- CoAP
- CoAPSv1.2

CoAP Methods
- POST
- GET
- FETCH

CDF
A record
AAAA record

Resolution time [s]
0.0
0.5
1.0
Resolution time [s]
0.0
10
20
30
40
Resolution time [s]
0.0
10
20
30
40
Resolution time [s]
0.0
10
20
30
40
Resolution time [s]
0.0
10
20
30
40
Resolution time [s]
0.0
10
20
30
40
Resolution time [s]
0.0
10
20
30
40
Resolution time [s]
Experiment: Resolution Time

DNS Transports
- UDP
- CoAPv1.2
- DTLSv1.2
- OSCORE
- CoAP

CoAP Methods
- POST
- GET
- FETCH

A record
AAAA record

Resolution time [s]

CDF

0.0
0.5
1.0

Resolution time [s]

Clear performance groupings visible
Experiment: Resolution Time

DNS Transports
- UDP

A record

AAAA record

CDF

Resolution time [s]

Frame Size [bytes]

UDP
DTLSv1.2
CoAP
CoAPSv1.2
OSCORE

CoAP Methods
- POST
- GET
- FETCH

Packet size

L2 max. frame size

Group 1
Experiment: Resolution Time

- DNS Transports
  - UDP
  - CoAP

- CoAP Methods
  - POST
  - FETCH

A record

AAAA record

CDF

Resolution time [s]

Group 2
Experiment: Resolution Time

DNS Transports
- CoAPSv1.2
- DTLSv1.2
- OSCORE
- CoAP

CoAP Methods
- POST
- GET
- FETCH

A record

AAAA record

CDF

Resolution time [s]

Group 3
Experiment: Resolution Time

Where do performance groups come from?

DNS Transports
- UDP
- CoAPSv1.2
- DTLSv1.2
- OSCORE
- CoAP

CoAP Methods
- ----- POST
- ------ GET
- ----- FETCH

A record

AAAA record

CDF
Resolution time [s]
Experiment: Resolution Time & Packet Sizes

DNS Transports
- UDP
- CoAPSv1.2
- DTLSv1.2
- OSCORE
- CoAP

CoAP Methods
- POST
- GET
- FETCH

A record

AAAA record

CDF

Resolution time [s]

Frame Size [bytes]

Packet size

L2 max. frame size

UDP

Query [F/P]  Query [G]  Resp. (A)   Resp. (AAAA)

Resolution time [s]

Frame Size [bytes]
Experiment: Resolution Time & Packet Sizes

DNS Transports
- UDP

CoAP Methods

A record
AAAA record

CDF

Resolution time [s]

0.0 0.5 1.0

0 10 20 30 40

Frame Size [bytes]

UDP

0 32 64 96 128 160 192

Query [F/P] Query [G] Resp. (A) Resp. (AAAA)

Group 1
No message fragmentation
Experiment: Resolution Time & Packet Sizes

DNS Transports
- UDP
- CoAP

CoAP Methods
- POST
- FETCH

A record

AAAA record

CDF

Resolution time [s]

Packet size

Frame Size [bytes]

UDP

CoAP

Group 2
Query unfragmented
Response fragmented
Experiment: Resolution Time & Packet Sizes

DNS Transports
- CoAPSv1.2
- DTLSv1.2
- OSCORE
- CoAP

CoAP Methods
- POST
- GET
- FETCH

A record
AAAA record

CDF

Resolution time [s]

Frame Size [bytes]

DNS Transports
- UDP
- DTLSv1.2
- CoAP
- CoAPSv1.2
- OSCORE

CoAP Methods
- POST
- GET
- FETCH

Query [F/P]
Query [G]
Resp. (A)
Resp. (AAAA)

Packet size
L2 max. frame size

Group 3
Both messages fragmented
Experiment: Resolution Time & Packet Sizes

- Fragmentation has larger impact on performance compared to transport or CoAP method

**CDF**
- A record
- AAAA record

**Frame Size [bytes]**
- UDP
- DTLSv1.2
- CoAP
- CoAPSv1.2
- OSCORE

**CoAP Methods**
- POST
- GET
- FETCH

⇒ Fragmentation has larger impact on performance compared to transport or CoAP method
Memory Consumption

- **DNS over OSCORE:**
  - Smallest ROM footprint when CoAP already present
  - Only half as much ROM as DTLS

- **DoC optimization:**
  - Abstract option handling in CoAP?

Evaluation of DNS over CoAP
Chair of Distributed and Networked Systems // M.S. Lenders
Frankfurt a. M., RIOT Summit '23
Folie 18 von 21
- DNS over OSCORE:
  - Smallest ROM footprint when CoAP already present
  - Only half as much ROM as DTLS
- DoC optimization: Abstract option handling in CoAP?
Outline

Motivation

Design Guidance from IoT DNS Traffic

DNS over CoAP

DoC RIOT Integration

Evaluation

Conclusion & Next Steps
Conclusion & Next Steps

• DoC with FETCH provides encrypted DNS for constrained IoT
  – Segmentable with block-wise transfer
  – En-route caching at CoAP proxies
• OSCORE outperforms CoAPS both in packet and build size
• Next:
  – Concise and compressed DNS message format (draft-lenders-dns-cbor)
  – mDNS protection with Group OSCORE?
Reproducible Research: Our Artifacts

• https://zenodo.org/record/8193681
• https://github.com/anr-bmbf-pivot/Artifacts-CoNEXT23-DoC