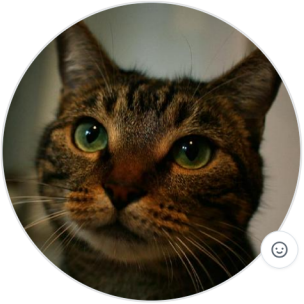
The D in sock_tls stands for Datagram

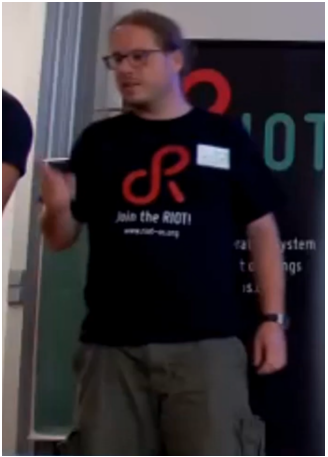
Jakob Hermanowski
Frankfurt University of Applied Sciences
jakob@jhermanowski.de
September 3, 2026

Who am I?

Repositories 31 Projects Packages



jhermanowski
jhermanowski



Agenda

FRANKFURT UNIVERSITY OF APPLIED SCIENCES

DTLS in RIOT

TLS in RIOT

My work on DTLS

Future work

Recap: What is DTLS?

Datagram Transport Layer Security

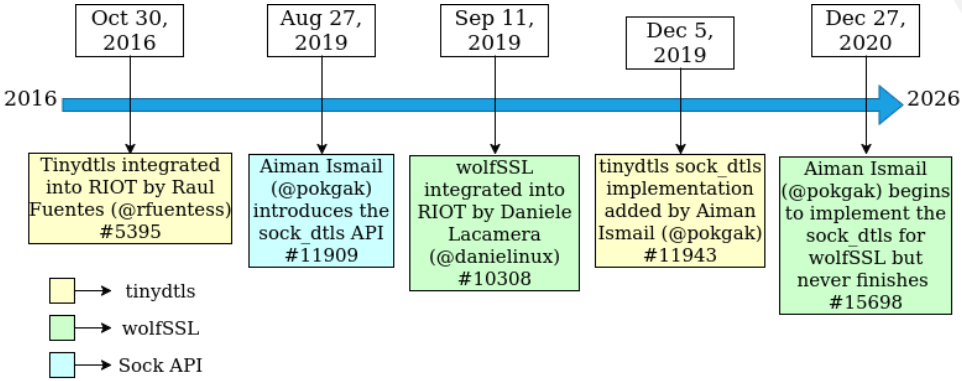
TLS adapted for **UDP** (instead of TCP)

Often preferred in IoT

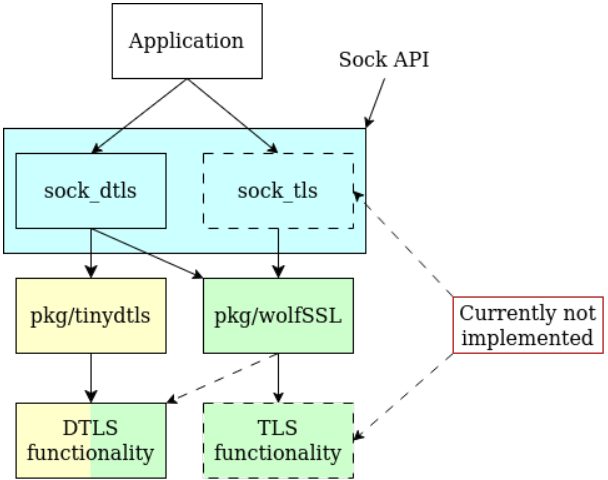


Cynthia Lee

DTLS in RIOT


Oct 30, 2016
Aug 27, 2019
Sep 11, 2019
Dec 5, 2019
Dec 27, 2020
2016
2026
Tinydtls integrated into RIOT by Raul Fuentes (@rfuentess) #5395
Aiman Ismail (@pokgak) introduces the sock_dtls API #11909
wolfSSL integrated into RIOT by Daniele Lacamera (@danielinux) #10308
tinydtls sock_dtls implementation added by Aiman Ismail (@pokgak) #11943
Aiman Ismail (@pokgak) begins to implement the sock_dtls for wolfSSL but never finishes #15698
tinydtls
wolfSSL
Sock API

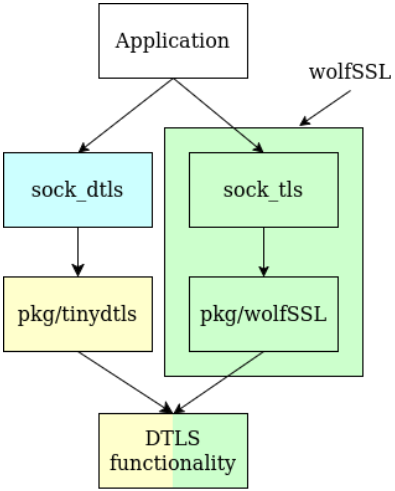
DTLS in RIOT in the future



DTLS in RIOT currently

sock_dtls is only implemented for tinydtls

wolfSSL has the module sock_tls, that provides DTLS functionality



Agenda

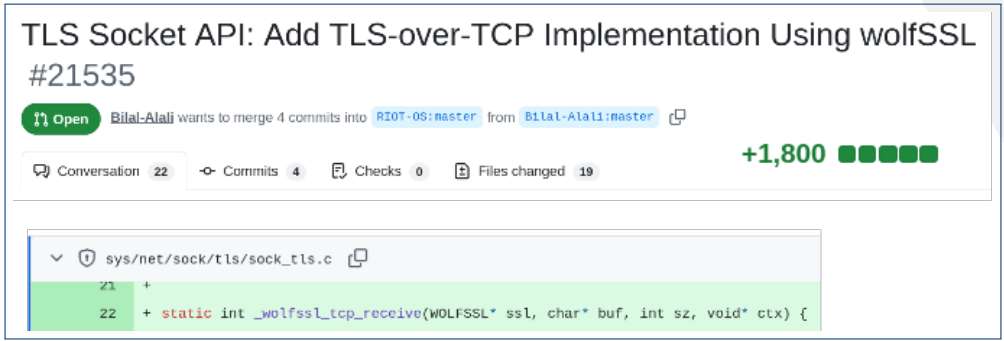
DTLS in RIOT

TLS in RIOT

My work on DTLS

Future work

Existing TLS pull request

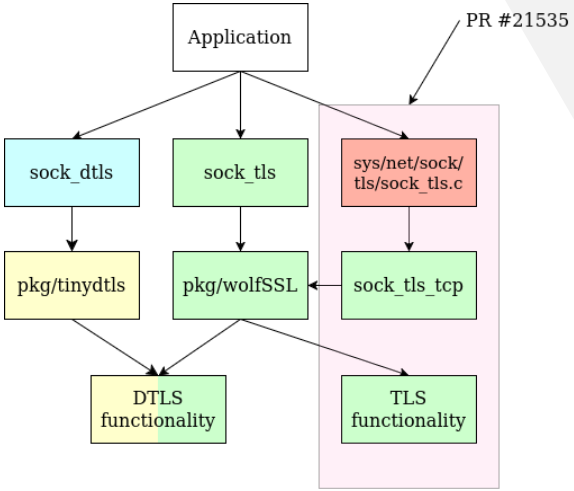


AWS IoT core and Azure IoT Hub require TLS

Existing TLS pullrequest

Implementation-specific code in generic sys/net/sock

sock_tls API does not exist



Cleaning up

- ☐ Change naming scheme for wolfSSL
- ☐ Implementing sock_dtls for wolfSSL



Agenda

DTLS in RIOT

TLS in RIOT

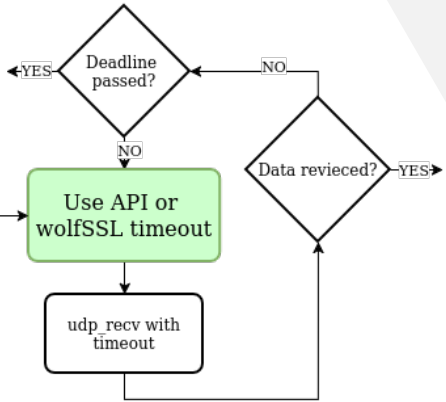
My work on DTLS

Future work

Design choices - Timeouts

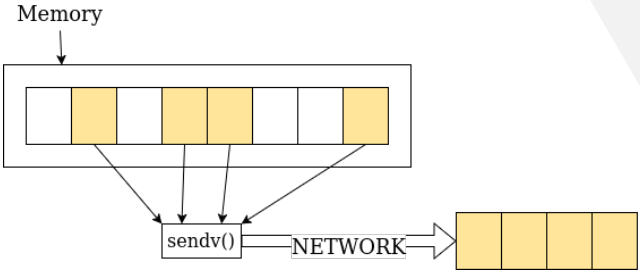
WolfSSL UDP receive callback:

```
if (wolfSSL_timeout < api_timeout) {
    timeout = wolfSSL_timeout;
}
```



Design choices - Vectored I/O

WolfSSL does not support vectored I/O



Design choices - Nonblocking

FRANKFURT UNIVERSITY OF APPLIED SCIENCES

We force wolfSSL to only send the ClientHello to respect the API specification

```
wolfSSL_set_using_nonblock(remote->ssl, 1);
ret = wolfSSL_connect(remote->ssl);
wolfSSL_set_using_nonblock(remote->ssl, 0);
```

Agenda

DTLS in RIOT

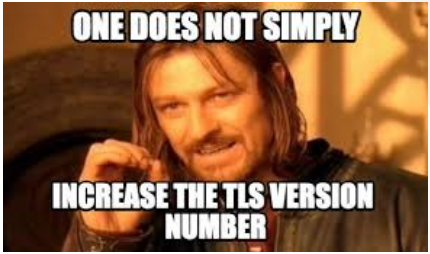
TLS in RIOT

My work on DTLS

Future work

Future work

- ☐ Revisiting the sock_dtls API specification
- ☐ Enabling DTLS 1.3
- ☐ Introducing sock_tls API
- ☐ Implementing sock_tls API for wolfSSL



TLS 1.3 - Eric Rescorla

Questions



You made it to the end!