SWORN: Secure Wake on Radio Nudging
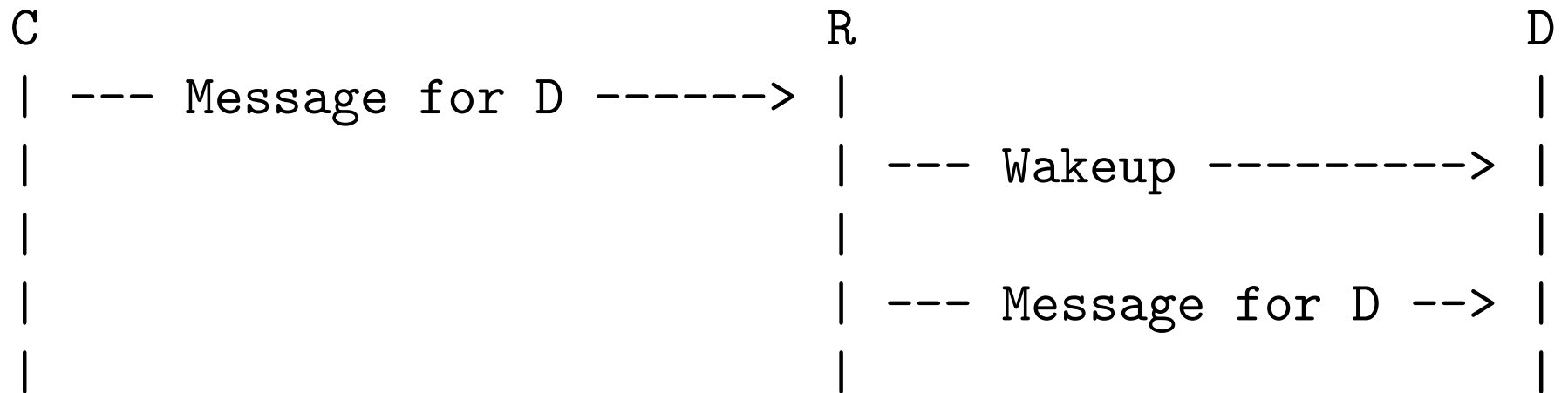
draft-bormann-t2trg-sworn

Olaf Bergmann, Carsten Bormann, Benjamin Piepiora

Hackathon @IETF99, 2017-07-16, Prague
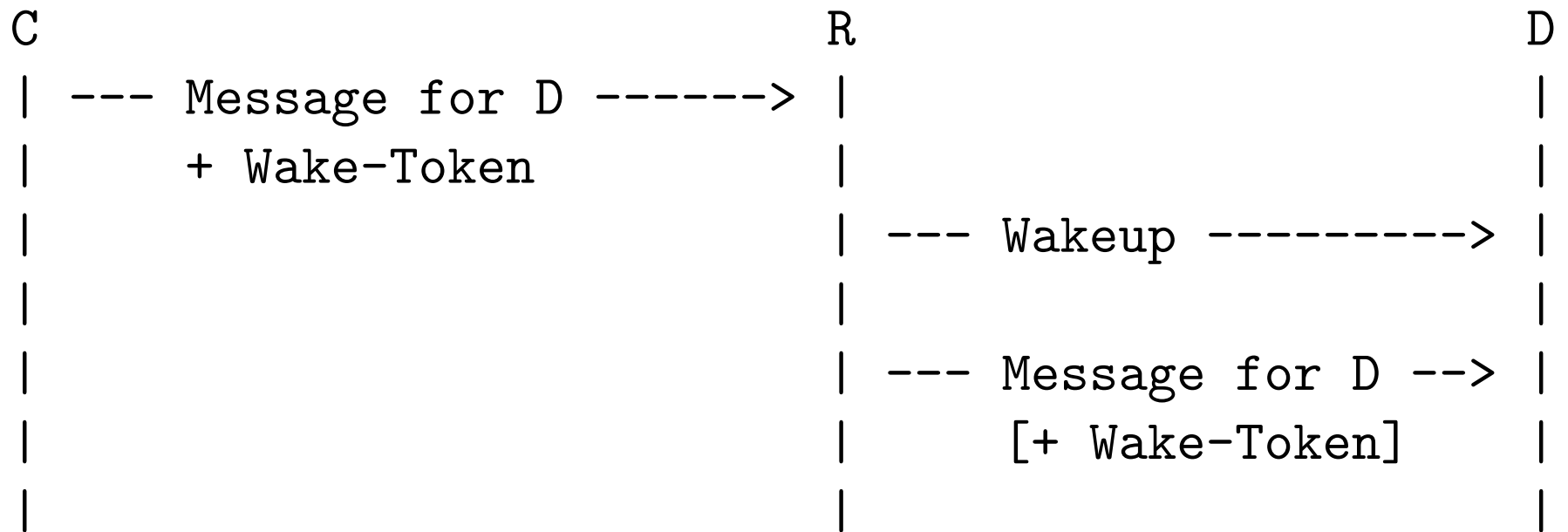
Universität Bremen

lemonbeat

Basic Scenario

```
  C                                     R                         D
  | --- Message for D ------> |                                   |
  |                           | --- Wakeup ---------> |
  |                           |                                   |
  |                           | --- Message for D --> |
  |                           |                                   |
```

- ▶ Last-mile router R wakes device D before message is forwarded
- ▶ When connected to the Internet, only authorized messages
  should cause a wakeup

Authorizing The Wakeup

```
C                                          R                           D
|  --- Message for D ------> |                           |
|       + Wake-Token          |                           |
|                             | --- Wakeup ---------> |
|                             |                           |
|                             | --- Message for D --> |
|                             |       [+ Wake-Token]     |
|                             |                           |
```

- ▶ C retrieves grant (CWE) from D's overseeing principal
- ▶ C forms authorization token (CWS) with grant key and wakeup information
- ▶ R inspects messages for valid SWORN tokens before and drops not authorized messages

Results

Demonstrator:

- ▶ **DONE:** C adds CoAP header and Wake-Token option
- ▶ **DONE:** R checks for SWORN tag and unpacks Wake-Token
- ▶ **DONE:** drop unauthorized messages
- ▶ **DONE:** remove CoAP header when forwarding
- ▶ in progress: open-source RFC 8152 ruby gem for CWT etc.