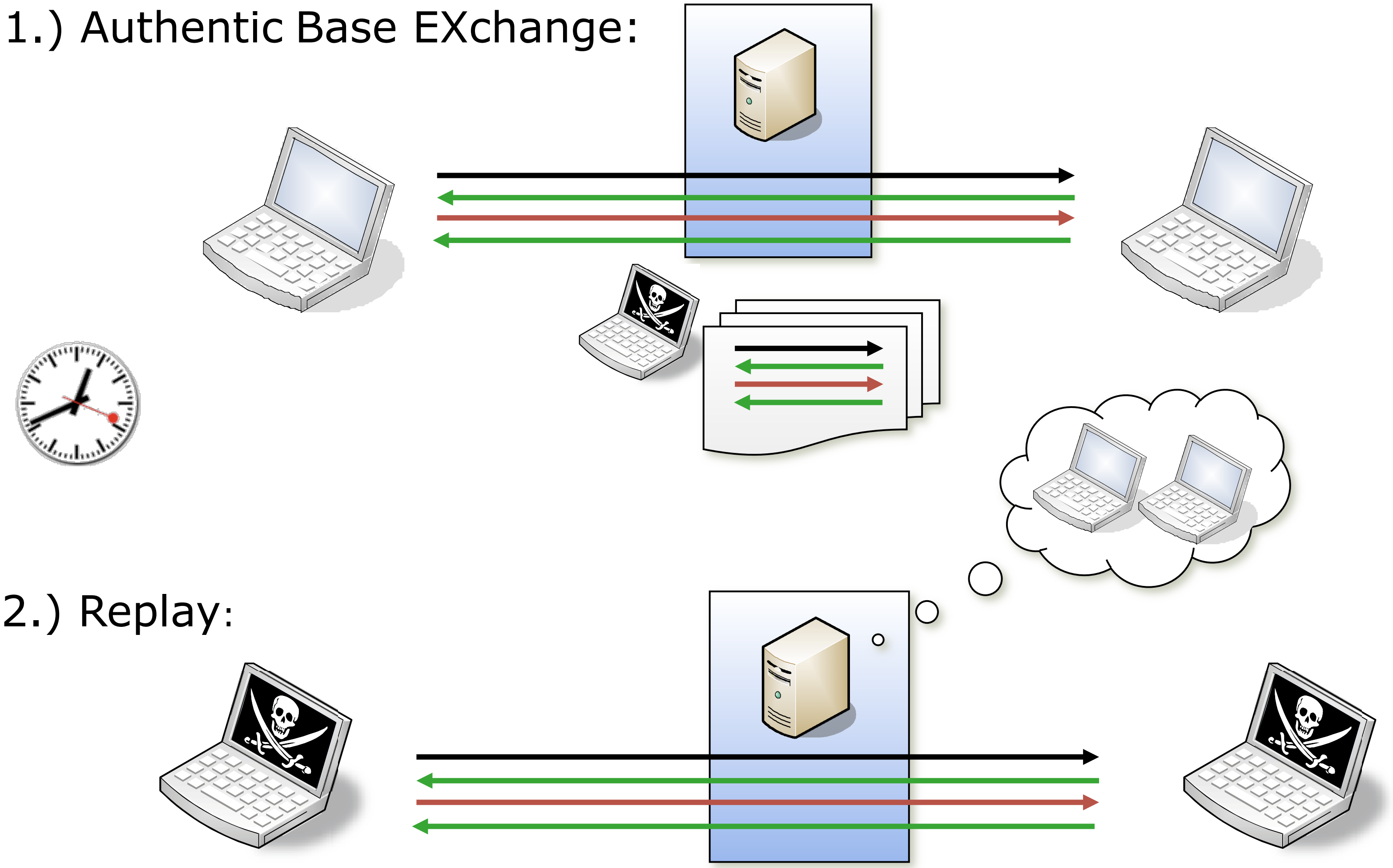
Update draft-hip-heer-middle-auth-04

Tobias Heer, René Hummen,
Miika Komu, Klaus Wehrle

Recap: Replay Attack

1.) Authentic Base EXchange:

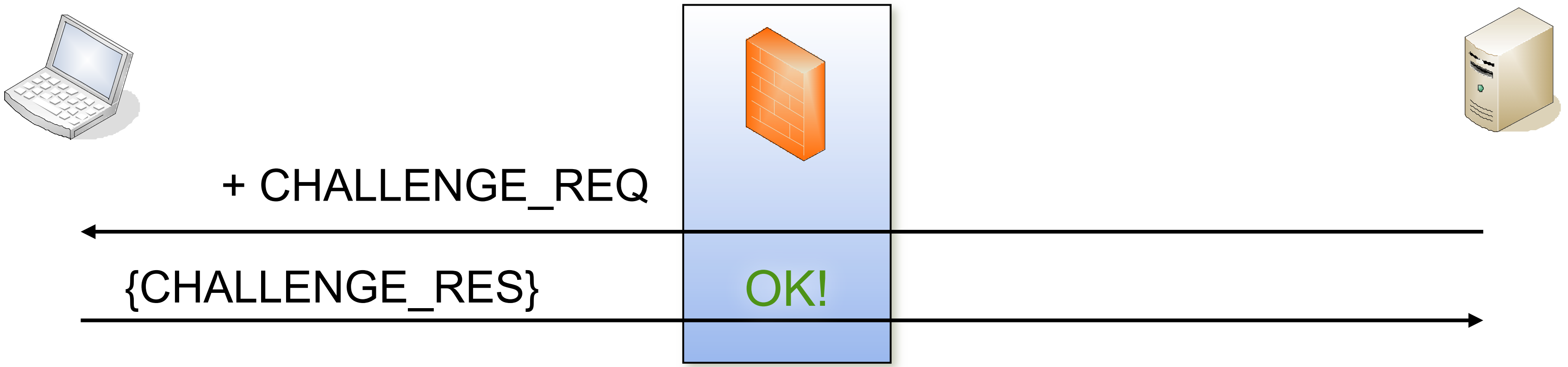


2.) Replay:

Recap: What’s the Problem?

- Everyone can replay a BEX
  - – No knowledge of private key needed
- Only end-to-end freshness in BEX
  - – Middleboxes can’t verify freshness of BEX

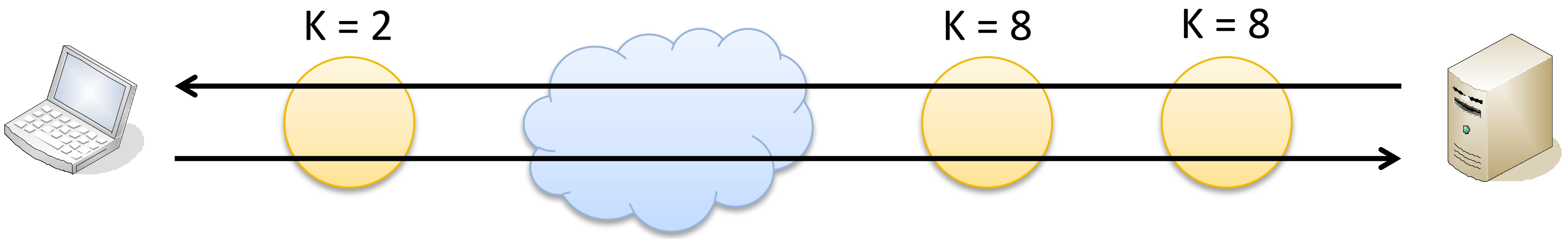
Proposed solution:



Changes Since Version 02

- Single solution for multiple middlebox challenges
  - New CHALLENGE_RESPONSE parameter layout
- Authentication of the CLOSE exchange
- Addressing of packet space restrictions
- Editorial changes

Problems with Multiple Middleboxes



- Middleboxes add own CHALLENGE_REQUEST
- End-host has to compute multiple solutions
- Exceeding packet sizes
  - CHALLENGE_RESPONSE = CHALLENGE_REQUEST + puzzle solution

Compute Single Puzzle Solution

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Type              |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| K, 1 byte     |   Lifetime    |                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               /
/                                                               /
/                   Opaque, (variable length)                   /
/                                       +-+-+-+-+-+-+-+-+-+-+-+-|
/                                       |         Padding       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

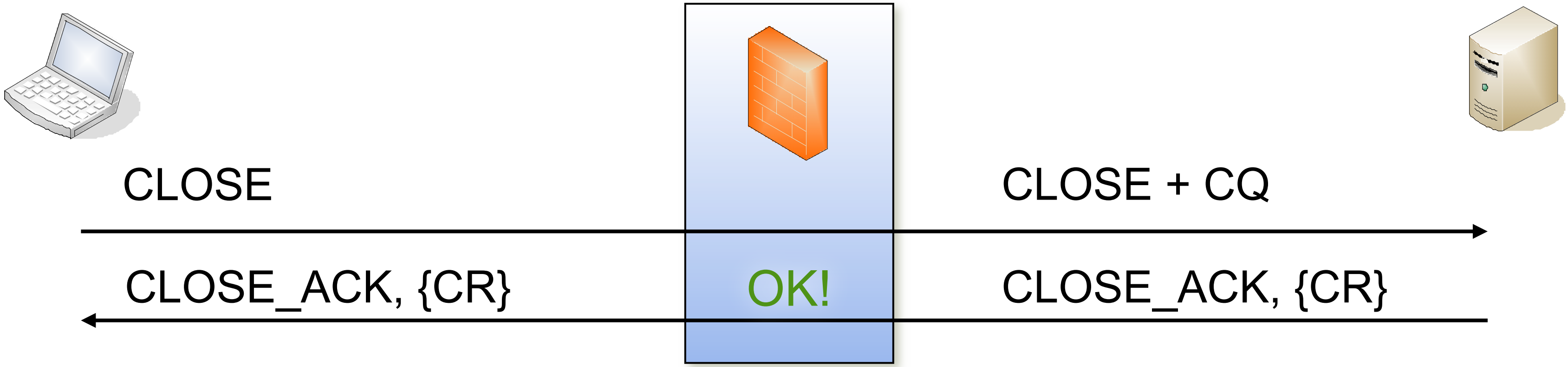
CHALLENGE_REQUEST

- Puzzle seed derivation
  - Concatenation of received opaque values
- Puzzle difficulty: max(K_i)
- Puzzle Lifetime: min(Lifetime_i)

New CHALLENGE_RESPONSE Layout

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            Type               |            Length             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| K, 1 byte     |   Lifetime    |      No. opaque values        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                  Puzzle solution #J, 8 bytes                  /
/                                                               /
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Opaque length         |        Opaque length          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                  Opaque, (variable length)                    /
/                                   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                                   |                           /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                           /
/                  Opaque, (variable length)                    /
/                         +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
/                         |              Padding                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Authentication of CLOSE



- Authentication of one peer suffices
  - Exchange freshness ✔
  - Replayed CLOSE dropped by peer
- Inclusion of HOST_IDs not required
  - Permit, but rate limit CLOSE if HIs unknown

Status Update of the Mobile ACcess Project

Tobias Heer, René Hummen, Hanno Wirtz,
Nicolai Viol, Klaus Wehrle

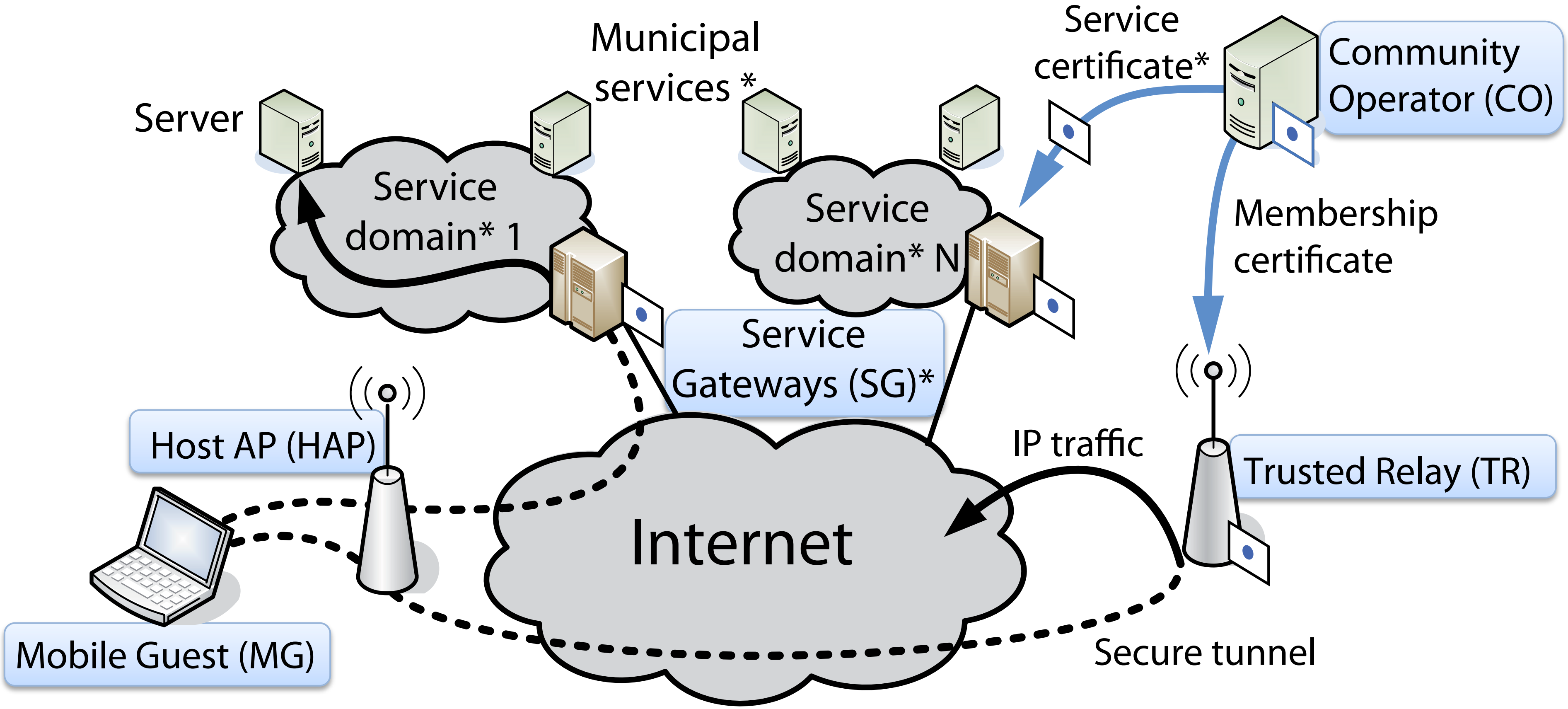
Chair of Communication and Distributed Systems

RWTH Aachen University

Recap: Project Goals

- Concept for ubiquitous Wi-Fi access in the cities of Aachen and Monschau
- Collaborative network with private participation (Wi-Fi sharing as basis)
  - Security and mobility → HIP
- Location-aware services

Basic Network Architecture

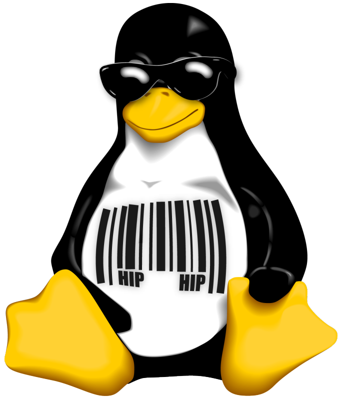


Preliminary Results

- Full implementation with testbed at the chair
  - Concept feasibility
- Collaboration through use of private APs
  - Good coverage and reachability
  - Limited uplink not problematic
- HIP abstracts nicely from network dynamics and patchwork characteristics

Release of HIPL v1.0.6

- Improved stability and robustness
- Optimized handovers
- Implemention of draft-hip-heer-middle-auth



Small **demo**

… at the next power plug near you