draft-heer-hip-midauth-01.txt

Tobias Heer[*], Miika Komu[+],
Klaus Wehrle[*]

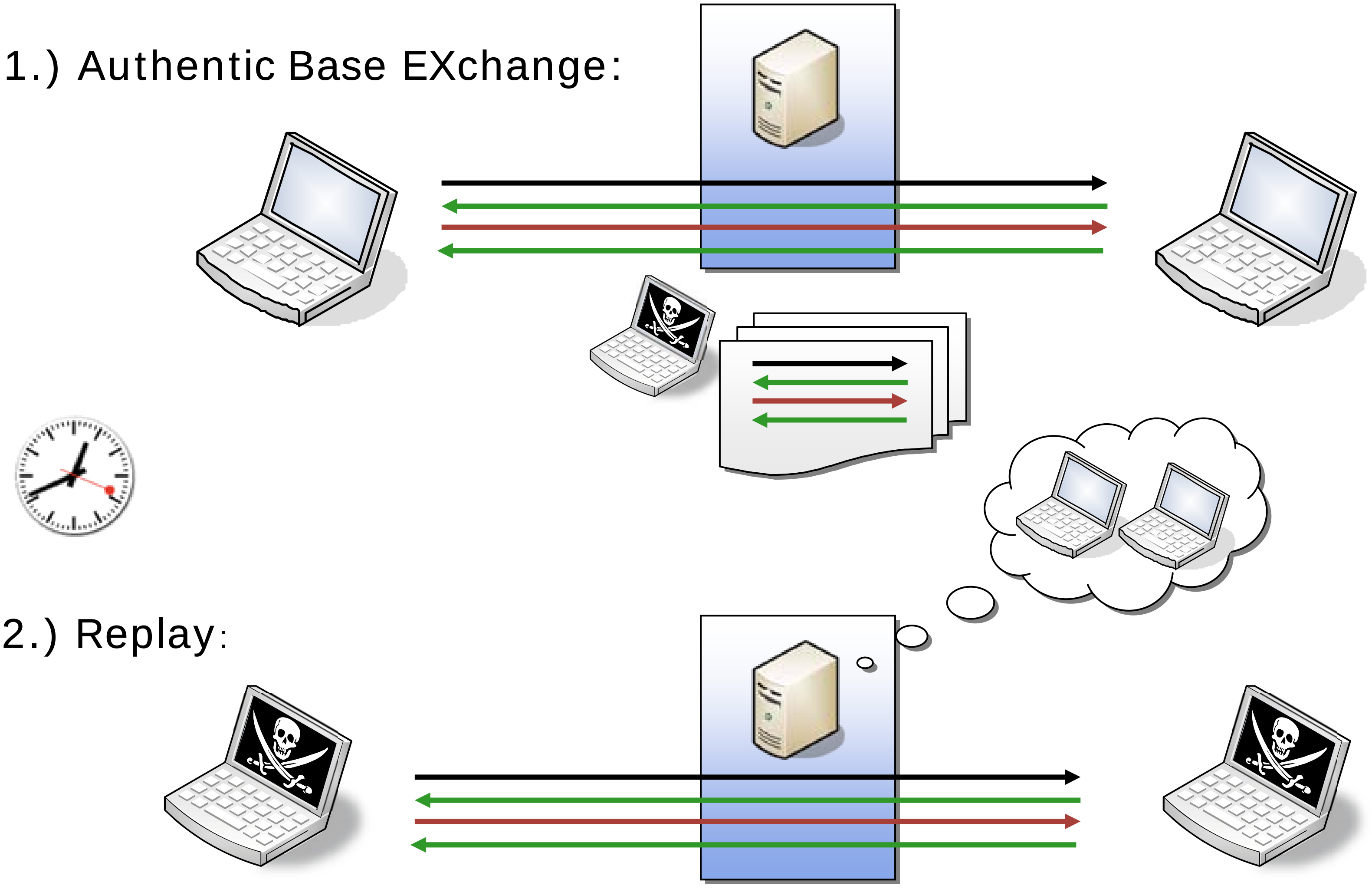
*) Distributed Systems Group
RWTH Aachen University, Aachen, Germany
http://ds.cs.rwth-aachen.de

+) HIIT
Helsinki, Finland
http://www.hiit.fi

HI Verification by Middleboxes

- Middleboxes need to be able to verify host identities
  - Firewalls, intrusion detection, logging
  - Accounting
  - Access control / Certificates
  - Peer-to-Peer systems
- General functionality partially provided by BEX
  - E.g., RSA/DSA signatures in control packets
- Mechanism prone to replay attacks

Replay Attack



1.) Authentic Base EXchange:

2.) Replay:

What‘s the Problem?

- Everyone can replay a BEX
  - No knowledge of private key needed
- Middleboxes can‘t verify freshness of BEX
  - No timestamp (and that‘s good)
- No signed IP Addresses
  - No src/dst IP addresses covered by signature (and that‘s good)
- End-host nonces are useless to middleboxes

How Severe is the Problem?

- Only relevant to middleboxes
- Full impersonation towards the middlebox
- Attack can be launched...
- … by any one
    - No special knowledge necessary
- … at any time
    - No temporal restrictions
- ... from anywhere
    - No spatial restrictions (IPs)
- ... towards any middlebox
    - A BEX/UPDATE can be replayed to different middleboxes

draft-heer-hip-middle-auth

- Scope
  - MB that authenticate packets/hosts „on the fly“
  - No explicit registration
  - No explicit middlebox detection
- Support for authentication by middlebox during
  - BEX
  - Mobility signaling
- Protection from DoS on middlebox

Authentication Mechanism

- Let MB „participate“ in BEX, UPDATE
- MB injects parameters to HIP control packets
- Challenge - response
  - Pretty much like ECHO_REQUEST / RESPONSE
- ECHO_REQUEST_M, ECHO_RESPONSE_M
  - Middlebox adds ER_M parameter to control packet
  - Receiving host echoes parameter in **signed part** of response packet
- DoS protection for middleboxes
  - Puzzle mechanism

New Parameters

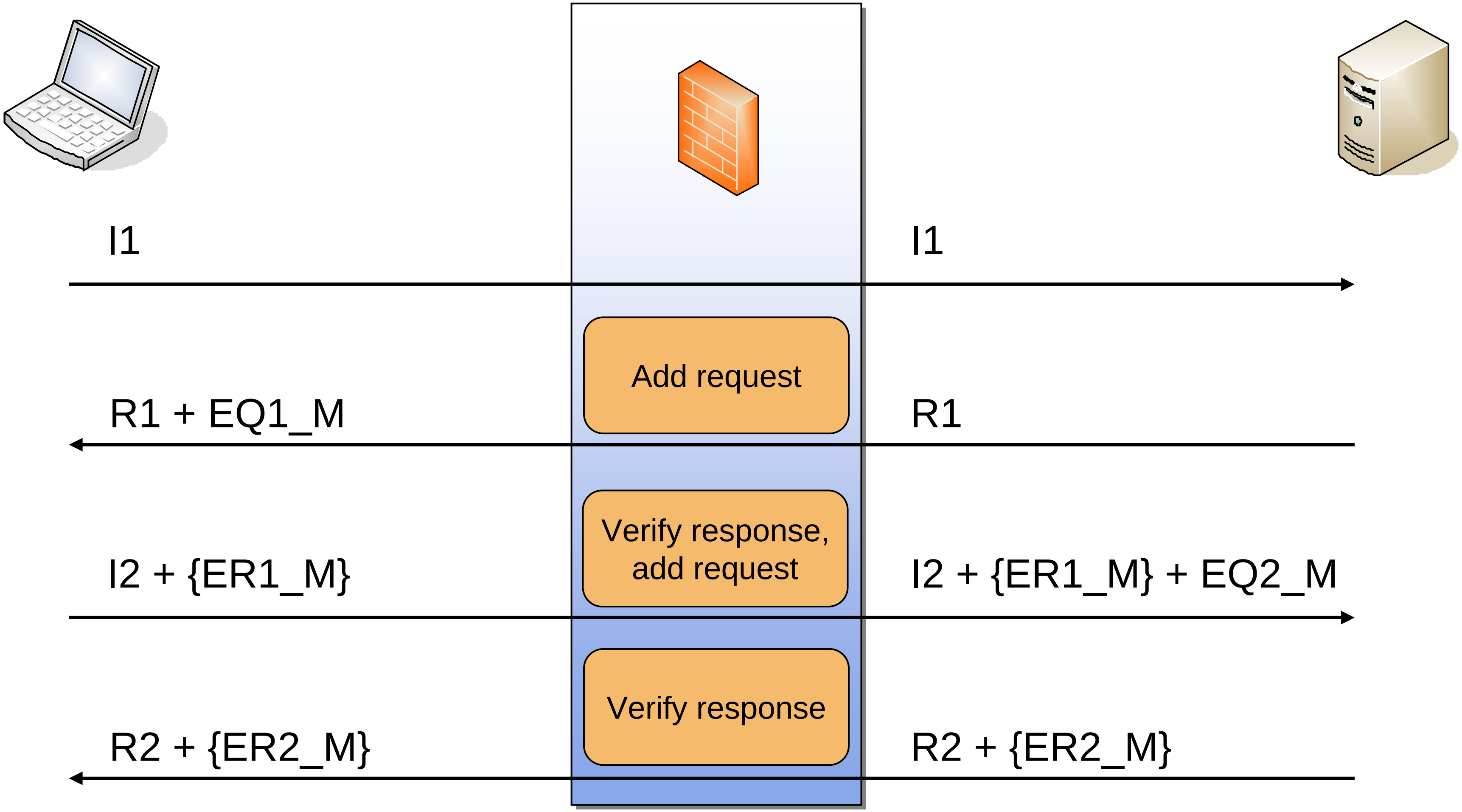
- ECHO_REQUEST_M
  - Identical to ECHO_REQUEST (except type no.)
  - In unsigned part of packet (65332)

- ECHO_RESPONSE_M
  - Identical to ECHO_RESPONSE_SIGNED
  - In signed part of packet (962)

New Parameters (cont‘d)

- PUZZLE_M
  - Similar to PUZZLE
  - Larger opaque data field (6 bytes vs. 2 bytes)
  - In unsigned part of packet (65334)
- SOLUTION_M
  - Similar to SOLUTION
  - Larger opaque data field (6 bytes)
  - In signed part of packet (322)
- Puzzle + request / solution + response should be one parameter (ordering problem)

Authentication: BEX



I1

I1

Add request

R1 + EQ1_M

R1

Verify response, add request

I2 + {ER1_M}

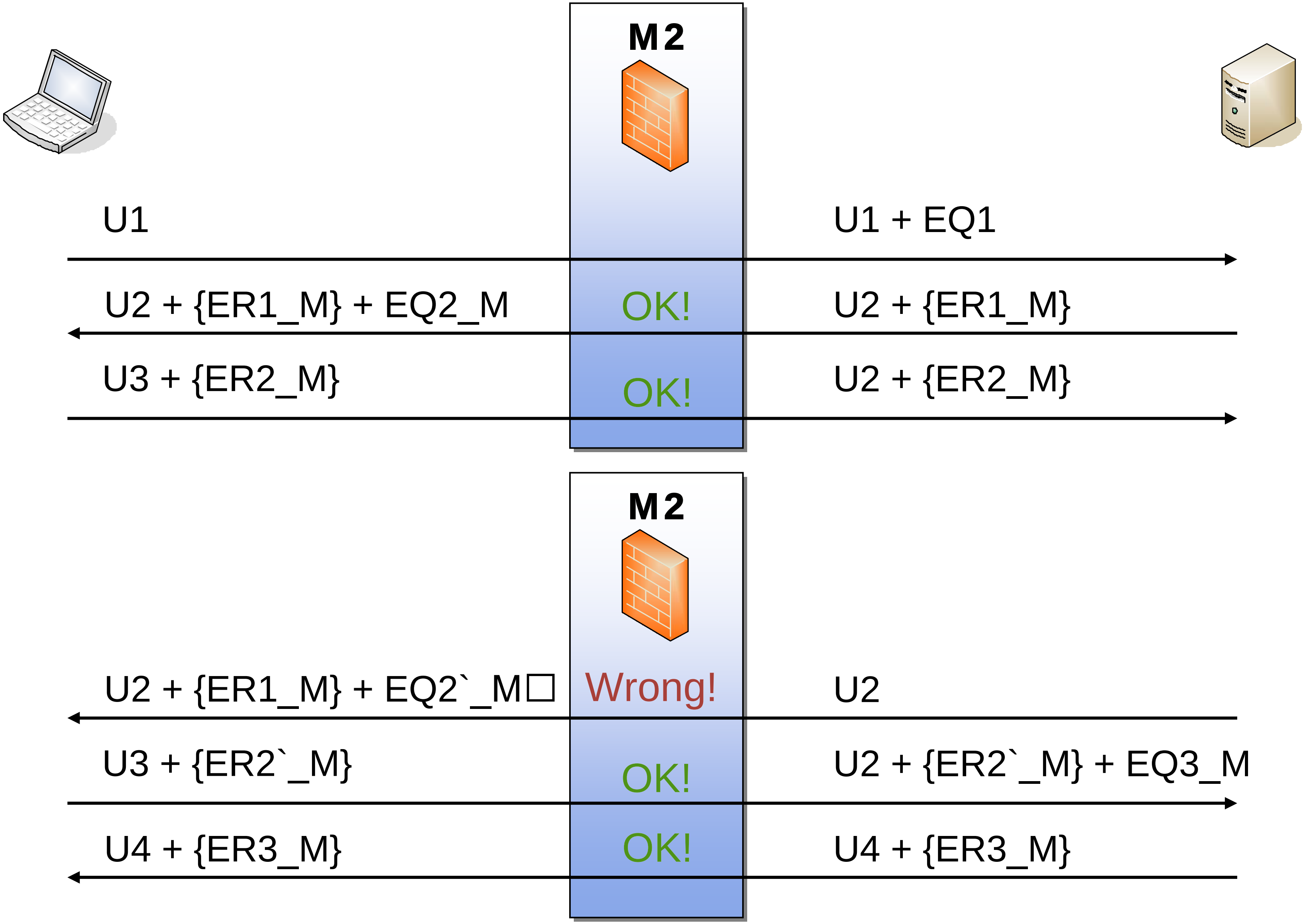
I2 + {ER1_M} + EQ2_M

Verify response

R2 + {ER2_M}

R2 + {ER2_M}

Authentication: UPDATE



M2

U1

U1 + EQ1

U2 + {ER1_M} + EQ2_M

OK!

U2 + {ER1_M}

U3 + {ER2_M}

OK!

U2 + {ER2_M}

M2

U2 + {ER1_M} + EQ2`_M□

Wrong!

U2

U3 + {ER2`_M}

OK!

U2 + {ER2`_M} + EQ3_M

U4 + {ER3_M}

OK!

U4 + {ER3_M}

Parameter Handling

- Middleboxes
  - MUST preserve order of parameters
  - MUST add further parameters after present ones
  - Helps host to determine location of MB

- End-hosts
  - MUST preserve order when copying to response
  - Sign packet
  - Helps MB to find parameter

Missing HOST_ID

- Problem: no HOST_ID in UPDATE packet
  - But: MB must figure out PKs
  - Request from URL (Hash and URL)
    - Slow (1 RTT)
    - Insecure (resource exhaustion, reflection, amplification)

- Solution: send HOST_ID in UPDATEs
  - Carrying ECHO_RESPONSE_M
  - Carrying SOLUTION_M

- BUT: larger packets

Open Issue: ESP - HIP Bindings

- Strong authentication for HIP packets
- Weak binding between ESP and HIP
  - No packet-level authentication for ESP
  - Packet injection possible

- Use of the extension: Attackers cannot...
  - ... open a channel by themselves (...~~by any one~~)
  - … store and reuse old BEXes (… ~~at any time~~)
  - ... use arbitrary network locations and connection properties (… ~~from anywhere~~)
  - ... cannot replay BEX to different middleboxes (… ~~towards any middlebox~~)

Conclusion

- draft-heer-hip-middle-auth
  - Prevent replay attacks
  - Use BEX and UPDATE to authenticate communicating peers
  - Enables secure access control without explicit registration
  - Protection from DoS
  - Is this useful for the RG?

draft-nikander-hip-mm-00 (2003)

- Reason for signature in update packet:
  - “The purpose of the signature is to allow middleboxes to verify the integrity of the packet. The HMAC allows the peer node to verify the packet very fast.”