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:

+ CHALLENGE_REQ

{CHALLENGE_RES} OK!
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

- Puzzle seed derivation
  - Concatenation of received opaque values
- Puzzle difficulty: max(K_i)
- Puzzle Lifetime: min(Lifetime_i)
3. Security Services for the HIP Control Channel

In this section, we define the adversary model that the security analysis in the later sections will be based on.

3.1. Adversary model and Security Services

For discussing the security properties of the proposed HIP extension we first define an attacker model. We assume a Dolev-Yao threat model in which an adversary can eavesdrop on all traffic regardless of its source and destination. The adversary can inject arbitrary packets with any source and destination addresses. Consequently, an adversary can try to break the protocol by illicitly trying to authenticate as a HIP entity. We assume an attacker model in which an adversary can eavesdrop on all traffic regardless of its source and destination. The adversary can inject arbitrary packets with any source and destination addresses. Consequently, an adversary can try to break the protocol by illicitly trying to authenticate as a HIP entity.
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

- Server
- Host AP (HAP)
- Mobile Guest (MG)
- Municipal services
- Service domain *1
- Service domain *N
- Service Gateways (SG)*
- Community Operator (CO)
- Membership certificate
- Service certificate*
- Internet
- IP traffic
- Secure tunnel
- Trusted Relay (TR)
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
- Implementation of draft-hip-heer-middle-auth
Small demo

... at the next power plug near you