

T-110.557 Research Seminar on Telecommunications Software

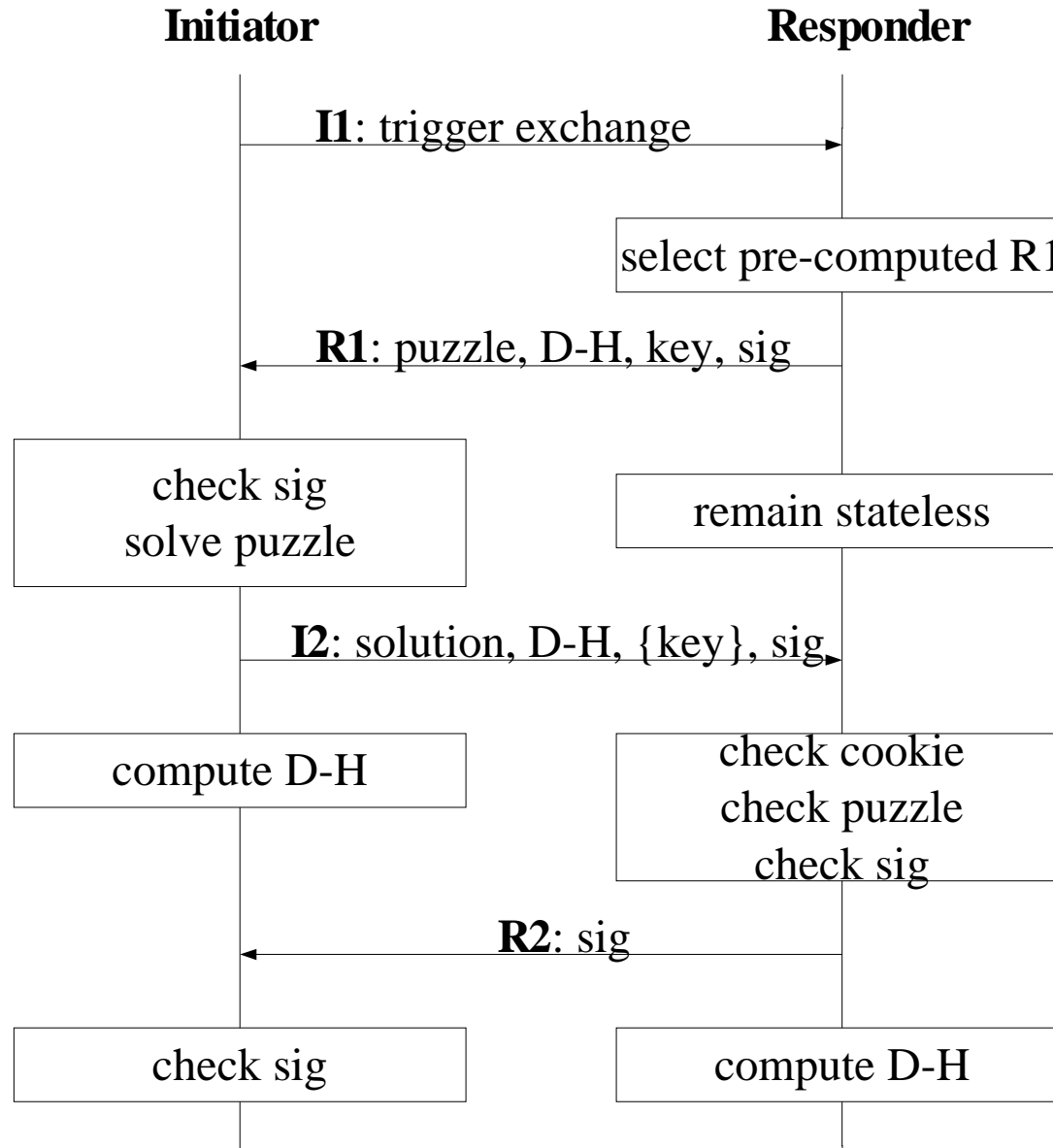
# Integrating Legacy User Authentication with HIP

Jani Hautakorpi  
([Jani.Hautakorpi@hut.fi](mailto:Jani.Hautakorpi@hut.fi))

# Contents

- HIP base exchange
- Selected legacy user authentication mechanisms:
  - Digest Access Authentication
  - EAP (Extended Authentication Protocol)
  - XAuth (Extended Authentication within IKE)
- Proposal on how to integrate legacy user authentication with HIP
- Real-life scenario

# HIP Base Exchange



# Digest Access Authentication

- Originally developed for HTTP
- Currently used e.g. with SIP
- Uses *challenge/response* paradigm:
  - Challenge: *nonce* value (hexadesimal data)
  - Response: checksum from username, password, requested URI, ...
- Verifies that both parties know the shared secret
- Text-based mechanism

# EAP

- Originally designed for environment, where IP connectivity was not available
- Today, used also on top of UDP and TCP
- Uses *challenge/response* paradigm
- Defines e.g. terms: *backend authentication server*, *EAP server* and *pass-through agent*
- Supports many authentication mechanisms
- EAP can be encapsulated either to RADIUS or to DIAMETER packets

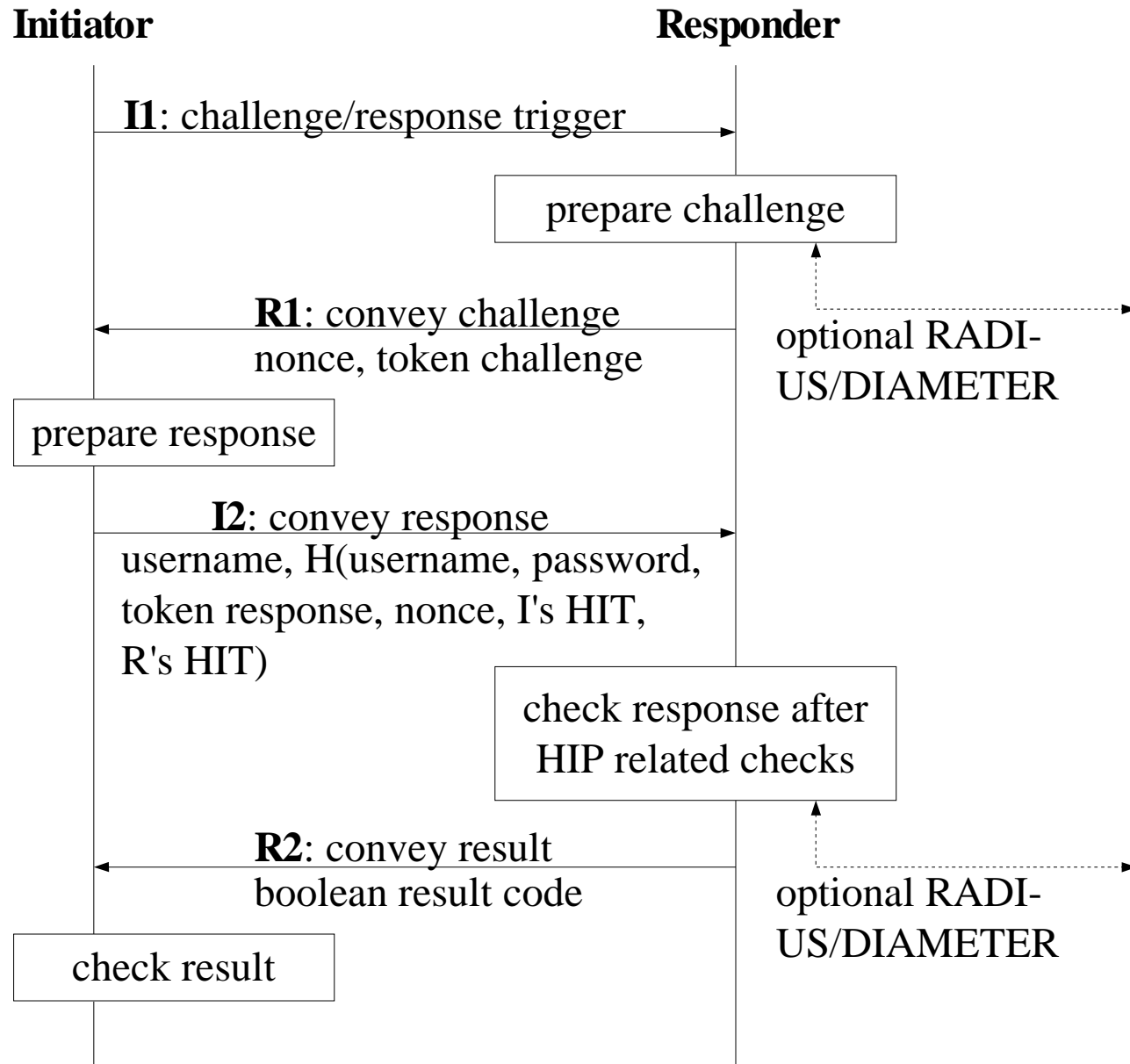
# XAuth

- Was an attempt to provide legacy user authentication within IKE
- Just an extension to IKE, didn't affect to IKE itself
- Uses secure ISAKMP messages, so transmitted credential are encrypted
- ISAKMP is a binary protocol
- Ability to periodically authenticate users

# Authentication Proposal for HIP (1/3)

- At the present, HIP authenticates only host
- Some fundamental ideas behind the proposal:
  - HIP's puzzle mechanism must be preserved
  - Users could be logically bound to SAs
  - Design should be as simple as possible
  - Adequate level of security for most use cases
  - Mechanism should be effective (RTT- & time-wise)
- Proposal is a high-level proposal, no bit-level issues discussed

# Authentication Proposal for HIP (2/3)

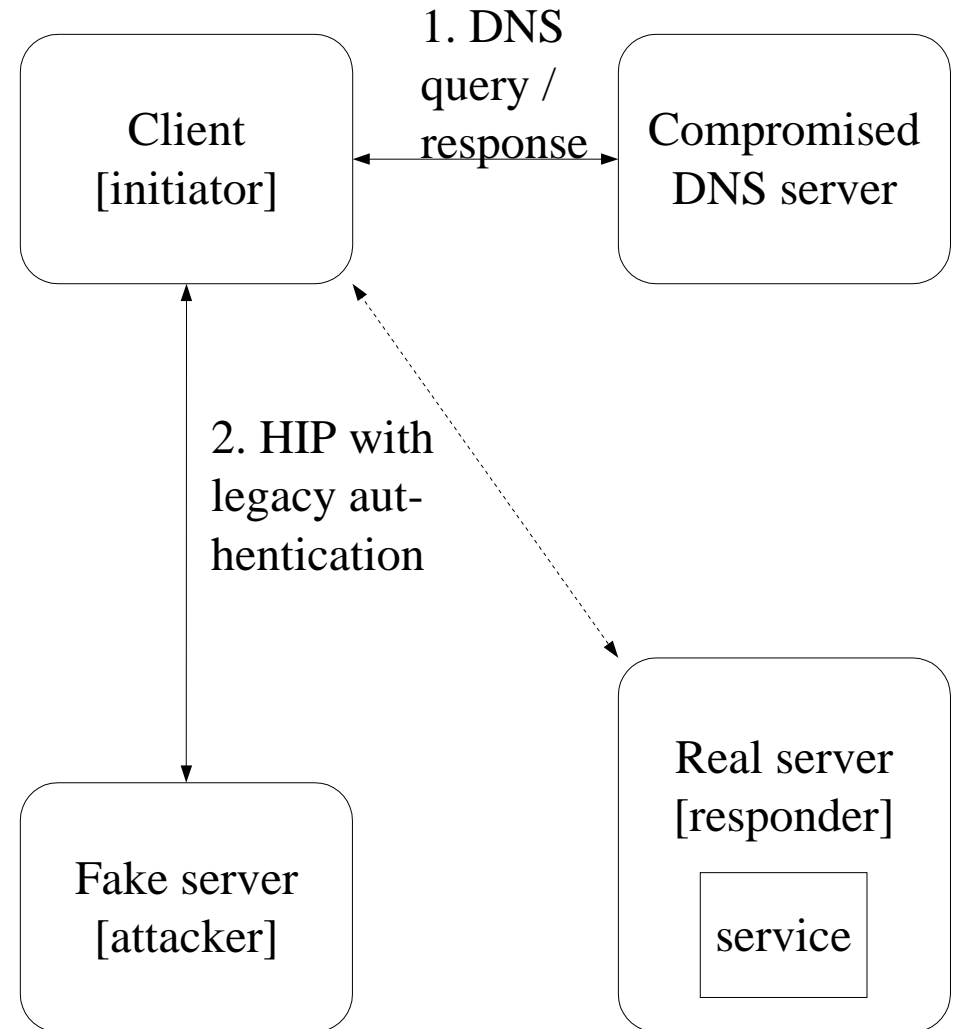


# Authentication Proposal for HIP (3/3)

- Key features:
  - Incorporated to HIP base exchange
  - Uses *challenge/response* mechanism
  - Only *two-factor* authentication allowed
  - Possibility to use *backend authentication servers*
  - Approximately host-wide ACLs can be deployed
  - Reliable log data can be produced
  - User authentication **does not** use asymmetric cryptography

# Real-life Scenario

- Resilient to the attacks that has been directed toward DNS
- Attacker has hacked a DNS server
  - HI, HIT and IP of the real server has been changed
- Attacker cannot get user's credentials



Questions, comments?