Accountability and host identities

Seppo Heikkinen
seppo.heikkinen@tut.fi
Department of Communications Engineering
Tampere University of Technology

Introduction

- Provision of services needs accounting measures
  - Reporting and tracking resource consumption
  - Basis for compensating the resource provisioning
- Customer generally has no control over reporting
  - Data may base solely on the declaration of service provider
  - Trust relationship between the provider and the home operator
    - “Honesty” based on loss of reputation
- There might be unauthorised charges on customer bill, “cramming”, due rogue provider
  - But customer could also deny having used the service even if he did

Requirements

- Identify participants of the transaction
  - Who is liable for the incurred costs?
- Binding of participants to the transactions
  - Authorised parties
- Creation of undeniable evidence
  - Accounting only the service usage which has taken place
- Risk management
  - To what extend you commit yourself (granularity)
  - What is “fair”?

Some concepts

- Non-repudiation
  - Cannot deny your involvement
    - Origin of message
    - Receipt of message
- Fairness
  - Correctly behaving party should not be discriminated
  - “Both parties get something”

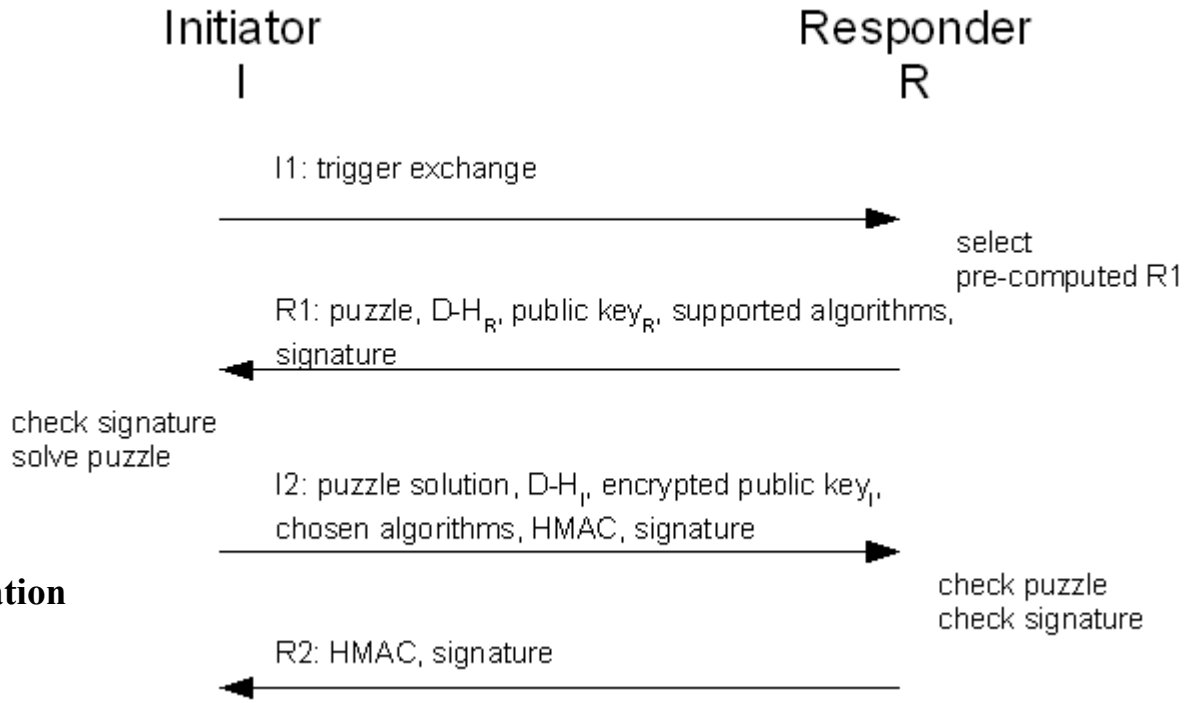
Host identity

- Conceptually, every entity has (abstract) host identity
- More specifically, public key pair can be representation of that identity (host identifier, HI)
  - In essence, you have a secure name
    - Proof of possession
- For concise representation use hashing (host identity tag)
  - Form, e.g., 128-bit hash
- Establish communication between host identities
  - Extra layer between transport and network layers

Host Identity Protocol

- Protocol for establishing an identity association between peers
  - Authenticate identity
  - Denial of service mitigation
  - Key agreement
  - Secure subsequent traffic
- Mobility and multihoming enhancements
  - Locator (IP address) no longer tied to the end point identifiers

HIP base exchange (BEX)



Identity association
(key material)

Potentially other associations

Hash chains

- A mechanism for multiple sequential authentications
- Create a chain by hashing the secret seed multiple times
- Release values in reverse order
  - Irreversible nature of hash chains makes it hard to guess the future value
- Binding of chain values easy to check
  - Hash functions usually fast

Hash chains:
x = secret seed
H = hash function
$H^n(x) = H(H^{n-1}(x))$
$H^n(x), H^{n-1}(x), H^{n-2}(x),\ldots,H(x)$
↑
hash chain anchor

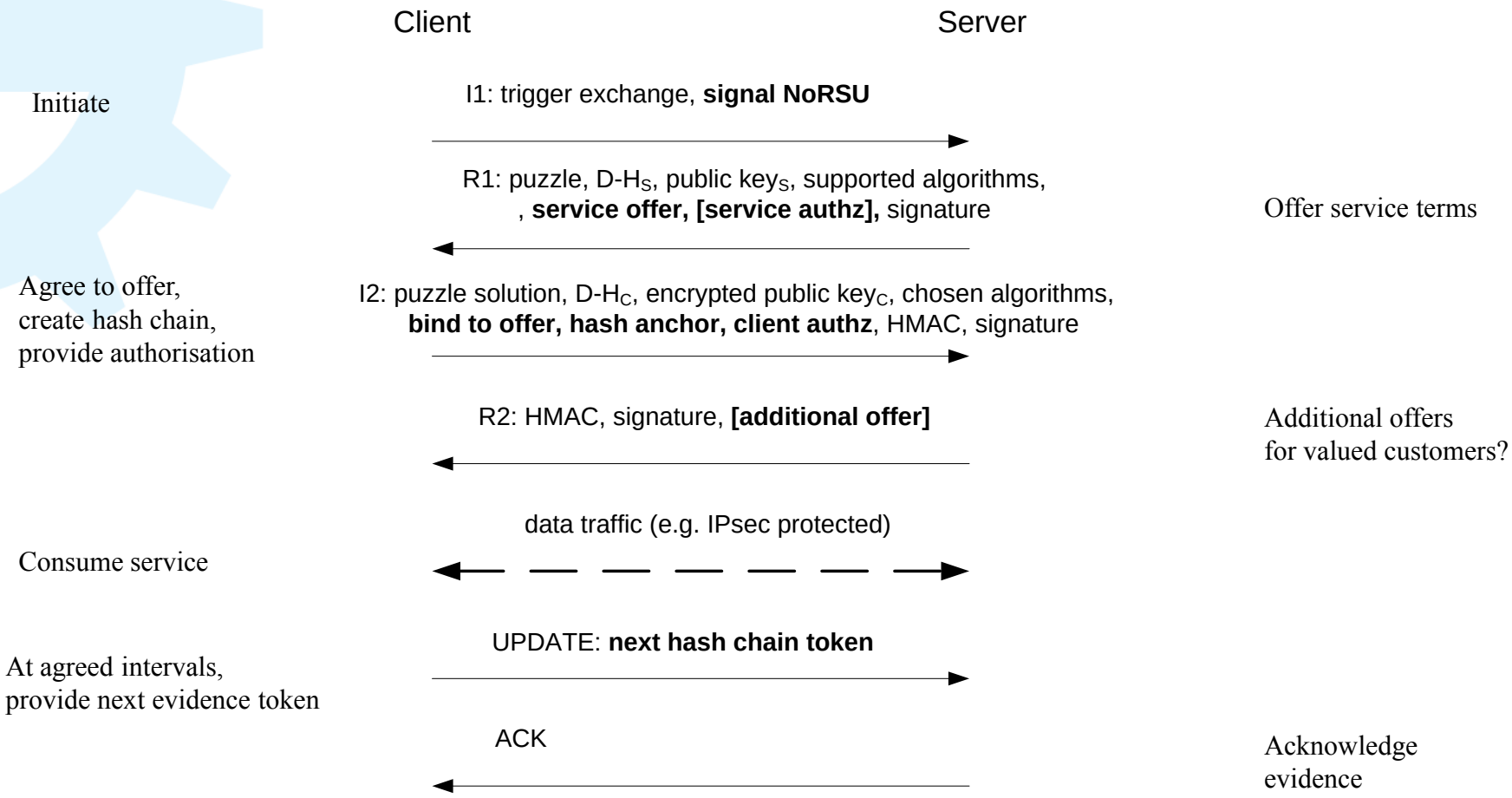
HIP based approach for non-repudiation

- Overload HIP with mechanisms to enable service terms negotiation and evidence generation
- Use Simple PKI (SPKI) certificates to create assured statements about the intentions of the participants
  - Offers for service and corresponding response to agree to the terms
  - Bound to the host identities
- Create hash chains to “pay” for the service usage
  - Bind chain anchor to the negotiation step
  - Compact size as evidence

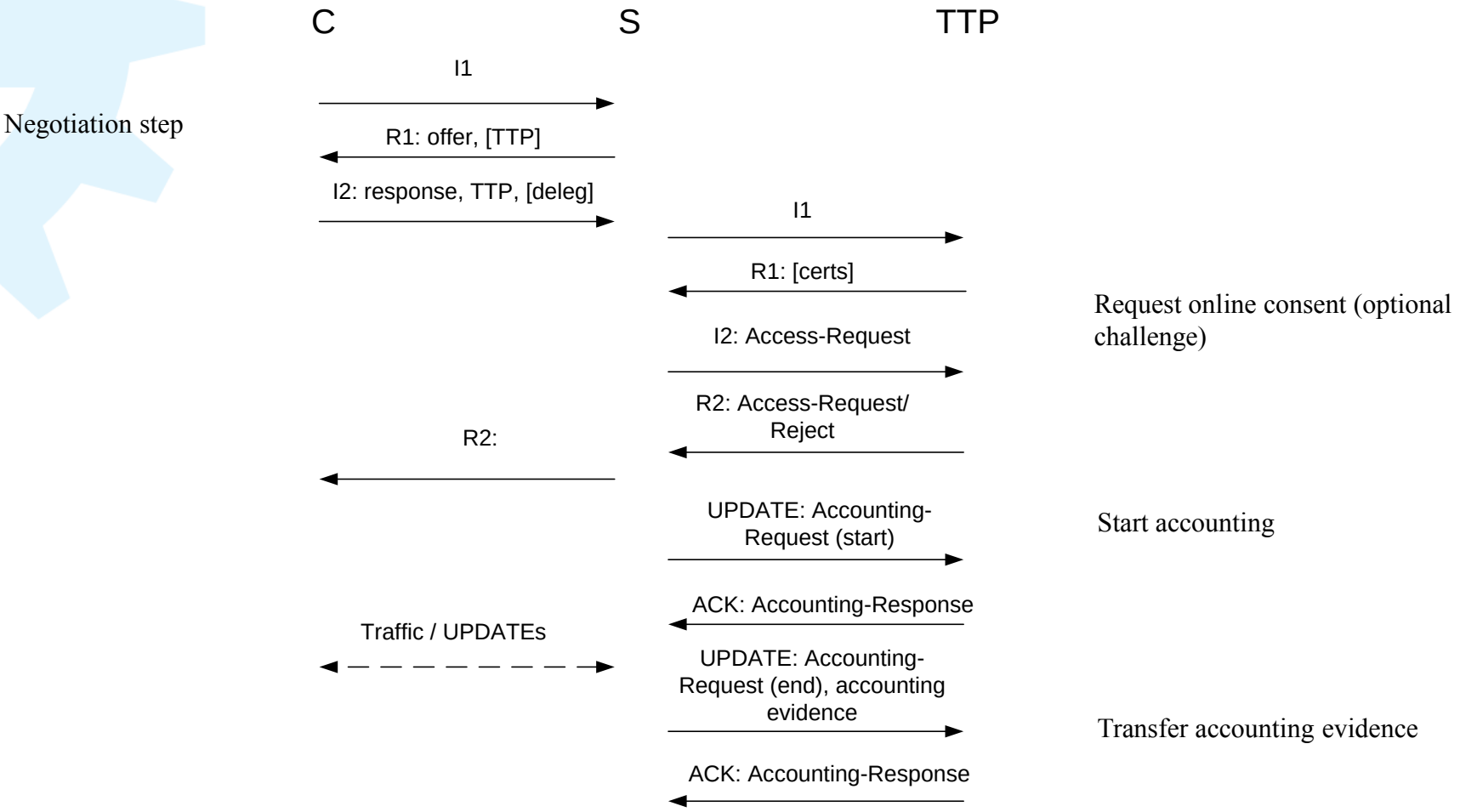
HIP based approach for non-repudiation cont'd

- Protect traffic with the negotiated security association
  - Keying material for, e.g., IPsec
- RADIUS interface towards the home operator
  - Online authorisation
  - Transfer of accounting evidence

Non-Repudiable Service Usage (NoRSU)



RADIUS enhancements



Characteristics of the solution

- Everything can be traced to the used identities
  - BEX includes offers/responses with respective identities
  - Hash chain anchor included in the responses
  - Only the original entity knows the hash chain values in advance (provided secret seed is not leaked)
  - Traffic protected with key material generated within BEX
- Hash chain payment is incremental
  - You commit yourself only to a portion of the service
    - Volume/time based
- Simple risk management
  - If you do not get service, do not provide any hash chains
  - If you do not receive hash chains, terminate service provisioning

Some practical challenges

- Host identities basically network level constructs
  - Might want to use also application identities (delegation)
  - Security of the keys
    - Secure platforms, pluggable modules?
- IP packet size constraints
  - If you want to avoid fragmentation
- Perception of time
  - Time synchronisation
- Lost packets cause uncertainty
  - Network malfunction or dishonest party?

Questions?

Thanks for listening!

Seppo Heikkinen
seppo.heikkinen@tut.fi