Identity-Bound Accounting

Seppo Heikkinen (seppo.heikkinen@tut.fi), Santeri Siltala (santeri.siltala@tut.fi)
Department of Communications Engineering
Tampere University of Technology, Finland

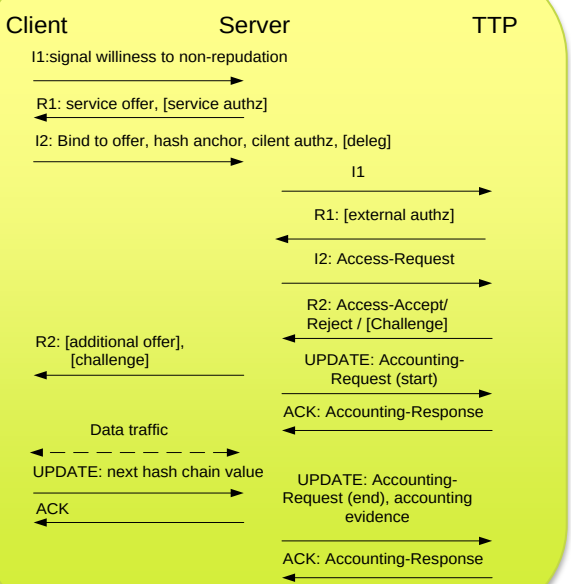
Aims

Provision of services needs accounting measures, i.e. tracking and reporting resource consumption. Generally, usage figures are exchanged irrespective of the client, hence the client has no control whether the figures are accurate or not. Client could also deny the correctness of those figures.

*In order to be fair to both parties, non-repudiation measures should be used to ensure that the **client gets the service it is paying for** and the **service provider gets undeniable evidence** of the used resources. Such **evidence** needs to be **bound to the used identities** in a secure fashion.*

For meeting these requirements, we have devised a system which ensures

- **Identification** of the parties securely
- **Trust** relationships between the parties
- Offline/online **authorisation** to use the service
- **Negotiation** of service terms
- **Non-repudiable evidence**
- **Granularity** of service usage (risk management)
- **R**



Building blocks

- Host Identity Protocol (HIP)
  - Identification of hosts (crypto-id)
  - Key exchange and identity association
  - Denial of Service protection
  - Channel protection, bound to negotiation
  - Decoupling of locator and identity
- SPKI certificates
  - Authorisation (offline) and delegation
  - Negotiation (offers and responses)
  - Bound to host identities through signatures
- Hash chains
  - Non-repudiable evidence tokens
  - Granularity
  - Bound to certificates
- RADIUS
  - Transfer of evidence to TTP
  - Optional online authorisation

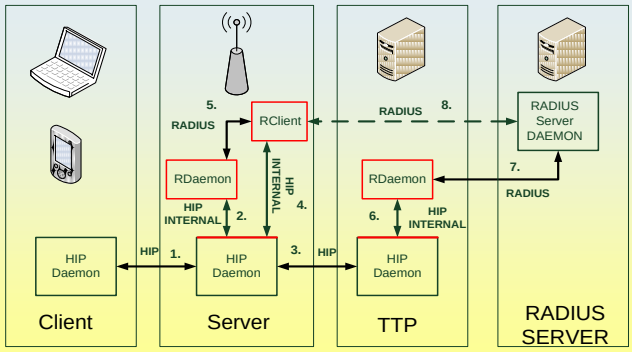
Binding process in action

Negotiation bound to the host identity, hash chains bound to the negotiation, data traffic bound to the identity and key exchange.

- If the client receives service, it submits a new hash chain token.
- If the service receives a hash chain value, it will provide service.

Implementation

- Based on HIP for Linux (HIPL) platform (1.0.4)
- FreeRADIUS 2.1.8
- HIP messages overloaded with extra parameters
- Certificates with S-encoding and efficient binary encoding
- Time and volume based charging (release frequency of hash chains)



Challenges

- Constrained size of IP packets (MTU)
- Synchronisation between the client and the server
- Lost packets cause uncertainty to honesty
- Finite length of hash chains
- HIPL only single threaded

TAMPERE UNIVERSITY OF TECHNOLOGY

This work was supported by TEKES as part of the Future Internet program of TIVIT (Finnish Strategic Centre for Science, Technology and Innovation in the field of ICT).