Applicability of host identities in ambient networking environment

Seppo Heikkinen
seppo.heikkinen@tut.fi
Networks and Protocols Group
Department of Communications Engineering
Tampere University of Technology

Outline

- Ambient environment
- Host identities
- Attaching roaming entities
- Authorisation issues
- Non-repudiable service usage
- Summary

Ambient environment

- Visions about the emerging networking technologies and convergence
  - Ubiquitous, pervasive, ambient intelligence, calm computing
  - User centric
- Heterogeneous access networks
  - Seamless connectivity everywhere (ubiquity)
  - Sensors
- Adaptable terminals
  - Reconfigurable platforms
  - Usability issues (natural interaction)
- User and network context
  - Automatic decisions based on context (intelligence)
  - Privacy issues

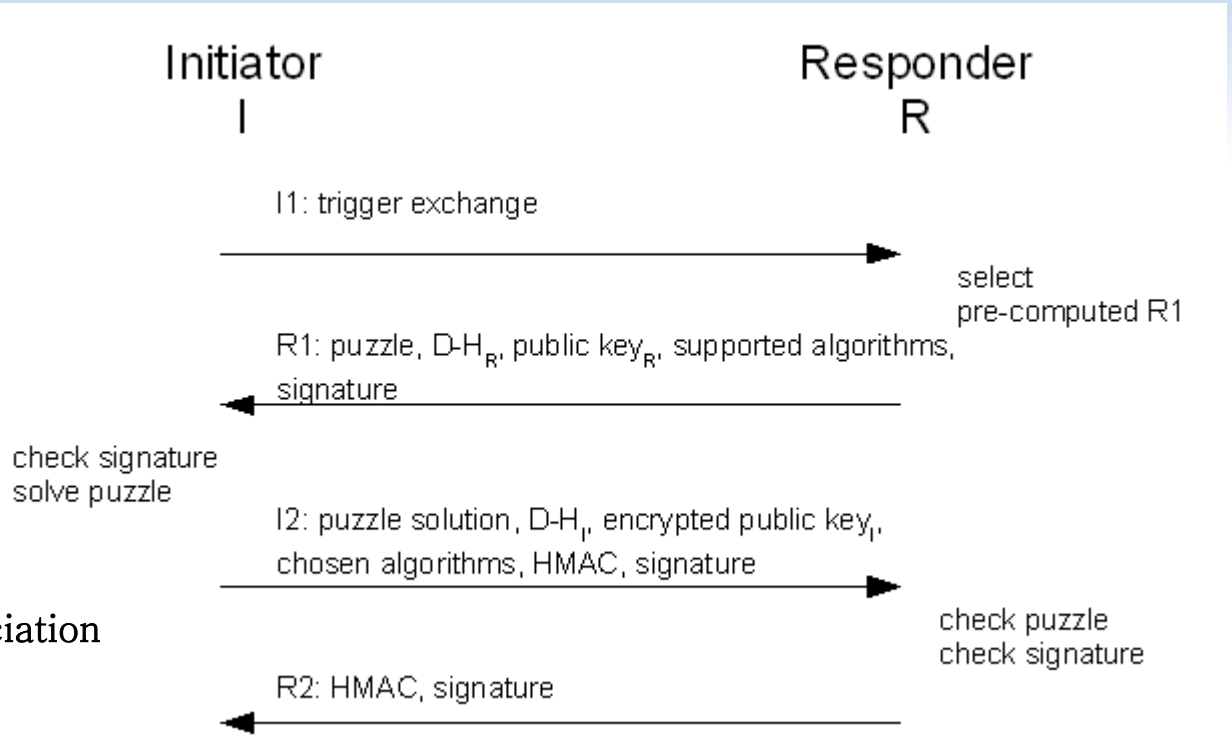
Ambient environment cont'd

- Service overlays
  - Cross-layer interaction
- Concept of "node is a network"
  - Dynamic (roaming) agreements
  - Composition
  - Controlled resource sharing
- New business models
  - Everybody could be an operator
  - Identity providers
  - Liability and trust issues

Host identities

- Provide end hosts secure names
  - Proof of possession
  - Even external parties of interaction can be identified
  - E.g. representation of public key pair
- Conceptual identity layer
  - Decouple locators and end point identifiers
    - Mobility
  - E.g. Host Identity Protocol (HIP)
- Identifiers can have "self-certifying" properties
  - Opportunistic trust (sameness)
  - Locality
- Identity management
  - Security domains
  - Identifiers on different levels

HIP base exchange (BEX)



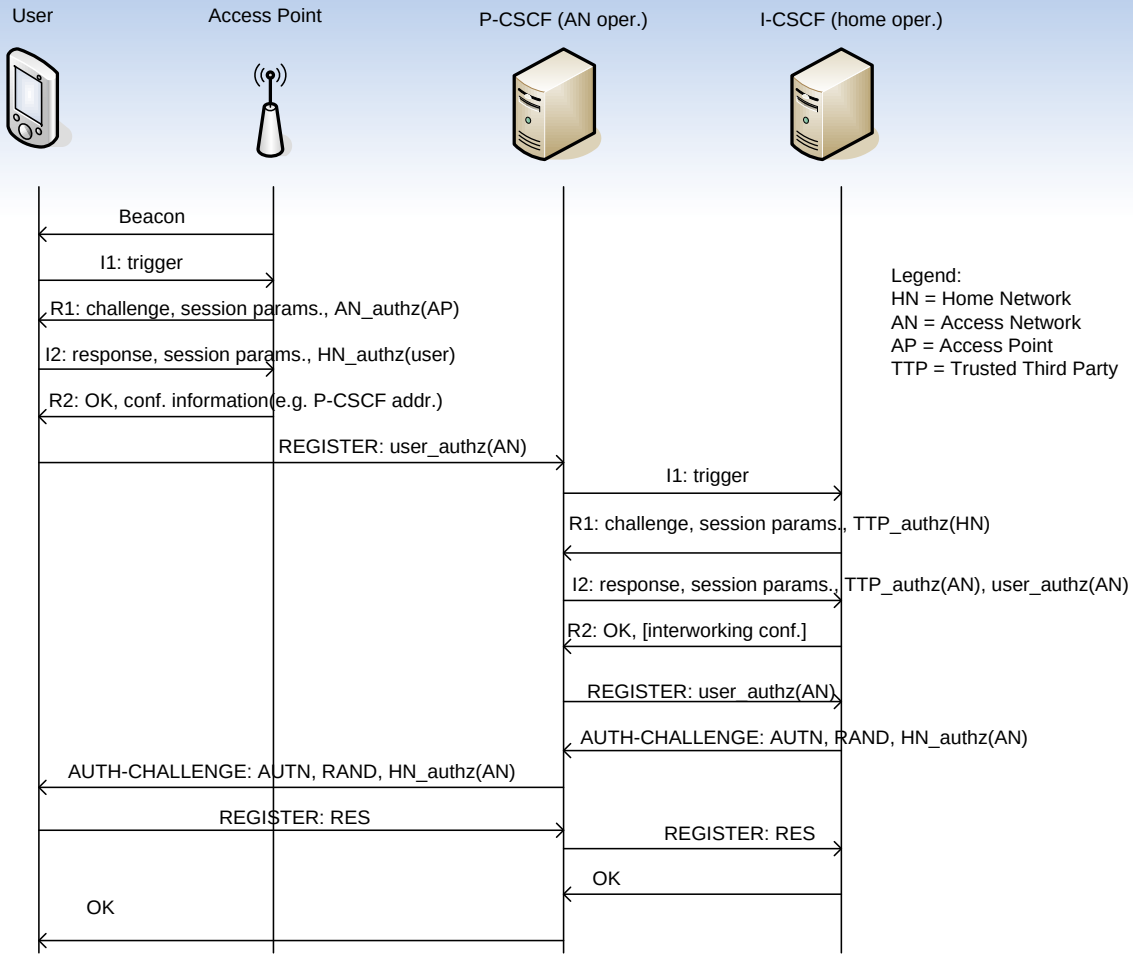
Identity association
(key material)

Potentially other associations

Attaching roaming entities

- Ambient technology enables "mini-operators"
  - More dynamic relationships
  - Roaming agreements on the fly
  - Trust issues among previously unknown partners
- Possibility to have common approach across different networks
  - Secure network attachment using identity information
  - Adapt to multiple layers, cross-layer interaction
- Authorisation to attach and access services
  - Who is liable for incurred costs
  - Naming of each participant
- Zero configuration
  - Also configuration of security (e.g. key management)
  - Deployment

Attachment example



Authorisation issues

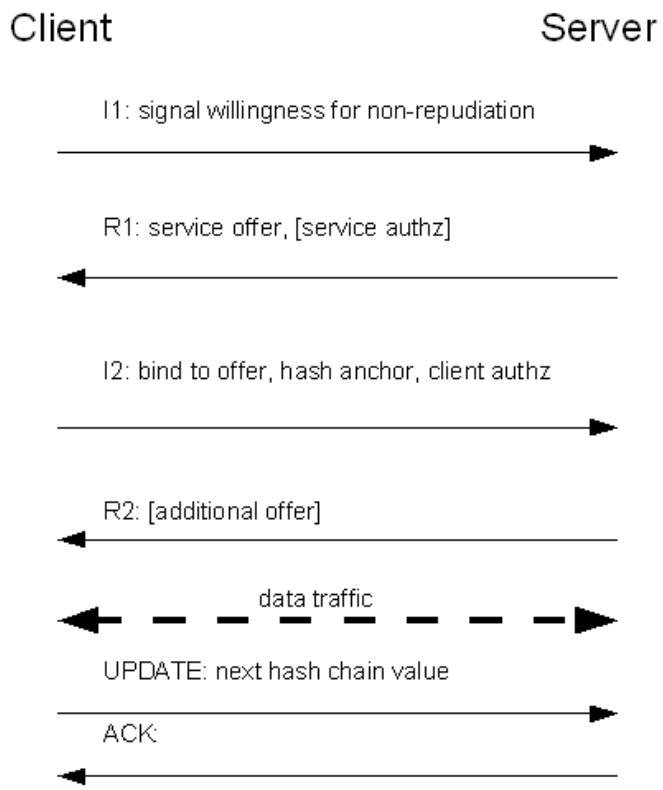
- Explicitly authorise actions
  - Real identity may not be so interesting, but authorisation is
    - Decoupling of authentication and authorisation
  - Strong binding of authorisation to an identifier
- Delegation
  - Improve efficiency by delegating actions
  - Privacy through short term identities
- Compensation is a form of authorisation
  - Who will pay
- Certificates as authorisation tokens
  - E.g. SPKI
  - Sizes of certificates vs. size of IP packets

Non-repudiable service usage

- Reputation may no longer be incentive enough to not to cheat
- Ensure that the compensation is provided according to real resource provisioning
- Bind identities to the offer of service and corresponding response
- "Pay" in a piecemeal fashion
  - If service is not provided, stop paying
  - If payment is not received, stop providing service
- Hash chains used to provide micropayment
  - Bound to identities through offer-response step
- Third parties still needed
  - Brokering and clearing

x = secret seed
H = hash function
$H^n(x) = H(H^{n-1}(x))$
$H^n(x), H^{n-1}(x), H^{n-2}(x),...$

Example



Offer:

```
(
 (cert
  (issuer (hash sha1 <hash value>))
  (offer (time 1 (s 60)))
  (validity (not-after 2008-10-30_12:00:00))
  )
 (signature (rsa-sha1 <sig>))
)
```

Response:

```
(
 (cert
  (hash-of-offer sha1 <hash value>)
  (hash-chain-anchor sha1 <anchor value>)
  (issuer (hash sha <hash value>)
  )
 (signature (rsa-sha1 <sig>))
)
```

Summary

- Host identities provide an interesting direction in the development of future architectures
- Ambient networking provides ubiquity and intelligence
  - Dynamic environment requires more security
  - Liability issues
- Secure naming of participants
  - Strongly bound statements
    - Authorisation and delegation
  - Non-repudiation
  - Privacy issues
- Proposals such as HIP can work as basis for solutions
  - Overloading BEX messages for efficiency
  - Some constraints in terms of frame sizes

Thank you!

- Comments/questions?

seppo.heikkinen@tut.fi