

# *Secure Identification and Authentication for Legacy Hosts in Ambient Networks*

*Kristian Slavov, Patrik Salmela, Tony Jokikyyny*  
Ericsson Research, NomadicLab



# *Presentation outline*

- ❖ Background
- ❖ Problem statement
- ❖ (Ignoring trivial solution of dual-connectivity)
- ❖ Solution: HIP proxy
  - Role of Legacy Authentication Services (LAS)
  - Solution walkthrough
  - Potential weaknesses
  - Security issues
- ❖ Summary

# *Background*

- ❖ Host Identity based networking paradigm
  - Identifier/Locator split
    - Network protocol agility
  - Cryptographic identities
  - Authenticated and encrypted communication channels
- ❖ A legacy host
  - Does not have usable networking identity
  - Cannot handle complex networking topologies

# *Problem*

## ❖ Legacy host

- How to connect to a host identity capable peer host?
- How to address the peer host using legacy network addressing (e.g. IPv4)?

## ❖ Host identity capable peer host

- How to identify and authenticate the legacy host?

# *HIP Proxy*

## ❖ Basically a simple proxy

- Store-(modify)-forward
- Ability to perform DNS resolution for the client host

## ❖ Additional features

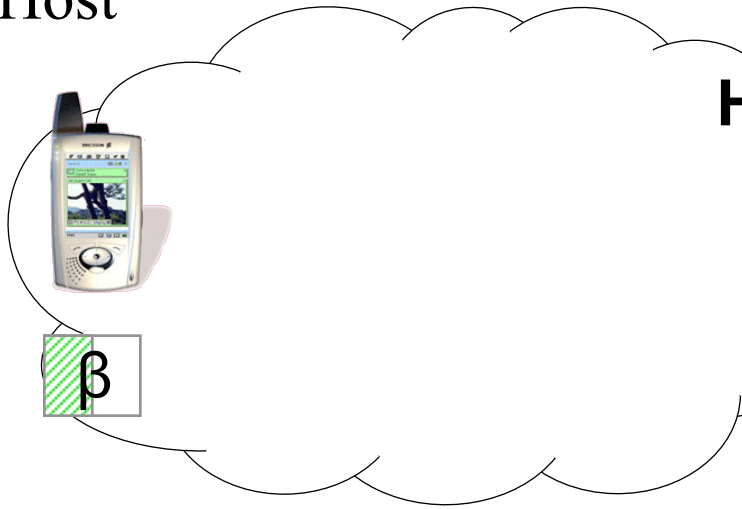
- Creates HIP connections on behalf of the legacy host
  - Creates temporary host identities for legacy hosts
  - Enables a mobile sub-network

# *Legacy Authentication Service*

- ❖ Stores (host) identities for subscribed users
  - AuC, AAA, etc.
- ❖ Understands legacy authentication procedures
  - SIM, HTTP-Digest, etc.
- ❖ Issues binding certificates
  - Binding between temporary and registered identity

# Step 1

Legacy Host



HIP Proxy



LAS

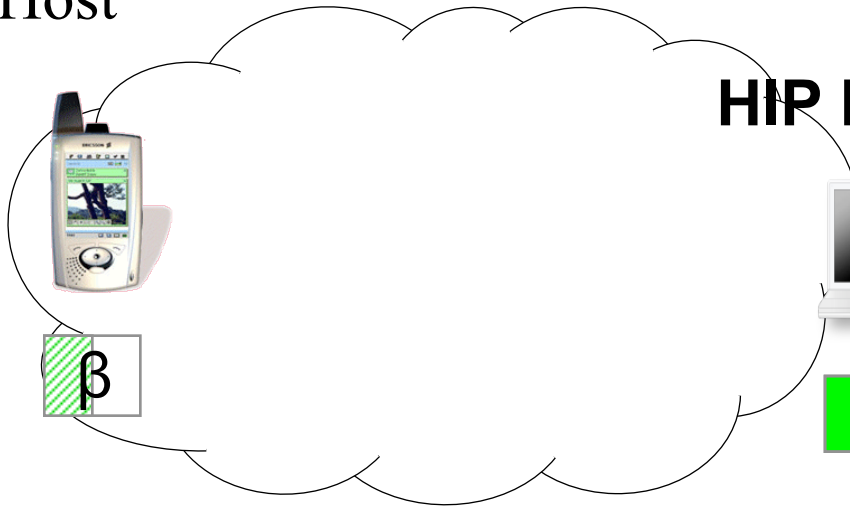


Peer Host



# Step 1

Legacy Host



LAS



Peer Host

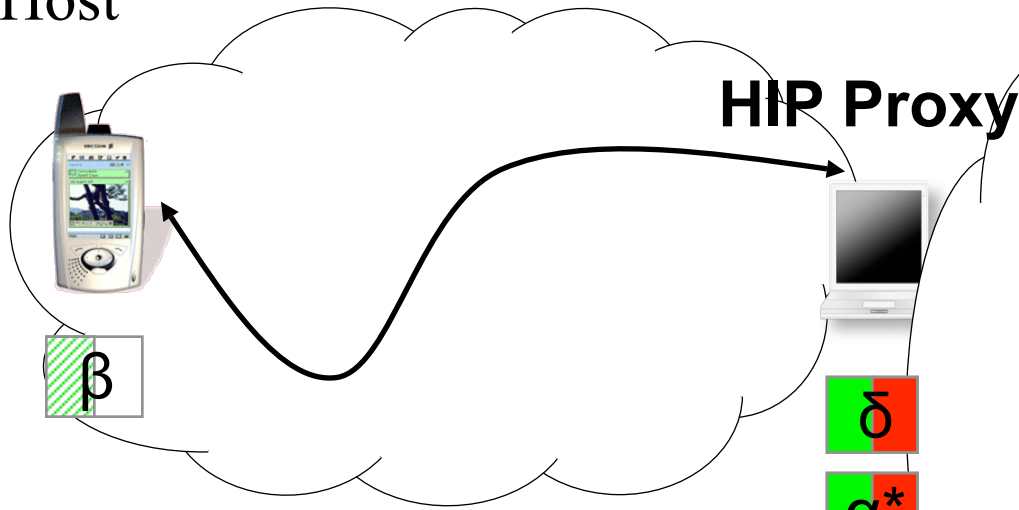


Legacy host performs network attachment.

HIP Proxy generates temporary identity for the legacy host.

# Step 1

Legacy Host



LAS



Peer Host

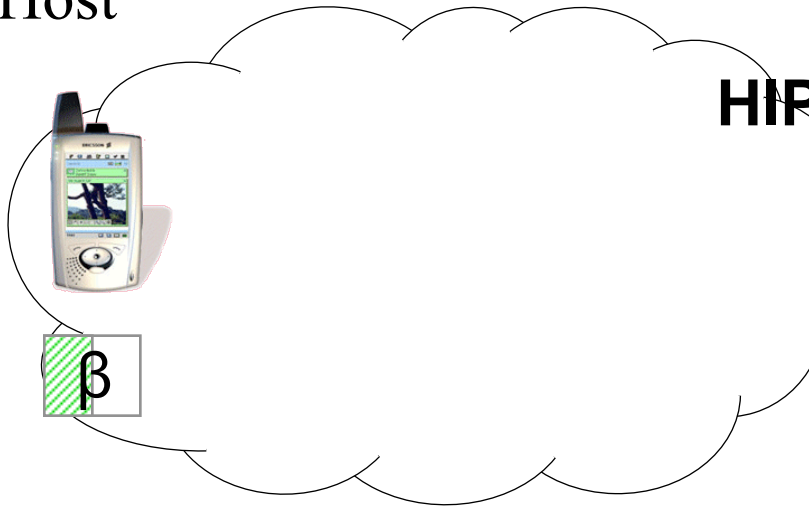


Legacy host performs network attachment.

HIP Proxy generates temporary identity for the legacy host.

# Step 2

Legacy Host



HIP Proxy



LAS

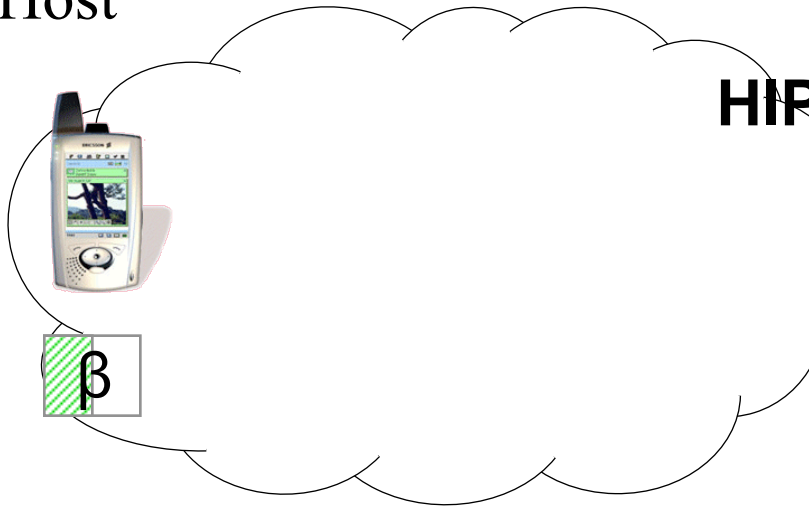


Peer Host



# Step 2

Legacy Host



LAS



Peer Host

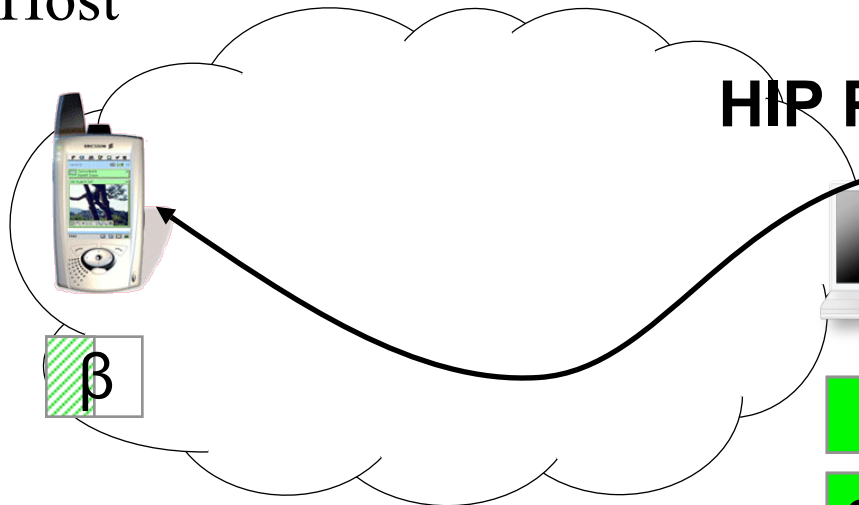


Legacy host authenticates itself to the network.

A HIP connection is established between HIP proxy and the authentication server.

# Step 2

Legacy Host



HIP Proxy



LAS



Peer Host

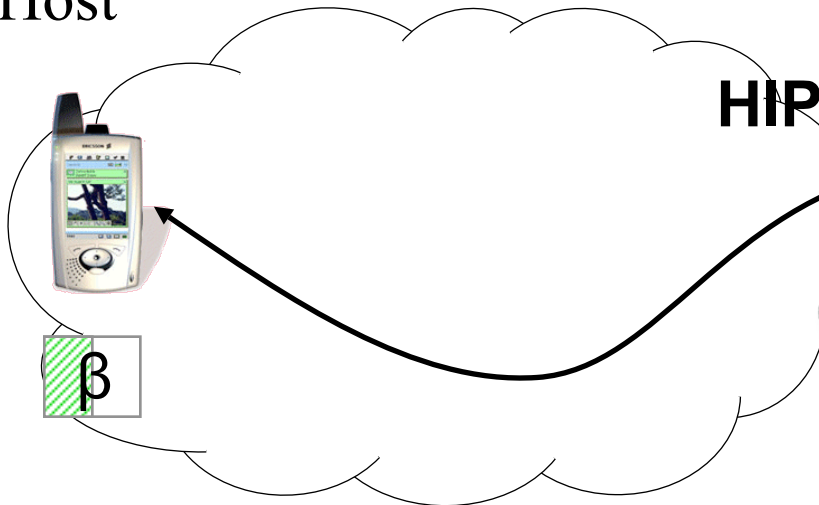


Legacy host authenticates itself to the network.

A HIP connection is established between HIP proxy and the authentication server.

# Step 3

Legacy Host



HIP Proxy



LAS

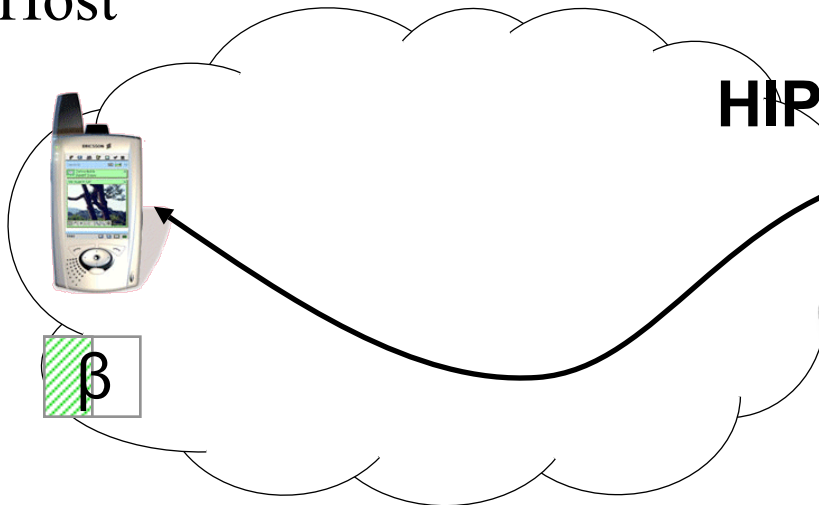


Peer Host



# Step 3

Legacy Host



HIP Proxy



LAS



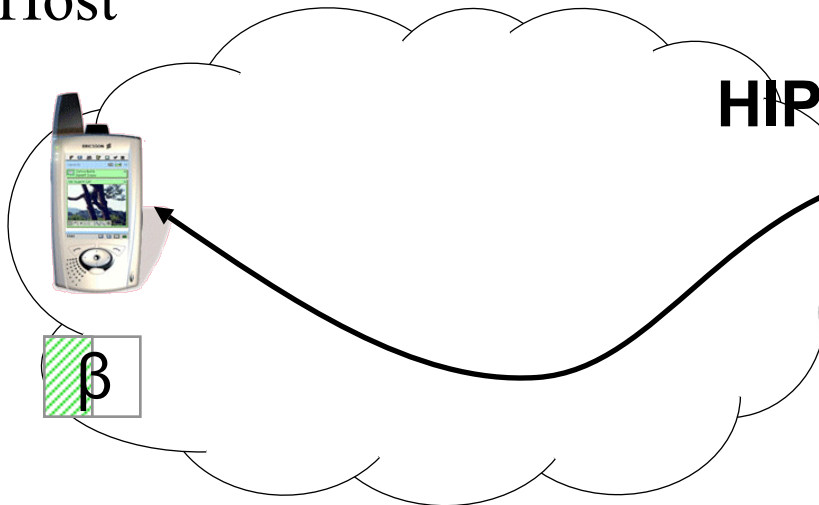
Peer Host



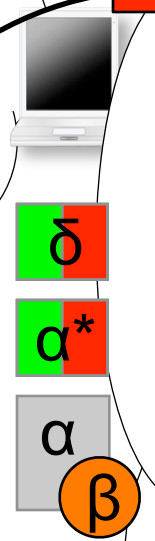
As a result LAS creates identity binding certificate for the HIP proxy.

# Step 3

Legacy Host



HIP Proxy



LAS



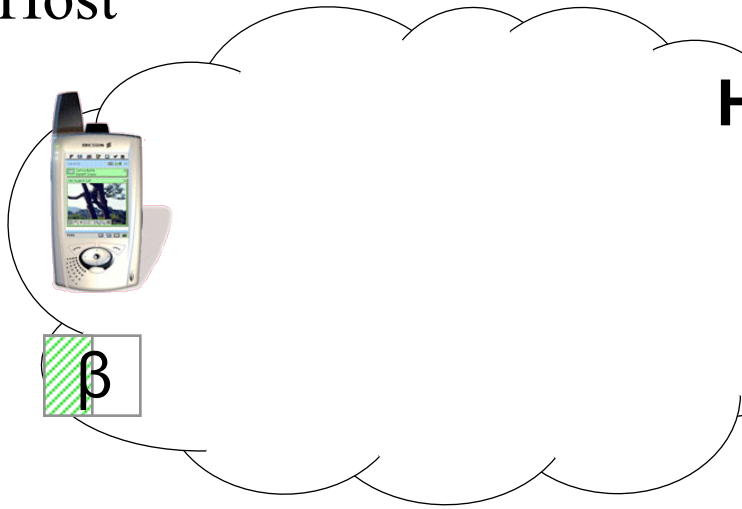
Peer Host



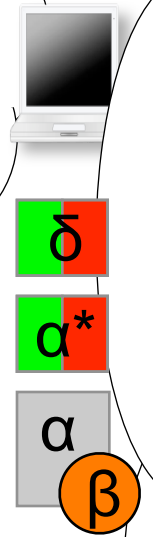
As a result LAS creates identity binding certificate for the HIP proxy.

# Step 4

Legacy Host



HIP Proxy



LAS

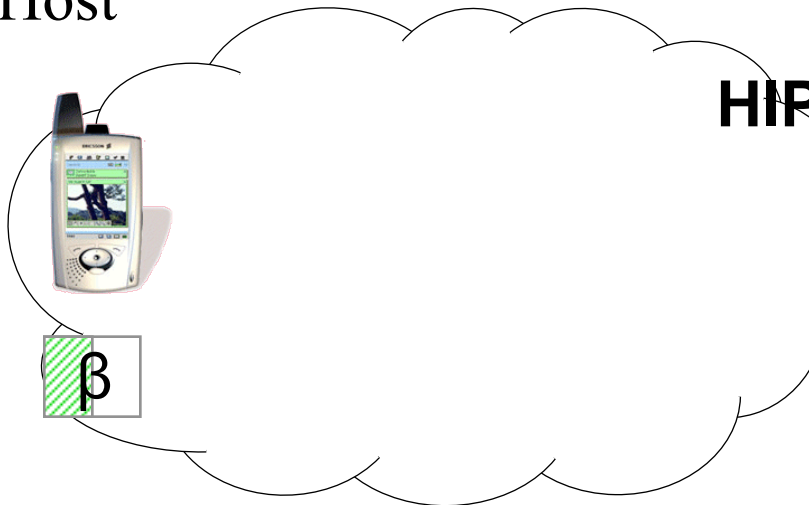


Peer Host

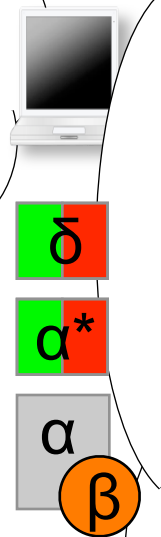


# Step 4

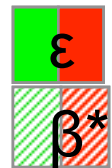
Legacy Host



HIP Proxy



LAS



Peer Host



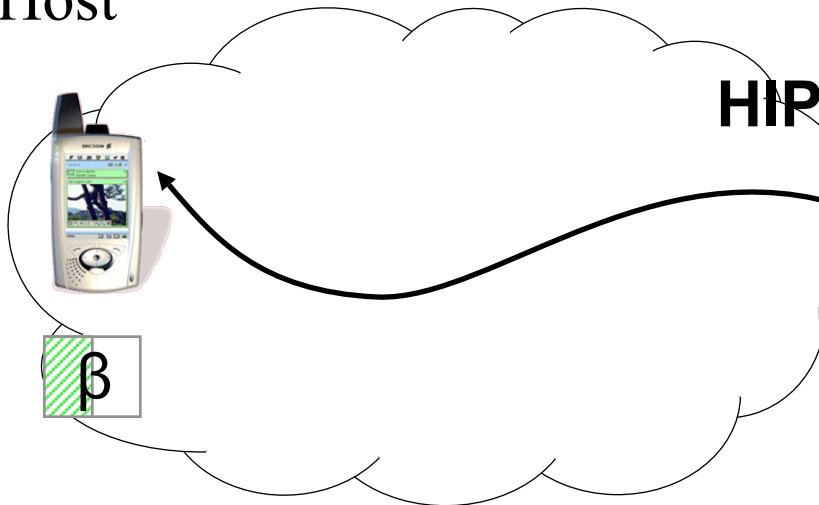
Traffic sent by the legacy host is intercepted at the HIP proxy.

New HIP association is created using identity certificate provided by the LAS.

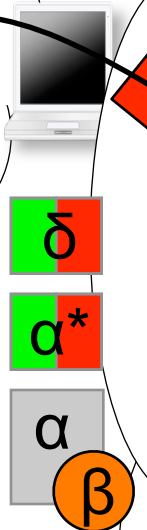


# Step 4

Legacy Host



HIP Proxy



LAS



Peer Host



Traffic sent by the legacy host is intercepted at the HIP proxy.

New HIP association is created using identity certificate provided by the LAS.



# Weaknesses

- ❖ Network access divided into two parts with different security properties
  - Access network (i.e. legacy host to HIP proxy)
  - Core network (i.e. HIP proxy to peer host)
- ❖ Access network is insecure
  - Security depends on the legacy host
  - Identification in the access network
- ❖ Name resolution
  - HIP Proxy will monitor and mangle DNS requests/responses

# Security issues

## ❖ HIP proxy

- Can misuse legacy host's identity to do bad things
  - Interesting target for hackers
- Operators may certify HIP proxies
  - LAS configured to issue identity binding certificates only to trusted HIP proxies

## ❖ Certificate revocation

- No one-size-fits-all solution
  - Legacy host cannot revoke the certificate
  - Unclear semantics of lifetime expiration
- The peer host must explicitly check from the CA

# *Conclusion*

- ❖ An opportunistic security solution
- ❖ Allows legacy hosts to communicate with host identity capable hosts
- ❖ Allows the peer hosts to better identify the legacy hosts
- ❖ Allows network mobility for legacy hosts