WISEciti WP4 T1: Secure Name Resolution
With flat cryptographic identifiers

HIP client

DHT node

DHT node

DHT node

Internet

DHT node

Current proposals

Name resolution query / announcement

Response

Payload security

WP4 proposal

Name resolution query / announcement

Response

Signaling security
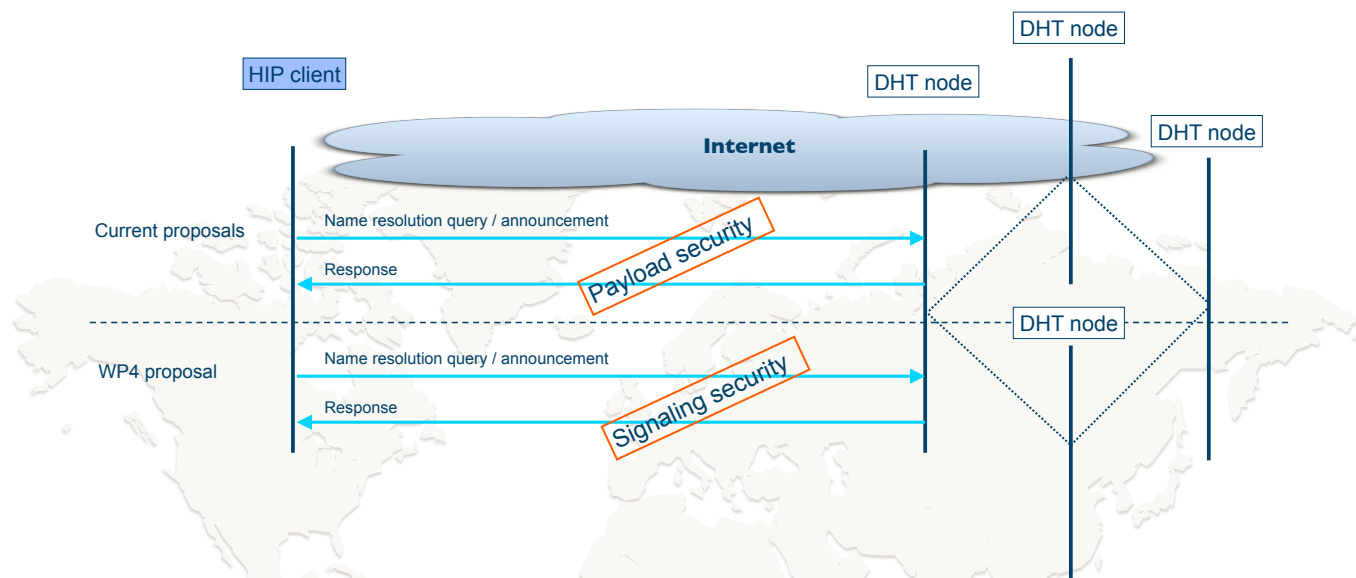
Cryptographic Identities – a solution for future internet

Distributed Hash Tables (DHT) – a solution for mapping uniformly distributed flat identifiers

Full Potential – Use cryptographic identities to protect identifier resolution

Host Identity Protocol (HIP) introduces Host Identity Tags (HIT), which are condensed representations of Host Identities (HI)
- Applications make network connections between HITs instead of pure IP addresses which also allows for seamless mobility
- For network routing the host must know the IP address of the destination peer
- To provide IP addresses we utilize DHTs

While DHTs provide good storage, the security is not in par with the rest of HIP's properties
- The aim is to provide adequate level of security to identifier mapping at DHT nodes by extending their application interfaces

We propose that DHT nodes act as gatekeepers, carefully considering what information is allowed in
- Concentrate on authenticating all name service traffic, providing protection against replaying, redirection, and name space pollution

Deliverables:

Prototype

Research report on security solution

ERICSSON
TAKING YOU FORWARD