Gap Analysis for
IDentity EnAbled networkS

draft-xyz-ideas-gap-analysis-00

Y. Qu (Ed.), A. Cabellos, R. Moskowitz, B. Liu, A. Stockmayer,
IDEAS BOF, IETF 99, July 2017, Prague
A Brief History of Identifier/Location separation

• The realization that IP addresses have overloaded semantics goes back to 1993 [RFC1498]
• Solution: Identifier-Locator Split
• Over the years several protocols have followed this paradigm, as an example:
  – HIP (RFC 6537)
  – LISP (RFC 6830)
• Identifier/LOC protocol use an infrastructure to store the relation between the two namespaces:
  – LISP Mapping System
  – RVS in HIP
Locator/ID Separation Protocol

1. Host A sends data to Tunnel Router X.
2. Tunnel Router X encapsulates the data and sends it to Tunnel Router Y.
3. Mapping System maps the Locator (X) to an Identifier (A).
4. Tunnel Router Y decapsulates the data and sends it to Host B.

**EID space**

**RLOC space**

**EID space**
Host Identity Protocol

• Bob’s slides
Common operation of ID/LOC protocols

1. Publish ID->LOC Mapping
2. Query Identifier
   Obtain location of HostA
3. Data Path

HostA

HostB
Privacy: Tracking of Location

1. Publish ID->LOC Mapping

2. Query Identifier Track Location of MN

Mobile Node

Attacker
Privacy: User-Defined Access Control Policies

1. Define Access Policy:
   E.g: I want to be reached only by people in my whitelist

2. Track Location

3. Query Identifier
   Obtain location of hosts

4. Data Path

Hosts

IDEAS Infrastructure

HostB

Attacker
User-Defined Access policies

• **GAP**: Existing protocols typically assume that Identifier/LOC information is **public**

• IDEAS introduces the notion of **privacy**:
  – Support fine-grained access policies to enable custom disclosure of Identity, Identifier and Locator(s) information
    • Not system-wide policies
  – Access policy tied to host **identity**
  – Identity is unique per entity
IDEAS introduces the notion of **IDENTITY**

**IDEAS Infrastructure**

1. **Publish IDy->IDf->LOC**
   - Define Access Policy
   - Use ephemeral IDfs

2. **Query Identity**
   - Obtain Ephemeral Identifier

3. **Query Ephemeral Identifier**
   - Obtain LOC

4. **Data Path**

**Hosts**

**HostB**
Identity (IDy) and Identifier (IDf) Split

• **GAP**: In Identifier/LOC protocols:
  – Identifier uniquely identifies the end-host
  – LOC identifies the network interface

• IDEAS introduces the notion of **identity** (IDy)
  – Identity is unique per entity
    • Allocation policies for identity
    • Permanent
    • Never revealed over the wire
  – Identifier is used as a session ID
    • Ephemeral IDfs can be used
    • Can be used in clear
  – Locator identifies the network interface
Common Infrastructure

IDEAS Infrastructure

IDf/LOC protocols

LISP
HIP
ILA

Data-Plane
Common Infrastructure

- **GAP**: Existing protocols offer their own mapping service for IDf/LOC
- IDEAS introduces a common infrastructure for IDy/IDf and IDf/LOC mappings
  - Work with existing protocols
  - Consistent policies
  - Ease network management
Summary

• IDEAS introduces the following new requirements:
  1. The notion of identity with its own lifecycle and requirements.
  2. Strong requirements for privacy tied to the identity. This requires fine-grained user-defined access control.
  3. A common infrastructure for IDy/IDf and IDf/LOC mappings.