Internet Indirection Infrastructure

Karthik Lakshminarayanan
UC Berkeley
Contrasting LNA, HIP, and i3

- LNA = “Layered Naming Architecture”
- LNA, HIP, i3:
  - All network architecture proposals
  - Separate location and identity
- What are the differences?
i3 Overview

• (Overlay) Forwarding Infrastructure that allows users to control routing and naming

• **Routing:**
  – Senders, receivers can control routing in the network
  – Set up the routing entries in the infrastructure

• **Naming:**
  – Fixed size IDs chosen by users/applications
  – ID typically identifies a service; can also identify end-hosts, etc.
i3 Overview

- Basic primitive is indirection
- Each packet is associated an identifier \( id \)
- To receive a packet with identifier \( id \), receiver R maintains a trigger \((id, R)\) into the overlay network
Mapping IDs

- $i3$ is implemented on top of Chord
  - But can easily use CAN, Pastry, Tapestry, etc
- Each trigger $t = (id, R) \text{ or } (id, id')$ is stored on the node responsible for $id$
- Use Chord recursive routing to find best matching trigger for packet $p = (id, data)$
What *i3* supports

- **Communication abstractions**
  - Mobility, Multicast, Anycast

- **Service interposition**
  - Receiver-driven, Sender-driven

- **Can combine primitives powerfully**
  - Receiver-driven heterogenous multicast
  - Service composition with server selection (using anycast)

- **Enables many applications**
  - NAT traversal, Secure VPN access
  - Protection against DoS attacks
  - IDS: route all packets through an intrusion detection box (e.g., Bro)
What *i3* supports

- **Communication abstractions**
  - *Mobility*, Multicast, Anycast
- **Service interposition**
  - Receiver-driven, *Sender-driven*
- **Can combine primitives powerfully**
  - *Receiver-driven heterogenous multicast*
    - Service composition with server selection (using anycast)
- **Enables many applications**
  - NAT traversal, Secure VPN access
  - Protection against DoS attacks
  - IDS: route all packets through an intrusion detection box (e.g., Bro)
Mobility

- Host just needs to update its trigger as it moves from one subnet to another
Sender-driven Service Composition

Use stack of identifiers in packets

Receiver is unaware of transformations
Heterogeneous Receiver-driven

Use stack of identifiers in triggers

Sender is unaware of transformations
Using \textit{i3} as a Lookup Infrastructure

- \textit{i3} employs \textit{short-cuts} if both sender and recipient allow it
- \textit{i3} is only used as a \textit{lookup} infrastructure
Using $i3$ as a Lookup Infrastructure

- $i3$ employs *short-cuts* if both sender and recipient allow it
- $i3$ is only used as a lookup infrastructure
Protocol Stack (Native Apps)

1. Client app sends a DNS request.
2. DNS passes the request to the i3 layer.
3. i3 layer sends an IP i3 message to the daemon.
4. The daemon receives the message and sends an ID to the transport layer.
5. The transport layer sends an ID to the receiver R.
6. Receiver R sends an ID to the transport layer.
7. The transport layer sends an ID to the i3 layer.
8. The i3 layer sends an IPi3 message to the client app.
9. Client app receives the IPi3 message and sends an ID to the transport layer.
10. The transport layer sends an ID to the i3 layer.
11. The i3 layer sends an IP message to the client app.
Status of i3

• Code publicly available: http://i3.cs.berkeley.edu
• Supports Linux & Windows XP/2000 legacy applications
• Several groups build applications on top of i3
  – U. of Waterloo: delay tolerant networks
  – UIUC: service composition
  – U. of Tübingen (Germany): mobility, security
Contrasting HIP, i3 and LNA

- **Infrastructure:**
  - HIP: rendezvous server
  - i3: integrated forwarding infrastructure; can be used for lookup also
  - LNA: uses an external lookup infrastructure

- **Semantics of IDs:**
  - HIP: IDs identify hosts
  - i3: IDs identify services; could also identify hosts
  - LNA: EIDs identify machines and SIDs services

- **Security:**
  - HIP: authentication, integrity, transport anonymity/DoS resistance
  - i3: IP anonymity, DoS defense at IP, rest through middleboxes
  - LNA: everything can be done through middleboxes