Host Identity Indirection Infrastructure – Hi^3

Jari Arkko, Pekka Nikander and Börje Ohlman
Ericsson Research

Presentation outline

- Motivation
- Background
- Secure i^3
- Hi^3
- Summary

Hi^3 motivation

- Question: How to get data based on HIT only?
  - HITs look like 128-bit random numbers
- Possible answer: DHT based overlay like i^3

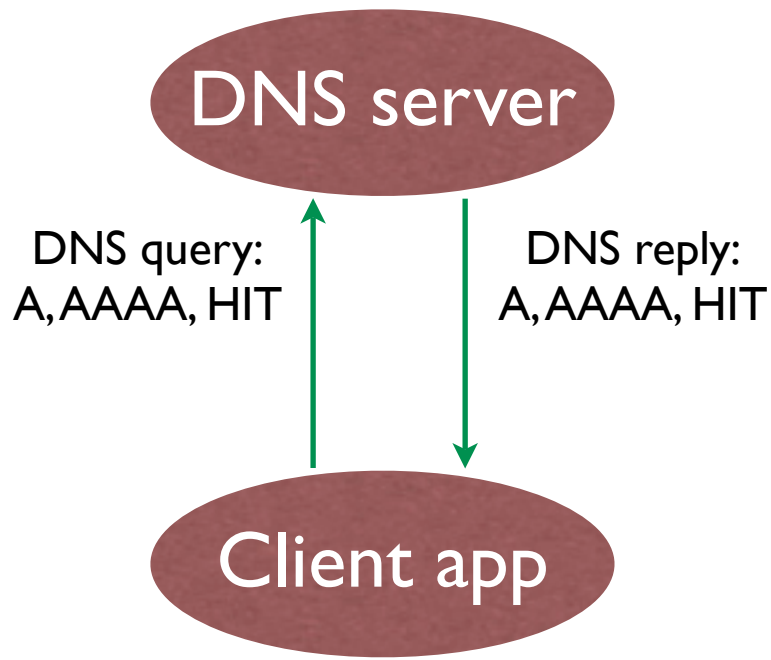
- Extra bonus: DDoS protection
  - Inherited from Secure i^3 and enhanced

Background

- Current HIP name resolution
- Basic HIP rendezvous service
- About Distributed Denial-of-Service attacks
- Two slide introduction to Distributed Hash Tables

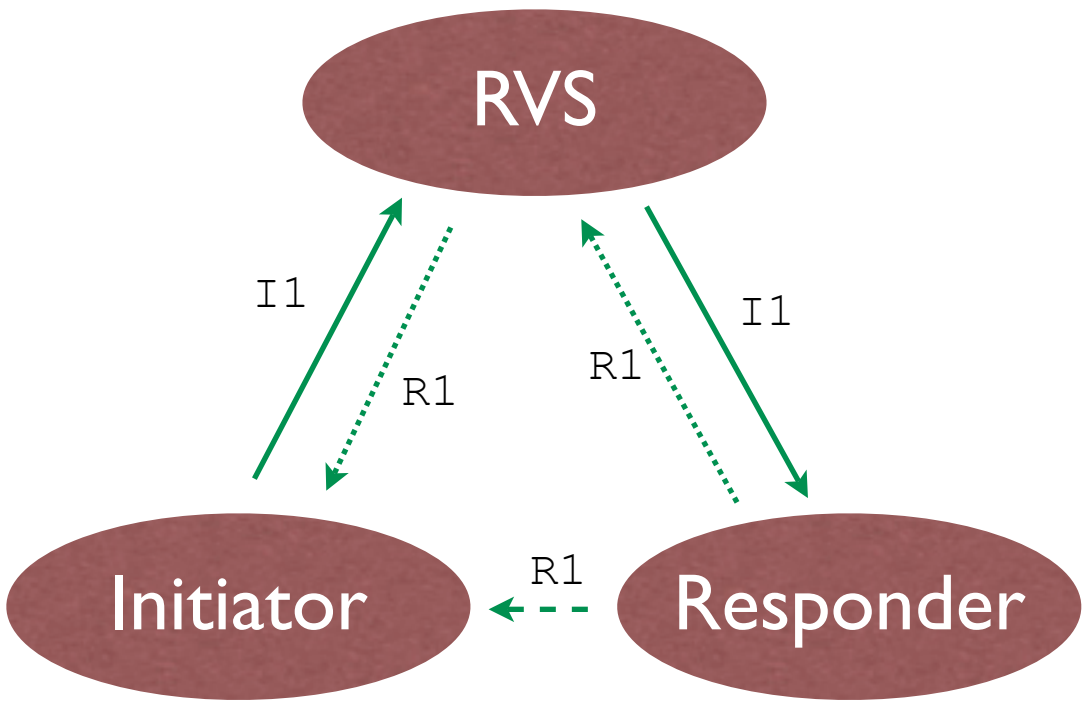
Current HIP name resolution

- HITs or HIs in the DNS
- DNS query asks for addresses and HITs
- Requires one to have a DNS name
- HITs not resolvable due to name space being flat



Basic HIP rendezvous service

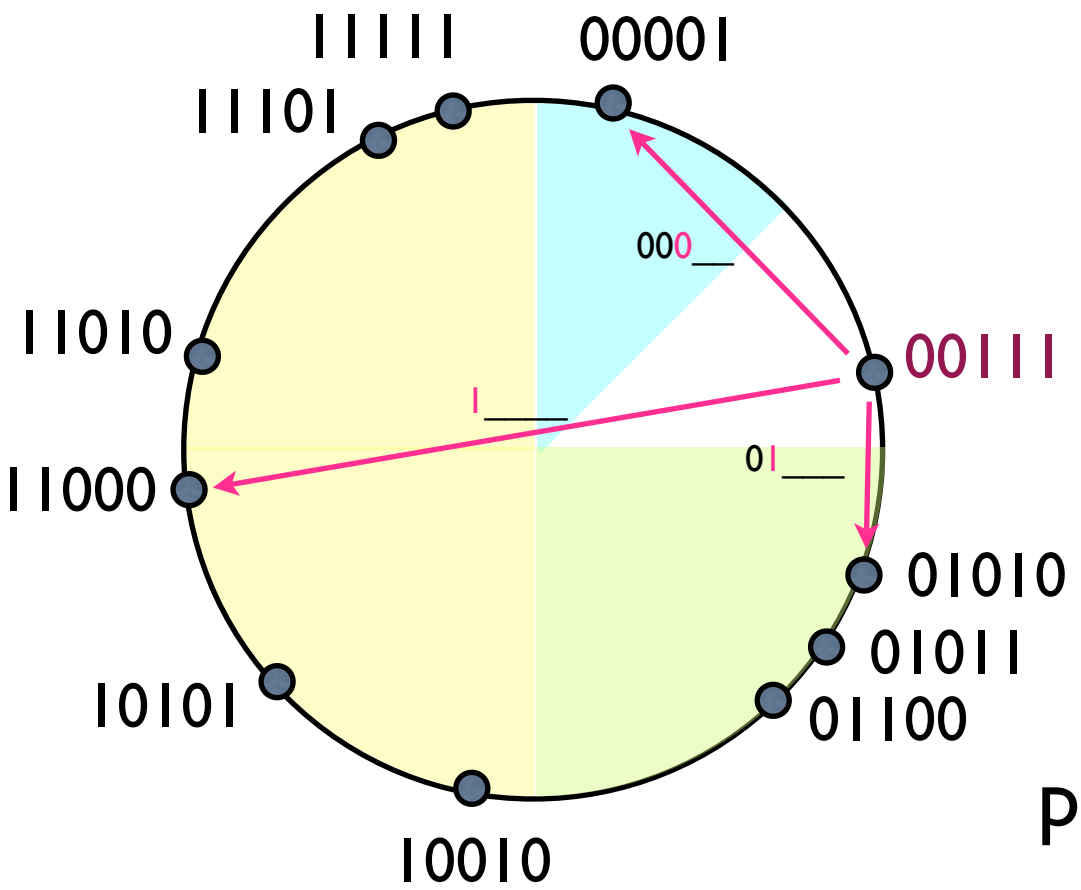
- Keep track of Responder's IP address(es)
- Forward `I1` to Responder
- Optionally forward `R1` back to the Initiator and then `I2` to the Responder
  - Keeps Responder's IP address(es) hidden until it has a chance to verify the puzzle



Distributed Hash Tables (DHT)

- Distributed directory for flat data
- Several different ways to implement
- Each server maintains a partial map
- Overlay addresses to direct to the right server
- Resilient through parallel, unrelated mappings

DHTs: Example



Prefix	Default node	Real node
00110	00110 = 6	none exists
0010_	00101 = 5	none exists
000___	00011 = 3	→ 1
01____	01111 = 15	→10
1_____	10111 = 23	→24

RT size = $\log_2(|\text{address}|)$

path length = $\log_2(|\text{address}|)$

About DDoS Attacks

- Attacks a victim from dozens to thousands of network locations at the same time
- Employs zombies, typically hacked PCs
- Observation:
  - Keeping IP address hidden protects from DDoS
- Question:
  - How to keep a server's IP address hidden?

Secure i^3

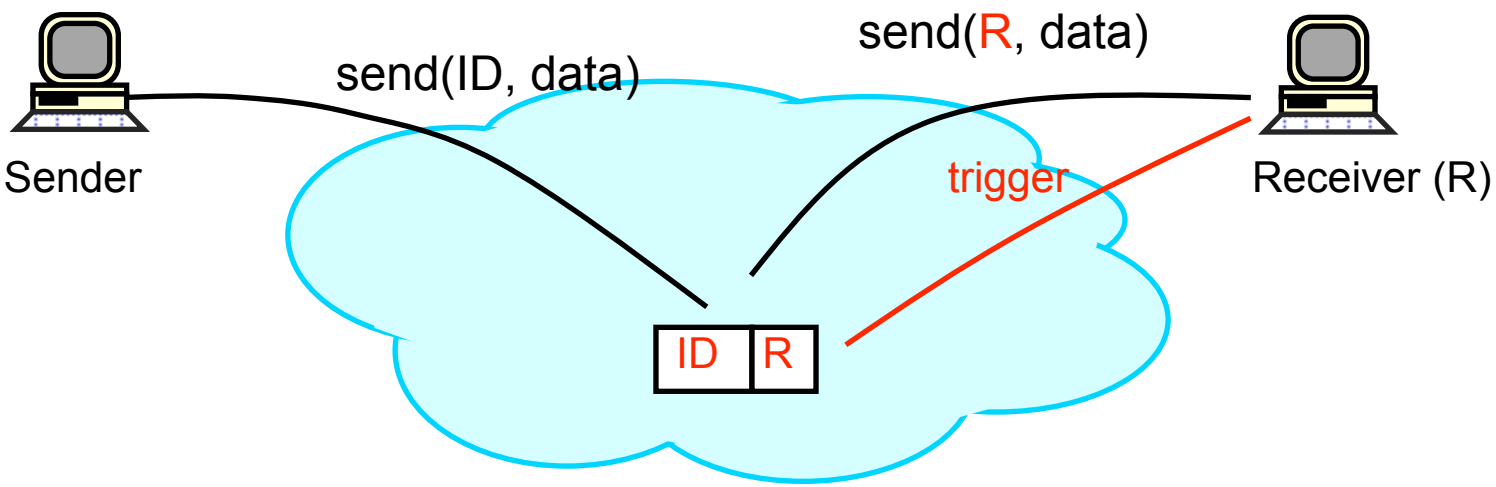
- i^3 overview
- Secure i^3 principles
- Diluting a DoS/DDoS attack in i^3

i^3 overview

- Efficient indirection layer on top of IP
  - Overlay network consisting of rendezvous servers
- Rendezvous based communication abstraction
  - Each packet has a recipient identifier
  - Rendezvous servers maintain triggers
- Trigger is an (id, destination) pair
  - Destination is typically an IP address

Rendezvous Communication

- Packets addressed to identifiers ("names")
- Trigger: (Identifier, IP address): inserted by receiver and then used by sender
- Triggers are mappings set up by end-hosts, and stored in DHTs (can point to other triggers too)



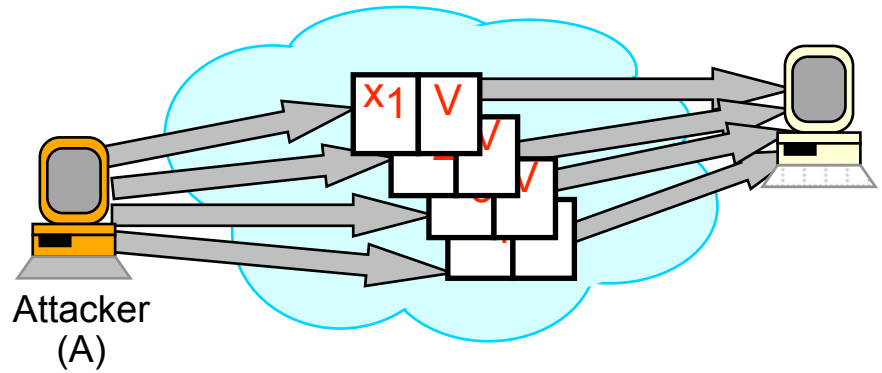
(Slide courtesy to Ian Stoica, UC Berkeley)

Secure i^3 principles

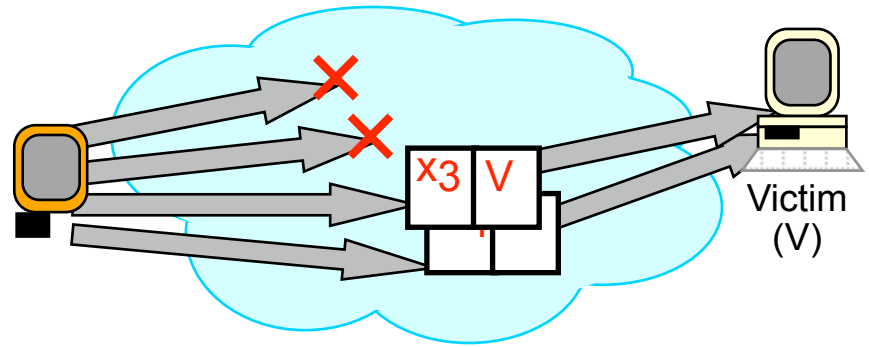
- Hide IP addresses
  - Must use overlay
- End-hosts have ability to defend against attacks (in the network)
- Don't create additional vulnerabilities

Diluting a DoS attack in i^3

Attacker floods victim via i^3 public triggers



Victim dilutes attack by dropping two of its four public triggers

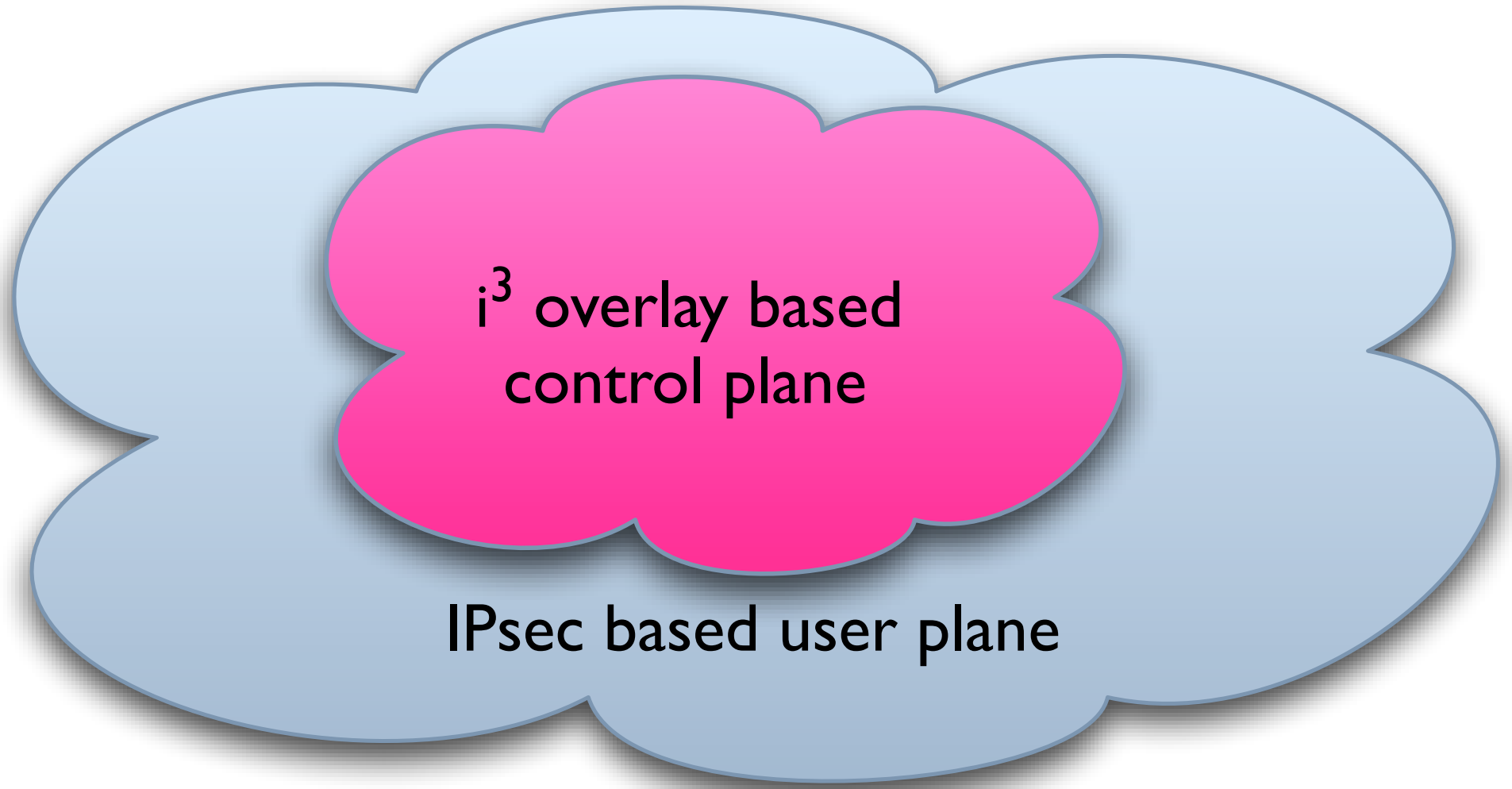


(Slide courtesy to Dan Adkins, UC Berkeley)

Hi^3

- Basic approach: Combine HIP and (Secure) i^3
  - Use i^3 as a transport for HIP packets
  - Use regular IP(sec) for regular data traffic
- Hides IP addresses until the Responder has been able to verify the puzzle
- HIP mobility and multi-homing can be used to redirect and redistribute regular traffic

Hi^3 overlay and IPsec connectivity



Hi^3 overlay and IPsec connectivity

- i^3 overlay for signalling (control plane)
  - Routes only HIP control packets
- E2E IPsec ESP for data traffic (user plane)
  - Firewalls/middle boxes opened dynamically
- Only end-to-end signalling (HIP)
  - Middle boxes "snoop" e2e messages

HIP vs IP connectivity

IP connectivity

Between any IP addresses

Created by routing

Hosts always reachable

Unsecure

Broken by NATs and FWs

HIP connectivity

Between any HITs

Created by DHT

Hosts reachable after signalling

(Opportunistically) Secure

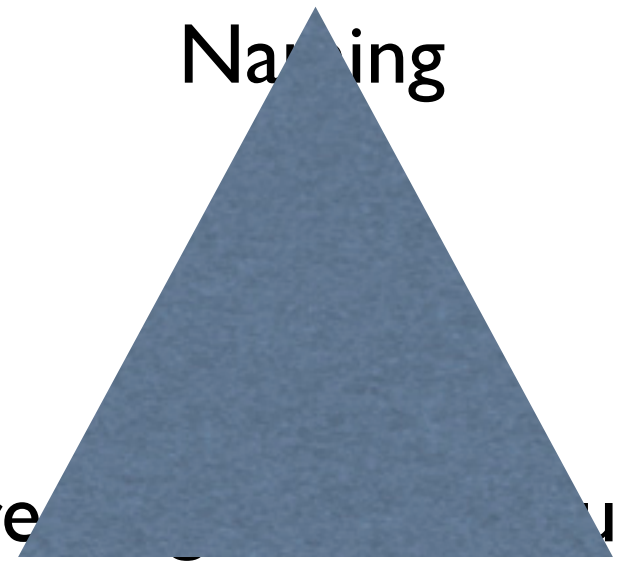
Goes through NATs and FWs

Upper layer view

- IP connectivity problematic today
  - Broken by firewalls, NATs, mobility
  - Two versions of IP: IPv4 and IPv6
- Hi^3 as a potential remedy
  - Restores end-to-end connectivity
  - Handles mobility and multi-homing
  - Protects from DDoS attacks

Where is network state?

- Routers know addresses
  - Just like today
- DHT knows HITs
  - Lease based storage
- Middle boxes know SPIs
  - Soft state



Summary

- Combine HIP and i^3
  - HIP packets flow through i^3 overlay
  - Regular traffic over today's IP
- IP addresses hidden in the beginning
- Solves the HIT referral problems
- Protects from DDoS attacks