End-To-End Privacy for Identity & Location with IP Saleem N. Bhatti, **Gregor Haywood**, Ryo Yanagida

### Service Routing and Addressing IETF112 RTG/INT side meeting (online) 10 Nov 2021

This talk is based on a paper presented at:

NIPAA21 – 2<sup>nd</sup> Workshop on New Internetworking Protocols, Architecture and Algorithms,

29th IEEE International Conference on Network Protocols,

01 Nov 2021

Paper preprint: https://saleem.host.cs.st-andrews.ac.uk/publications/2021/nipaa21/nipaa21.bhy2021.pdf



### The Ties that un-Bind: Decoupling IP from web services and sockets for robust addressing agility at CDN-scale

Marwan Fayed<sup>†</sup>, Lorenz Bauer<sup>†</sup>, Vasileios Giotsas<sup>†</sup>, Sami Kerola<sup>†</sup>, Marek Majkowski<sup>†</sup>, Pavel Odinstov<sup>†</sup>, Jakub Sitnicki<sup>†</sup>, Taejoong Chung<sup>\*</sup>, Dave Levin<sup>‡</sup>, Alan Mislove<sup>ø</sup>, Christopher A. Wood<sup>†</sup>, Nick Sullivan<sup>†</sup> <sup>†</sup> Cloudflare, Inc. \* Virginia Tech <sup>‡</sup> University of Maryland <sup>ø</sup> Northeastern University

#### ABSTRACT

The couplings between IP addresses, names of content or services, and socket interfaces, are too tight. This impedes system manageability, growth, and overall provisioning. In turn, large-scale content providers are forced to use staggering numbers of addresses, ultimately leading to address exhaustion (IPv4) and inefficiency (IPv6).

In this paper, we revisit IP bindings, entirely. We attempt to evolve addressing conventions by decoupling IP in DNS and from network sockets. Alongside technologies such as SNI and ECMP, a new architecture emerges that "unbinds" IP from services and servers, thereby returning IP's role to merely that of reachability. The architecture is under evaluation at a major CDN in multiple datacenters. We show that addresses can be generated randomly *per-query*, for



Figure 1: Conventional IP bindings to names, interfaces, and sockets, create transitive relationships between them that are difficult to track and reason about, which hinders changes to any binding without risking others.

#### SIGCOMM, Sep 2021 - https://dl.acm.org/doi/10.1145/3452296.3472922

🕨 🔍 💽 rfc6	6740	× +			V
1 ▷ C □ 🔒 datatracker.ietf.org/doc/html/rfc6740 🛛 🖓 🛆 Ξ					
Atkinson & Bhatti		Experimental		[Page 7]	
<u>RFC 6740</u>		ILNP Arch		November 2012	
	Layer	IP	ILNP		
App Tra Net Phy	lication   nsport   work sical i/f	FQDN or IP Address IP Address IP Address IP Address IP Address	FQDN Identifier Locator MAC address		
 FQDN = Fully Qualified Domain Name i/f = interface MAC = Media Access Control					
Table 1: Use of Names for State Information in Various Communication Layers for IP and ILNP					

As shown in Table 1, if an application uses a Fully Qualified Domain Name at the application-layer, rather than an IP Address or other lower-layer identifier, then the application perceives no architectural difference between IP and ILNP. We call such applications "well-behaved" with respect to naming as use of the FQDN at the application-layer is recommended in [<u>RFC1958</u>]. Some other applications also avoid use of IP Address information within the

RFC6740(E), IRTF RRG, Nov 2012 - https://datatracker.ietf.org/doc/html/rfc6740

## Identity and Location Privacy



- Modular network stack makes:
  - Design and implementation easy
  - Privacy hard
- Objectives:
  - Stop on-path attacks exploiting wire image
  - Avoid expanding trust boundary

### **Internet** Location

- Upper 64 bits
- Used globally and managed globally
- Uniquely labels a **subnet**
- Determined by the ISP

#### IPv6 address format (RFC4291 + RFC3587)

64-bits	64-bits	
IPv6 Unicast Routing Prefix	IPv6 Interface Identifier (IID)	

### Node Identity



- Lower 64 bits (IID)
- Used globally but generated locally
- Uniquely labels an **endpoint**
- Determined by node (e.g. SLAAC)

#### ILNP Identifier-Locator Vector (I-LV) (RFC6741)

64-bits	64-bits		
ILNP Locator (L64)	ILNP <u>Node</u> Identifier (NID)		

### 5

## Ephemeral Node Identifiers (NIDs)

- NIDs: transport-layer node identifiers •
- Simultaneously use multiple
- Can be one-use









## Location Privacy



- Routing information must be visible on path
- Solution: use multiple paths



## Location Privacy



- Location is still exposed unless using VPN/Tor
- Locator Rewriting Relays (LRRs) achieve this without tunneling
- Potentially easier for attacker to correlate
  - ...but that may be inevitable either way



Bob

### **Emulation Overlay**





### Results

### Ephemeral NIDs and



No Defences







Multihoming









# Concluding

- ILNP's architecture is useful for privacy
  - Isolate each flow with ephemeral NIDs
  - Multihoming makes attacker's job harder
  - LRRs provide low-cost location privacy
- Thank you!

