



# Measurement and Analysis of IPv6 Interface Identifier Patterns in the Real World

draft-ren-v6ops-ipv6-iid-patterns-measurement-00

Gang Ren<sup>1</sup>, Wei Zhang<sup>1</sup>, Xia Yin<sup>1</sup>, Lin He<sup>1</sup>, Haisheng Yu<sup>2</sup>

<sup>1</sup>Tsinghua University, <sup>2</sup>CNNIC



# Contents

- Background & Motivation
- Measurement Methodology
- Results and Analysis
- Conclusion

## Background & Motivation

### The Past

- RFC 7707 (Published 2016): Baseline for network reconnaissance.
- Data from 2012-2013: EUI-64 & Low-byte patterns were dominant.



### The Evolution

- Privacy Standards Boom: RFC 7217 (Opaque), RFC 8981 (Temporary), RFC 8064 (Deprecate EUI-64).
  - OS Default Changes: Windows, Linux, Android, iOS widely adopted privacy extensions.
- The IPv6 ecosystem has fundamentally changed. How do these standards impact real-world address patterns today? And what does it mean for modern network defense?

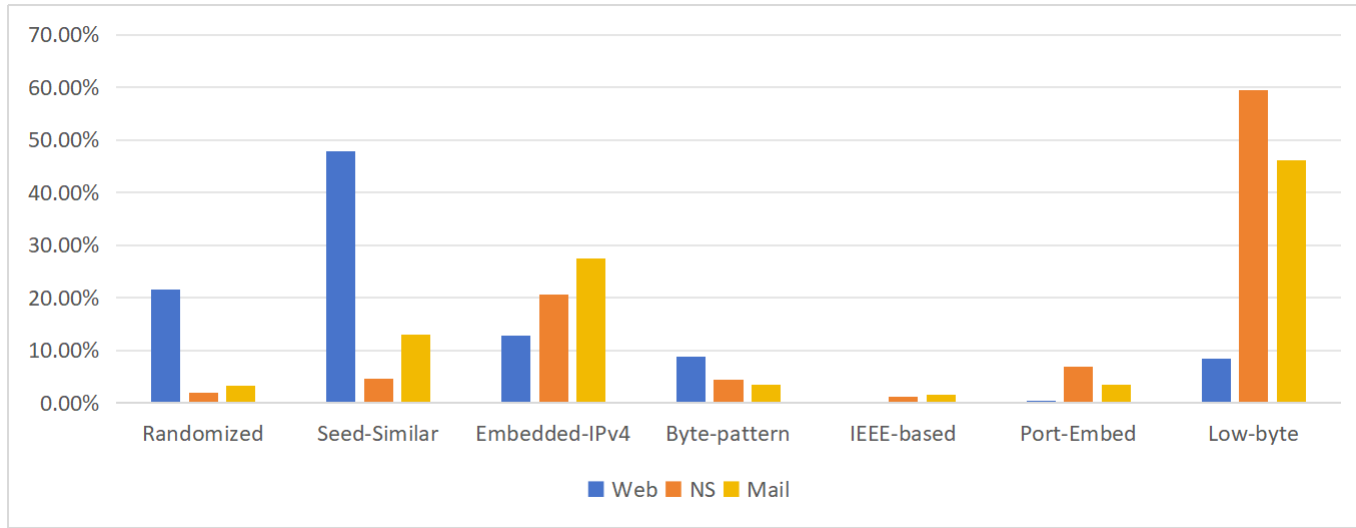
# Measurement Methodology: Data Sources

- Servers
  - Public Domains (Alexa, Tranco, .etc) :AAAA, MX, NS records
- Clients
  - BitTorrent DHT Network: Passive end-user collection
  - Public Mailing Lists: Extract sender IPs + Timestamps from Email Headers
    - Enables decade-long longitudinal tracking!
- Routers
  - BGP Prefixes -> Traceroute
  - Clients -> Traceroute: Edge

## Measurement Methodology: Interface ID Pattern Recognition

- **Old Method (RFC 7707 / addr6)**
  - Known Rules (EUI-64, Low-byte, etc.) → Everything else "Randomized" (High False Positives)
  - Non-random configs like ffff:ffff:ffff:abcd
- **Our Improved Method**
  - **Seed-Similar Pattern**
    - Known Rules (EUI-64, Low-byte, etc.) → **Compare with Seed List (First/Last 4 bytes)** → Everything else "Randomized"
- **Reduced false "Randomized" classification in servers by ~69%!**

# Server Patterns



## ■ Low-byte in RFC 7707

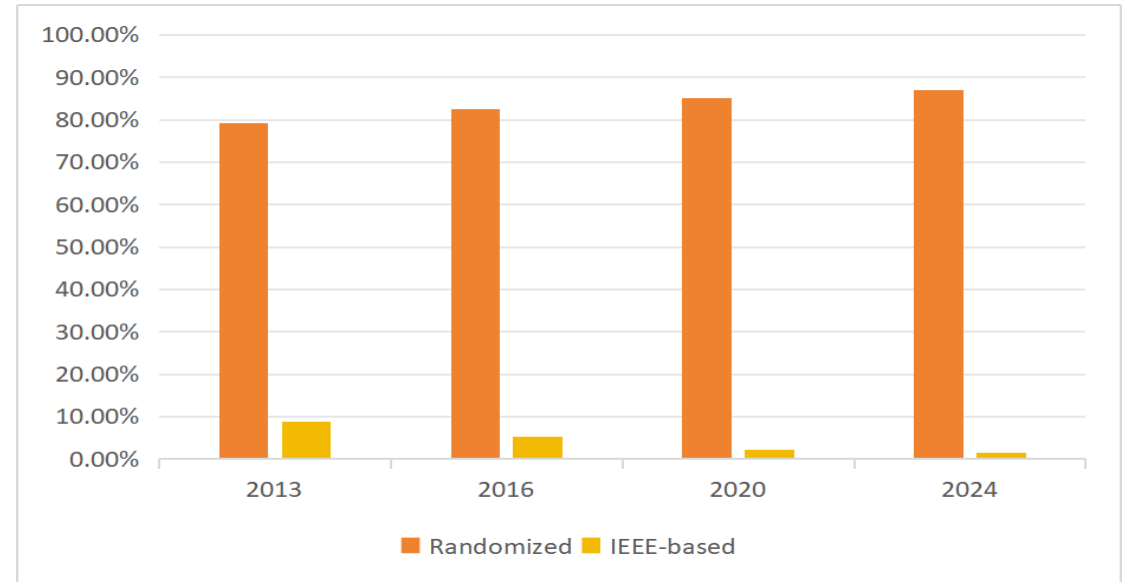
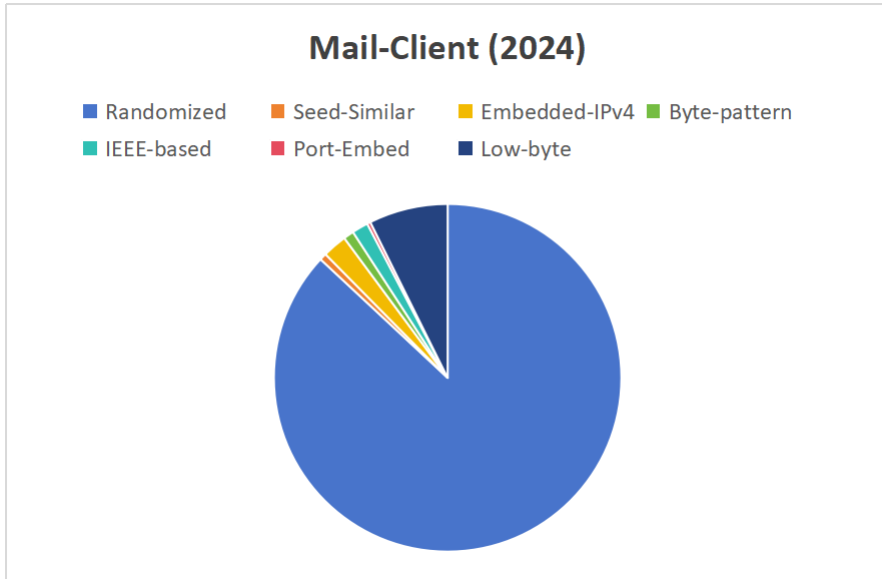
■ Web: 56.88%

■ NS: 56.58%

■ Mail: 92.65%

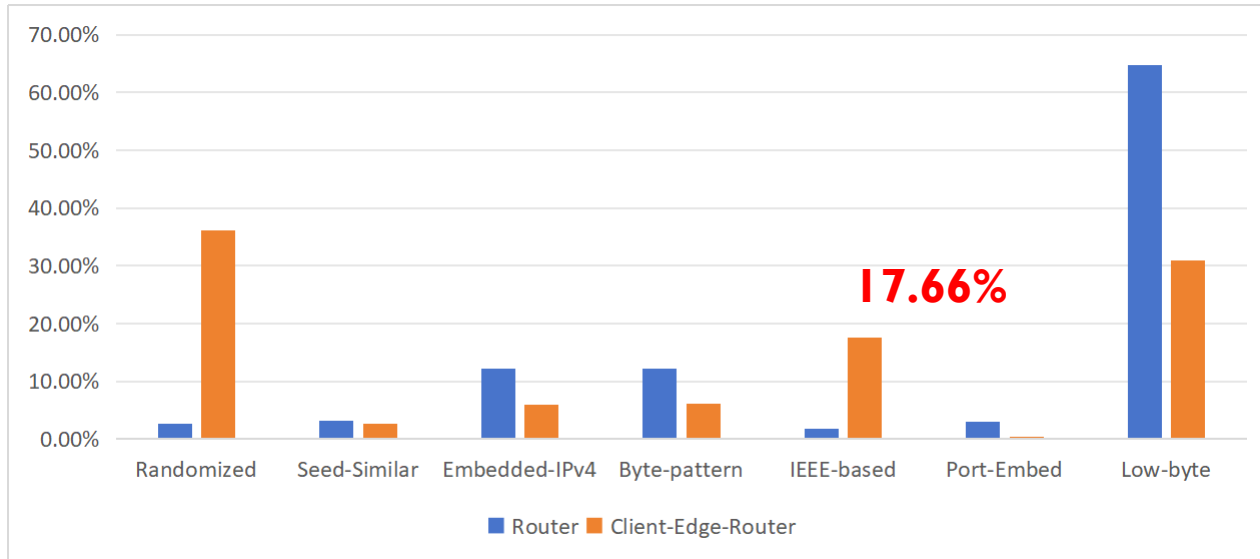
- Linear scanning (::1 to ::ff) is significantly less effective today.
- However: ~48% of Web servers are "Seed-Similar" (Not truly random).
- Result: Target Generation Algorithms (TGA) remain a highly viable reconnaissance vector.

# Client Patterns



- RFC 8981 (Temporary) & RFC 7217 (Stable Opaque) are overwhelmingly deployed.
- End-user tracking via MAC addresses is largely mitigated.

# RouterPatterns



- **Low-byte in RFC 7707**
- **Router: 70.00%**

- The Problem: Nearly 1 in 5 home gateways still defaults to EUI-64.
- The Impact: Acts as a "Super Cookie" for the entire home network. Exposes vendor OUI & enables persistent tracking.

## Conclusion

- Update Threat Models
  - RFC 7707 stats are outdated. We must update defensive models.
- Move Beyond Obscurity
  - Manual configurations (Seed-Similar) are easily exposed by modern scanning algorithms.
- Enforce RFC 8064 on CPEs
  - Call to action: Operators and the IETF community must push vendors to deprecate EUI-64 on edge devices to close the privacy gap.



# Q&A

Wei Zhang: [zhang-w22@emails.tsinghua.edu.cn](mailto:zhang-w22@emails.tsinghua.edu.cn)

Gang Ren: [rengang@cernet.edu.cn](mailto:rengang@cernet.edu.cn)