End-To-End Privacy for Identity & Location with IP

Saleem N. Bhatti, Gregor Haywood, Ryo Yanagida

University of
St Andrews

29th IEEE International Conference on Network Protocols
November 1st 2021

Identity and Location Privacy

University of St Andrews

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

Internet Location

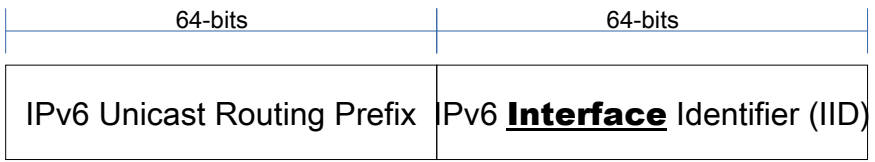
- Upper 64 bits
- Used **globally** and managed **globally**
- Uniquely labels a **subnet**
- Determined by the ISP

Node Identity

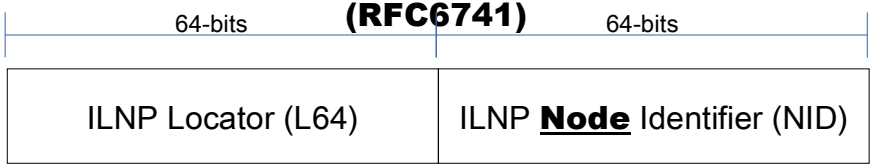
- Lower 64 bits (IID)
- Used **globally** but generated **locally**
- Uniquely labels an **endpoint**
- Determined by node (e.g. SLAAC)

University of St Andrews

IPv6 address format (RFC4291 + RFC3587)



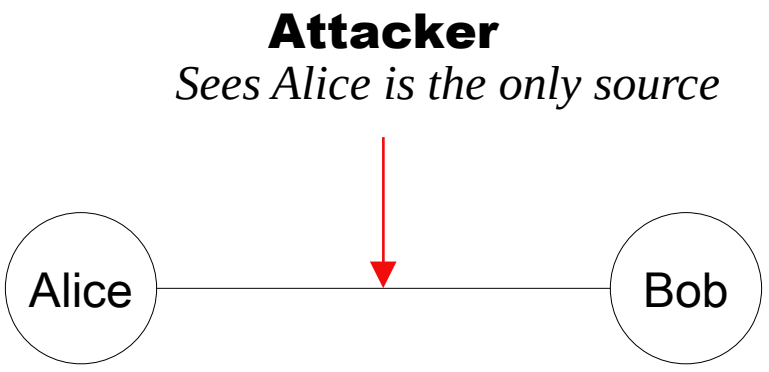
ILNP Identifier-Locator Vector (I-LV) (RFC6741)

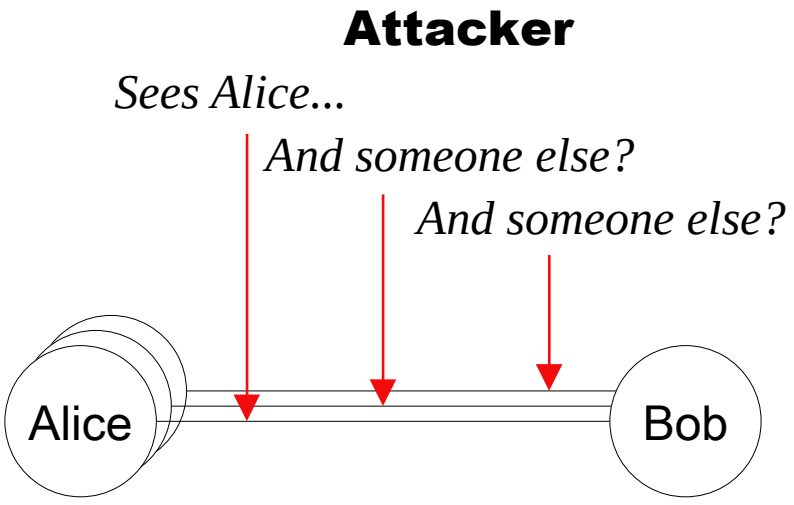


Ephemeral Node Identifiers (NIDs)

University of St Andrews

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

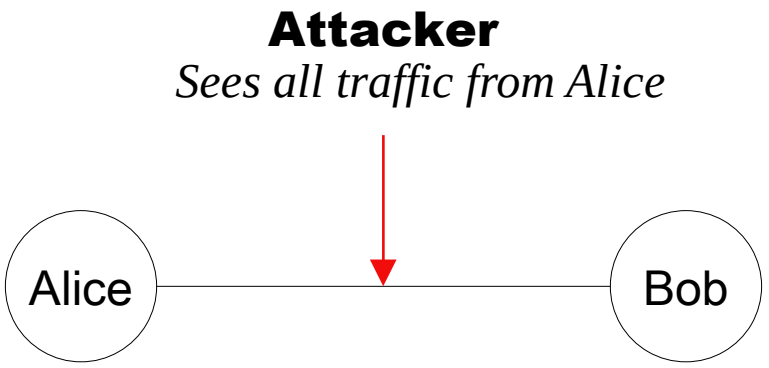


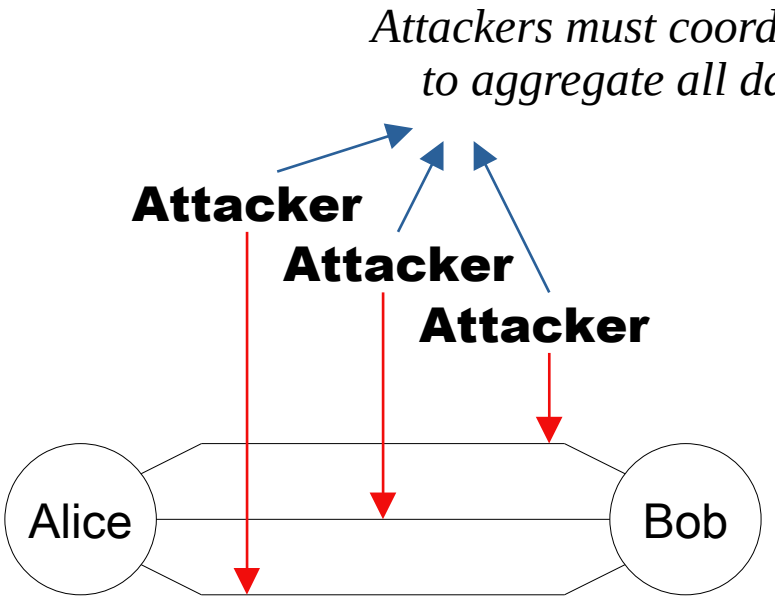


Location Privacy

University of St Andrews

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

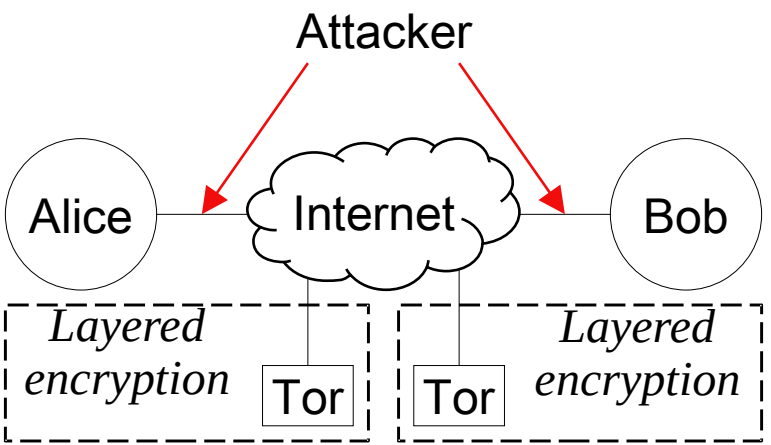


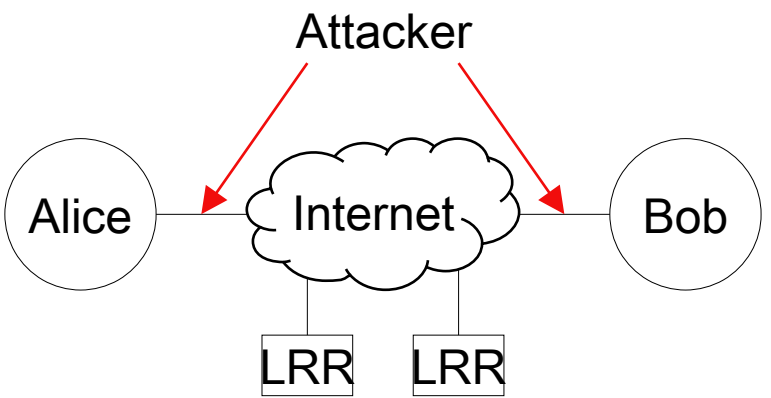


Location Privacy

University of St Andrews

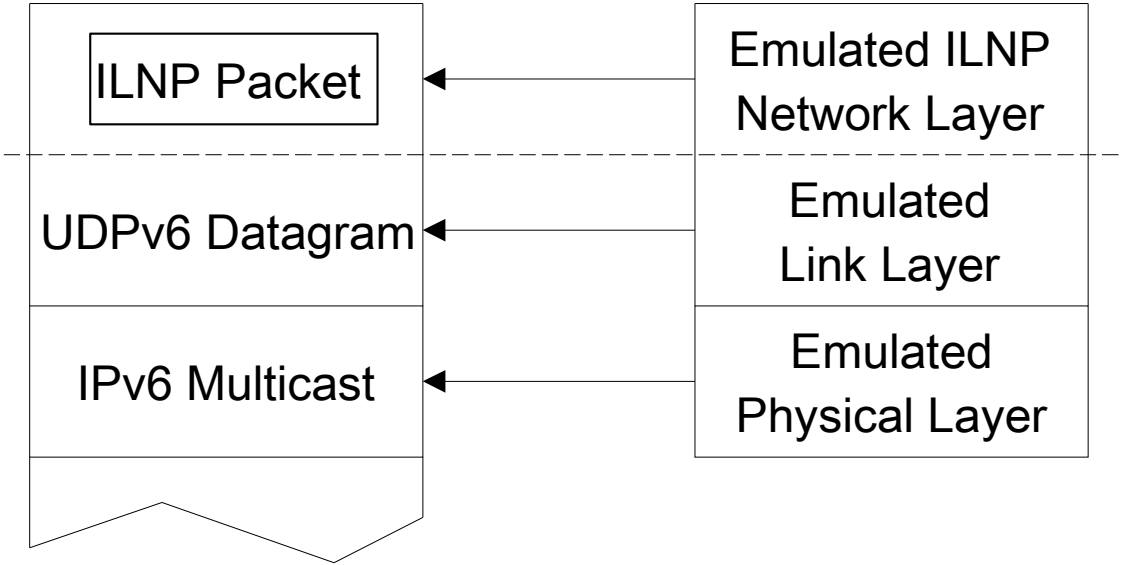
- Location is still exposed unless using VPN/Tor
- Locator Rewriting Relays (LRRs) achieve this without tunneling
- Potentially easier for attacker to correlate
  - ...but that may be inevitable either way

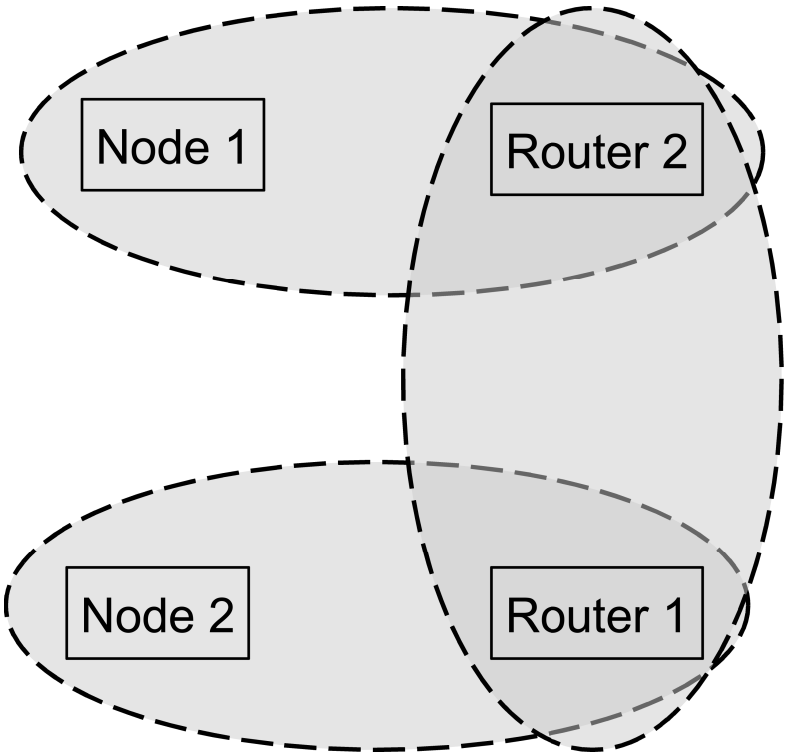




Emulation Overlay

University of St Andrews

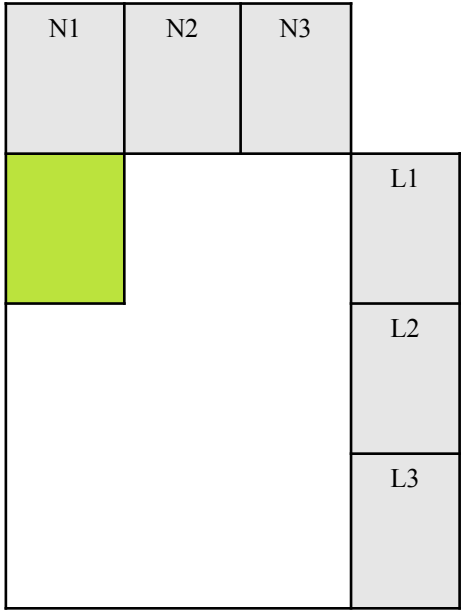


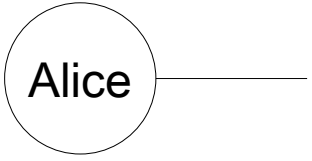


Results

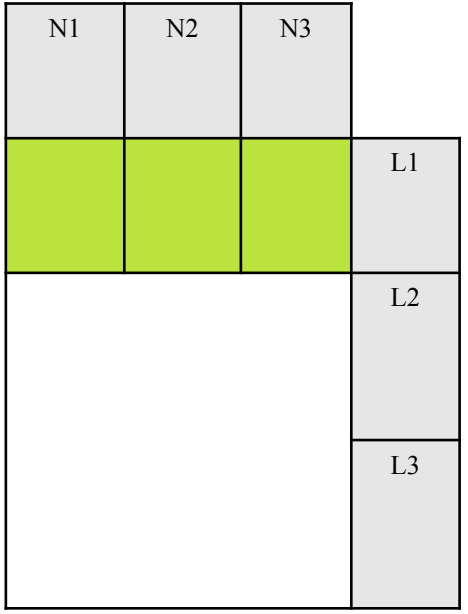
University of St Andrews

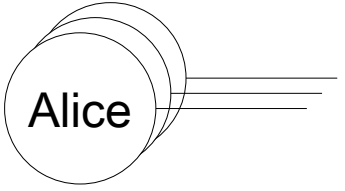
No Defences



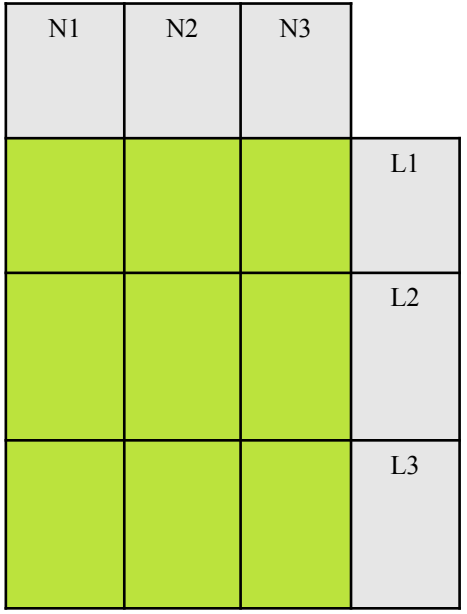


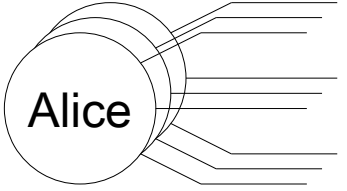
Ephemeral NIDs





Ephemeral NIDs and Multihoming





Concluding

University of St Andrews

- 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!