Balancing Accountability and Privacy in the Internet

David Naylor, Matthew K. Mukerjee, Peter Steenkiste

Accountability vs. Privacy

Accountability

know who sent a packet so we can punish them if they do bad things

↓

unforgeable **source address**

VS

Privacy

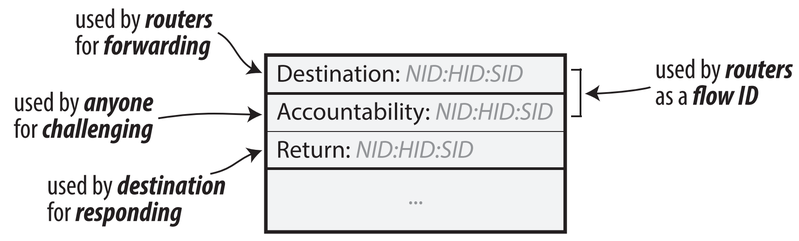
hide a packet's sender so activity can't be linked to them

↓

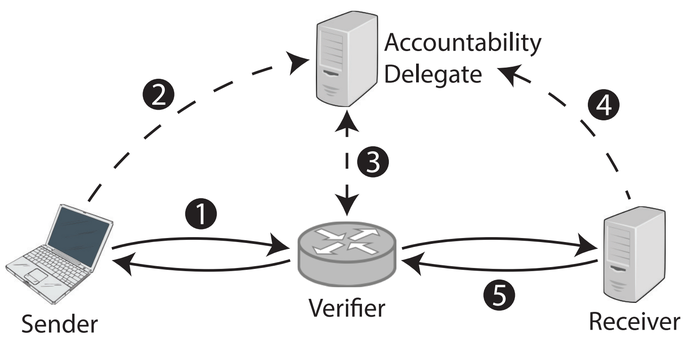
hidden **source addresses**

Observation:

Source addresses are overloaded. Why not separate **accountability** and **return address** roles into different header fields?



Delegated Accountability



❶ The **sender** sends a packet with an *accountability address* identifying its **accountability delegate**.

❷ The **sender** "briefs" its **delegate** about the packet it just sent.

❸ A **verifier** (e.g., any on-path router) can verify with the **delegate** that the packet is a valid packet from one of the delegate's clients.

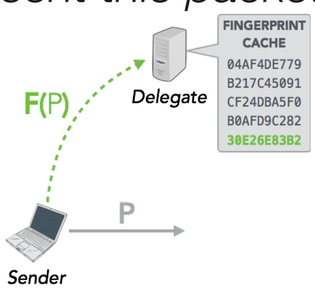
❹ If the **receiver** determines that packets are malicious, it uses the *accountability address* to report the flow to its **delegate**.

❺ The **receiver** uses the *return address* in the request as the destination address in the response.

Delegate Interface

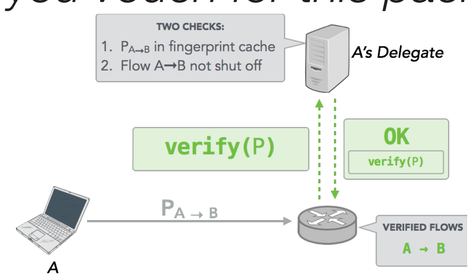
`brief()`

"I sent this packet."



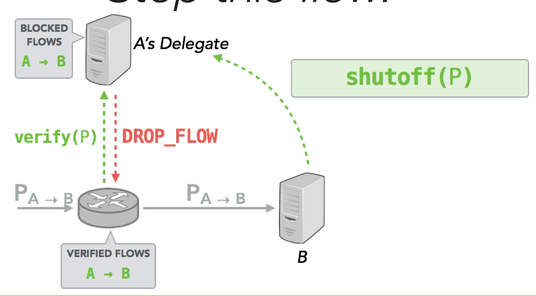
`verify()`

"Do you vouch for this packet?"



`shutoff()`

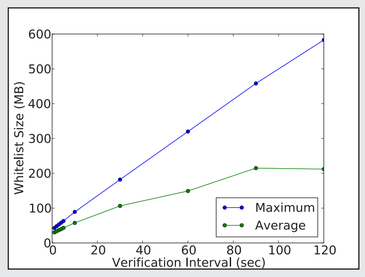
"Stop this flow."



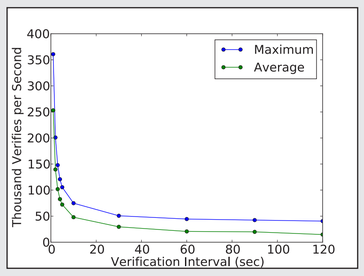
Is it technically feasible?

We evaluate the feasibility of delegated accountability with a trace of CMU network activity from July 2013 containing 10 million flows.

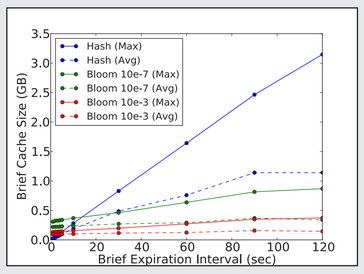
Whitelist Size



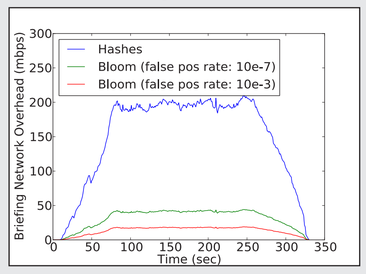
Verification Rate



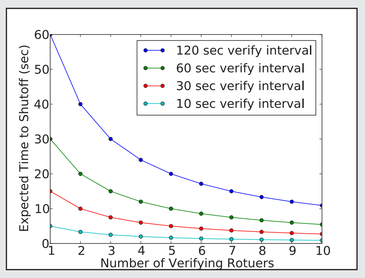
Brief Cache Size



Briefing Overhead



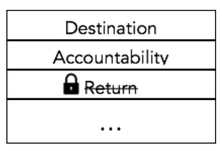
Time to Shutoff



Hiding Return Addresses

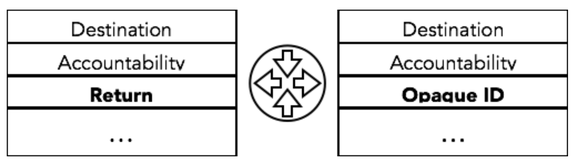
Example 1: E2E Encryption

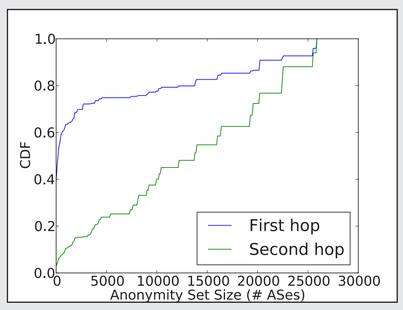
To hide the return address from **local observers or transit networks**, simply encrypt it end-to-end.



Example 2: NAT

To hide the return address from **the recipient or transit networks**, the sender's border router acts as a NAT.





◀ *Anonymity Set Size*

With a hidden return address, a packet's anonymity set grows the farther it travels from the sender.

50% of ASes have 180 "first-hop" siblings.
90% have 900 "second-hop" siblings

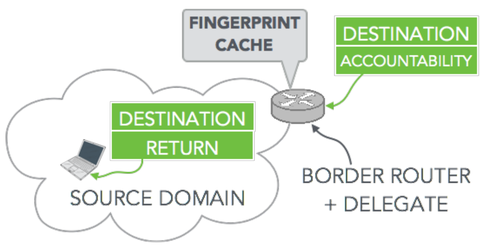
Deployment Models

Specialized Companies as Delegates

→ No burden on source domains (economy of scale)

→ Larger anonymity set

Source Domains as Delegates



→ No briefing overhead (router saves briefs as packets go by)

→ Lower verification latency

Carnegie Mellon University
BOSTON UNIVERSITY
THE UNIVERSITY of WISCONSIN MADISON
Duke UNIVERSITY

This work is part of the XIA future Internet architecture project:
www.cs.cmu.edu/~xia

This work is supported in part by NSF Grant #1040801 and NDSEG Fellowship 32 CFR 168a.