FABRID: Flexible Attestation-Based Routing for Inter-Domain Networks

Cyrill Krähenbühl, Marc Wyss, David Basin, Vincent Lenders,
Adrian Perrig, Martin Strohmeier
32nd USENIX Security Symposium, 9-11 August 2023

Presented by Andrew Stepanov
11 March 2025

Motivation and Problem Description

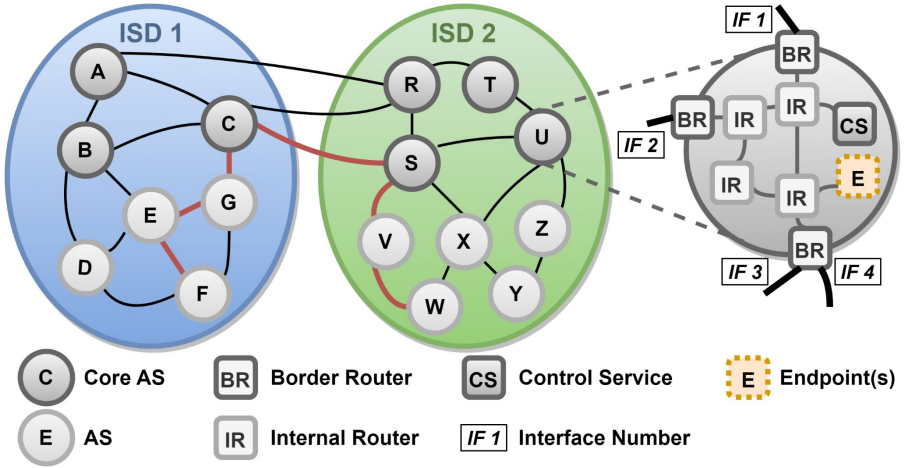
Users of the Internet do not get a say in how their packets are forwarded. This could lead to distrust from users, especially ones whose packets are contain sensitive information.

“Traffic is only received by network layer devices (routers) with attributes acceptable to the endpoints.”

- Users should be able to select attested paths based on fine-grained properties and verify that their packets were sent down their selected paths.
- Users’ packets should not reveal their desired attributes.
- Autonomous systems should not have to divulge their topology or risk having their machines targeted by Denial of Service attacks.
- Paths should be stable and efficient.

Background: Foundations in SCION

- Every AS has a Control Service that handles routing info, including paths that endpoints choose from.
- Packet headers contain endpoints' desired paths.
- Public keys of ASes are exchanged on the control plane.
- ASes are grouped into isolation domains with core ASes.
  - Traffic within an isolation domain is sent to and from core ASes. Traffic between isolation domains is sent between core ASes.
  - Core ASes handle path-segment construction beacons.



Background: Other Leveraged Works

DRKey:

- It is fully implemented in SCION.
- It is a protocol for setting up symmetric keys.
- It ensures secrecy of policy indices in users' packets.

EPIC:

- It is a partially implemented data plane extension for SCION.
- It provides source authentication and path validation.

FABRID

ASes advertise the existence of paths of routers with common attributes.

- They piggyback these ads on path-segment construction beacons.
- These include indexes to policies local to an AS or policies in a global registry.

Attestation is used to ensure ASes are honest.

Endpoints include preferences in packet headers.

Policies are specified using “simple” first-order-logic formulas.

$$
\begin{aligned}
PrefPol_u(r) \;:=\; & \left(\texttt{manu}(r) = m_1 \vee \texttt{manu}(r) = m_2\right) \\
& \wedge \forall c \in \mathcal{C} : \left(\texttt{software}(r,c) \wedge \texttt{name}(c) = s_{\text{crit}}\right. \\
& \left. \wedge\, \texttt{issuer}(\texttt{tag}(c)) = i\right) \rightarrow \texttt{version}(c) \geq v_{\min}
\end{aligned}
$$

Evaluation

FABRID was implemented in SCIONLab, a networking testbed specifically for experimenting with SCION.

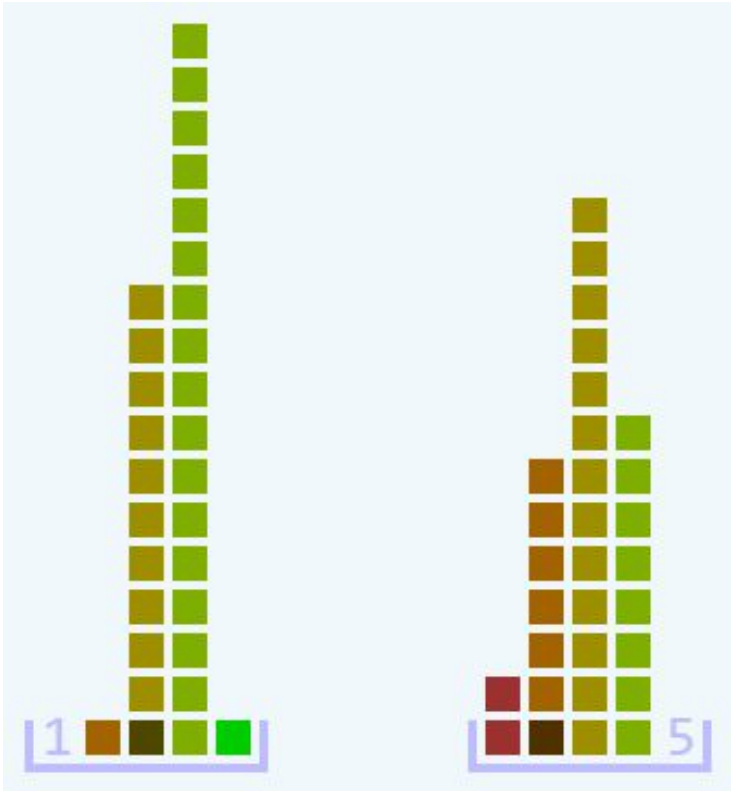
The authors tested backwards compatibility with SCION and evaluated FABRID's overhead.

Compared to EPIC:

- FABRID is 7%-20% slower.
- FABRID has a ~17% decrease in throughput.

Attestation takes approximately 2.4 seconds.

Scores



Discussion

Who would actually want to use FABRID?

- Succeeding in FABRID could require substantial investment from ASes.
- Should subsidies or other incentives be offered to ASes for using FABRID?
- Would regular users want FABRID?
- Is FABRID's target audience governments and large corporations?

Many of us found the assumption of benign ASes to be quite lax given that they are monetarily incentivized.

- How malicious should we consider ASes to be?
- Could a reputation system help prevent malicious actions by ASes?

Some of us are worried about FABRID being used for censorship.

Discussion

A lot of us were worried if FABRID could scale, especially to the size of the Internet.

- Could an append-only global registry keep up with policies and attestation?
- What stopping policies from becoming excessively numerous and overcomplicated.
- A lot of traffic goes through core ASes.

The authors interpreted the performance drops of FABRID as insignificant, but we were more skeptical of the performance in our reviews.

- Are the performance drops significant?
- Could this deter users from using FABRID? No one wants slower Internet.
- Could this deter ASes from using FABRID? Time is money.