EPIC

Every Packet Is Checked in the Data Plane of a Path-Aware Internet

Markus Legner, Tobias Klenze, Marc Wyss,
Christoph Sprenger, and Adrian Perrig

ETH zürich

USENIX Security Symposium 2020

Imagine an Internet in which . . .

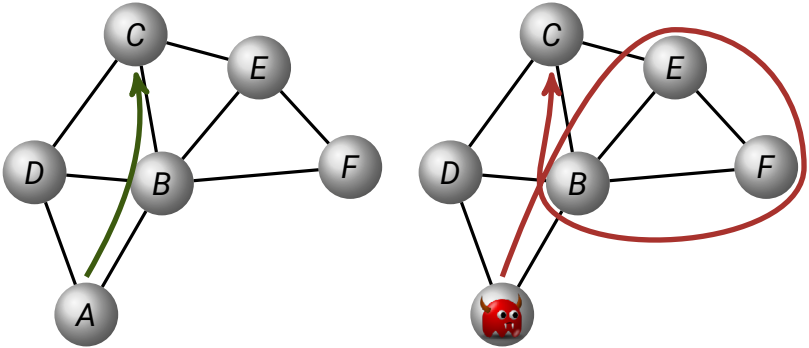
- . . . source-address spoofing is no longer possible as each packet's source can be verified by every router;
  Source Authentication
- . . . route hijacks are a problem of the past;
  Secure Routing
- . . . end hosts have control over the path of their packets;
  Path Control
- . . . end hosts can verify the actual path of their packets.
  Path Validation

Such an Internet exists already.

- Under development since 2010, today offered by several ISPs and in production use for several critical applications.
- SCION has two core components:
  - The *control plane* discovers paths; secured by signatures.
  - The *data plane* forwards data traffic; secured by symmetric cryptography.
- SCION is *path aware*: end hosts select a path to use and embed it in the packet header.
- OPT extension provides source authentication and path validation.

Power needs to be balanced between end hosts and network operators.

- In path-aware networks, hosts embed their chosen path in each packet.
- New challenge:
  How can autonomous systems pre-select allowed paths?

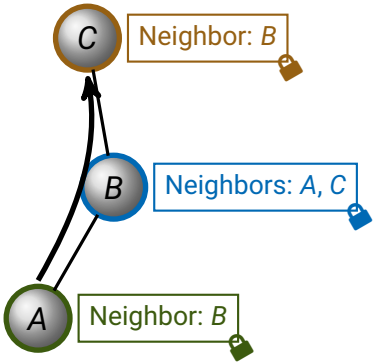


Power needs to be balanced between end hosts and network operators.

- In path-aware networks, hosts embed their chosen path in each packet.
- New challenge:
  How can autonomous systems pre-select allowed paths?
  Path Authorization
- SCION and other path-aware network architectures achieve path authorization through cryptographic tokens.
  - On today's hardware, cryptographic operations can be several times faster than memory lookups.
  - With hardware acceleration, encrypting/decrypting one AES block only requires ~10 ns on commodity CPUs.

SCION computes tokens in its control plane and checks them in the data plane.

- Autonomous systems exchange signed routing messages and collect path information:
  - local routing information (neighbors);
  - a cryptographic token, calculated as a message authentication code (MAC).
- Routing information is used in the data plane to determine where to forward packets.
  - Removes the need for huge forwarding tables.
  - Routers no longer need to perform longest-prefix matching.
- Token is checked to enforce path authorization.



The current approach suffers from a trade-off between overhead and security.

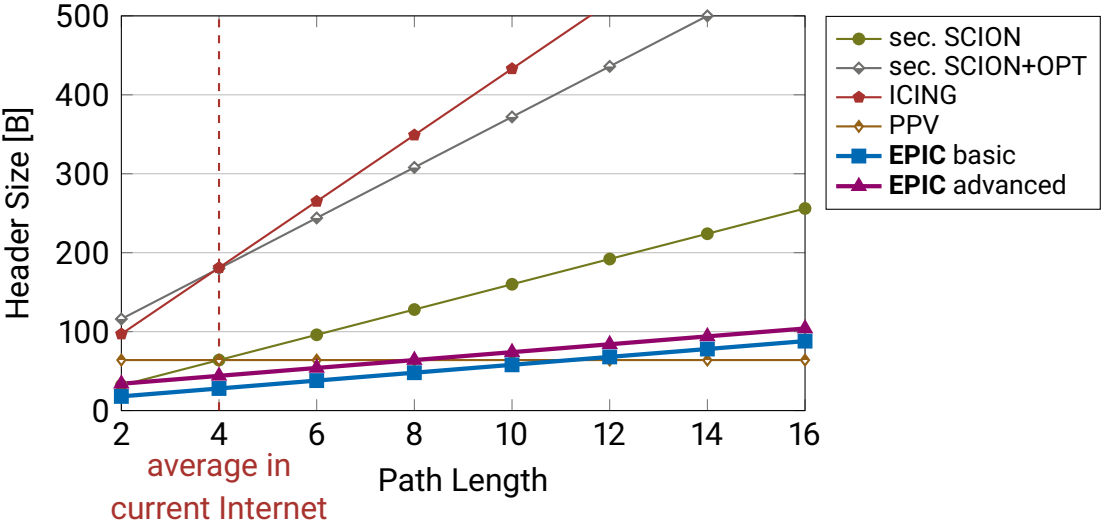
- Each hop of the path requires a token in the packet header.
- Each token must be long enough to withstand brute-force attacks.
- Core issue: even if the probability of forging a token is small, *a once-forged token can be reused for sending many packets*.

EPIC resolves the dilemma between communication overhead and security.

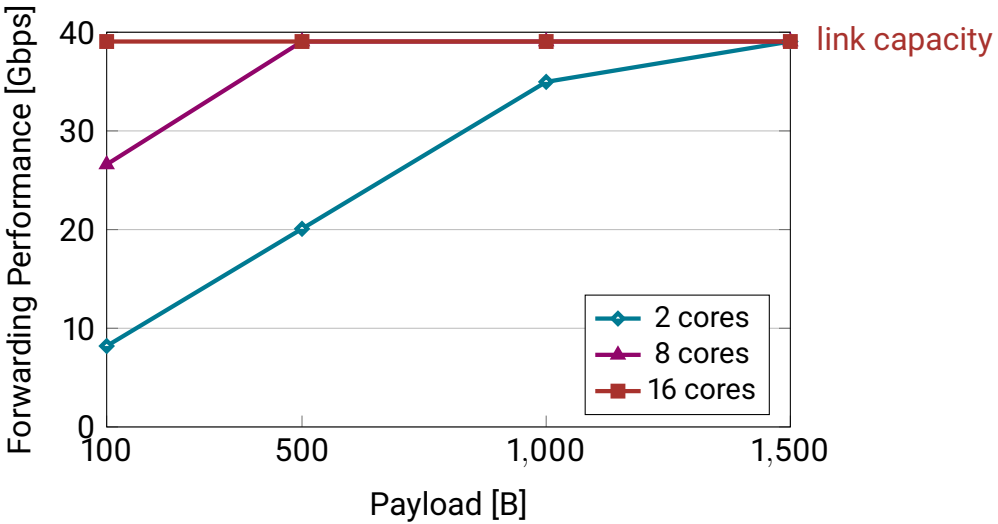
- Observation: *individual* forged packets are no threat to autonomous systems.
- By replacing static tokens by longer keys to compute *short per-packet MACs*, EPIC prevents the reuse of forged tokens.
- An attacker still has a small chance of forging a MAC to traverse an unauthorized link but this is limited to a *single* packet.
- Destination can filter packets based on a separate, unforgeable MAC.
- Source authentication and path validation are enabled by the additional use of efficiently derivable symmetric keys.
  - Previous systems (OPT, ICING) were too expensive to be used on every packet.

EPIC enables *path authorization*, *source authentication* by every router, and *path validation* by the destination with very small computation, storage, and communication overhead.

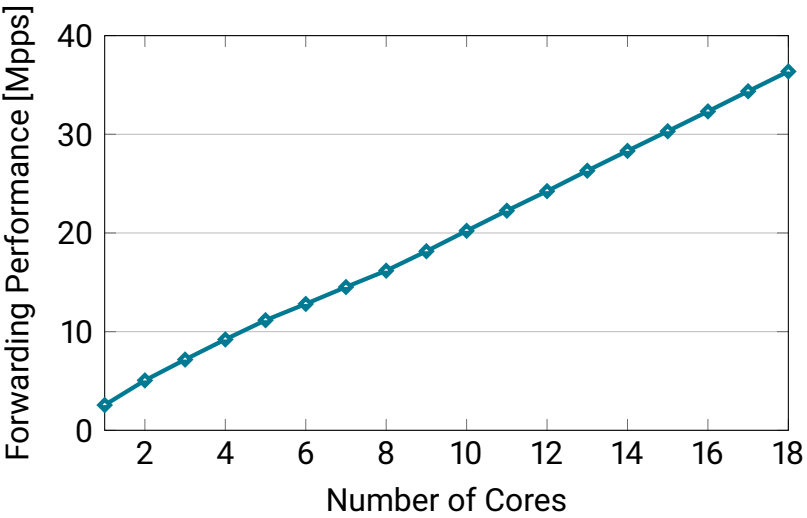
EPIC has low communication overhead.



EPIC is highly efficient and parallelizable.



EPIC is highly efficient and parallelizable.



EPIC achieves strong security properties while being highly efficient.

- ✓ EPIC solves multiple challenges of path-aware Internet architectures:
  - ✓ Strong path authorization—prevent reuse of forged packets.
  - ✓ Routers and destination can authenticate the source of all packets.
  - ✓ Source and destination can verify the path of a packet.
- ✓ Routers do not have to keep per-flow or per-source state.
- ✓ Low communication overhead.
- ✓ Low computational overhead:
  - ✓ Few AES operations in each router.
  - ✓ Checks can be parallelized with other packet processing.
- ✓ EPIC is efficient enough such that every packet can be checked.

Thank you, and please get in touch.

EPIC: Every Packet Is Checked in the Data Plane of a Path-Aware Internet

Markus Legner, Tobias Klenze, Marc Wyss, Christoph Sprenger, and Adrian Perrig
Department of Computer Science, ETH Zurich, Switzerland
{markus.legner, tobias.klenze, marc.wyss, sprenger, adrian.perrig}@inf.ethz.ch

Abstract

An exciting insight of recent networking research has been that path-aware networking architectures are able to fundamentally solve many of the security issues of today's Internet, while increasing overall efficiency and giving control over path selection to end hosts. In this paper, we consider three important issues related to this new networking paradigm: First, network operators still need to be able to impose their own policies to rule out uneconomical paths and to enforce as compliance, when data is not allowed to leave a particular jurisdiction; privacy leaks, when BGP hijacking attacks are used to de-anonymize users [43]; or re-routing attacks being used to obtain fake certificates [10]. Another shortcoming of the current Internet is that there is no way for an end user to verify the *actual* path a packet took on its way to the recipient. While applications such as `traceroute` enable network probing, the obtained information cannot be trusted due to the lack of authentication [2, 4].

Email: markus.legner@inf.ethz.ch