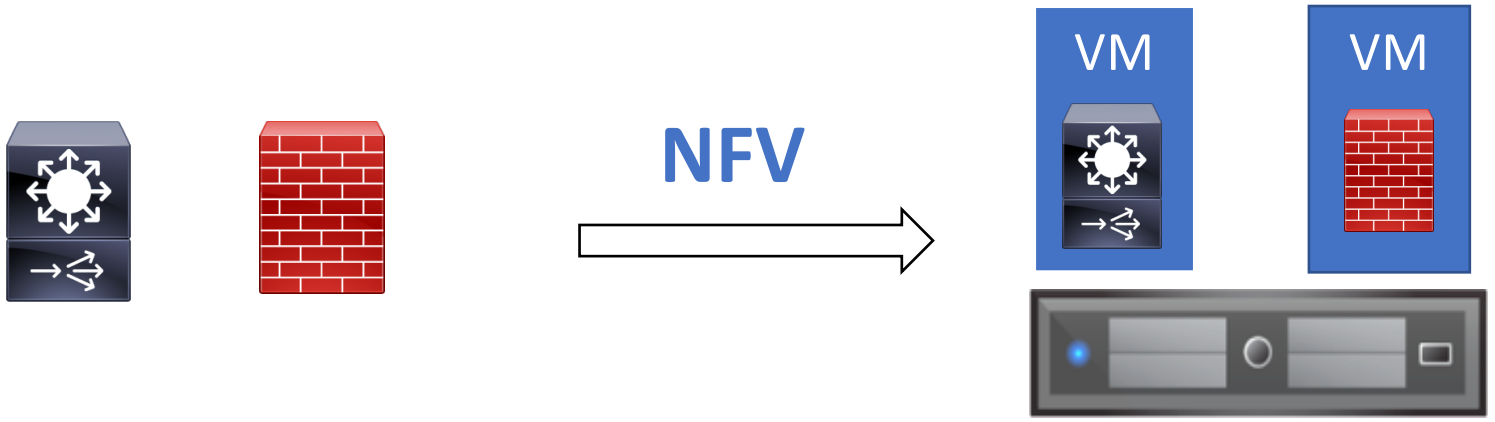
Don’t Yank My Chain:
Auditable NF Service Chaining

Guyue (Grace) Liu, Hugo Sadok, Anne Kohlbrenner,
Bryan Parno, Vyas Sekar, Justine Sherry

CyLab Carnegie Mellon University
Security and Privacy Institute

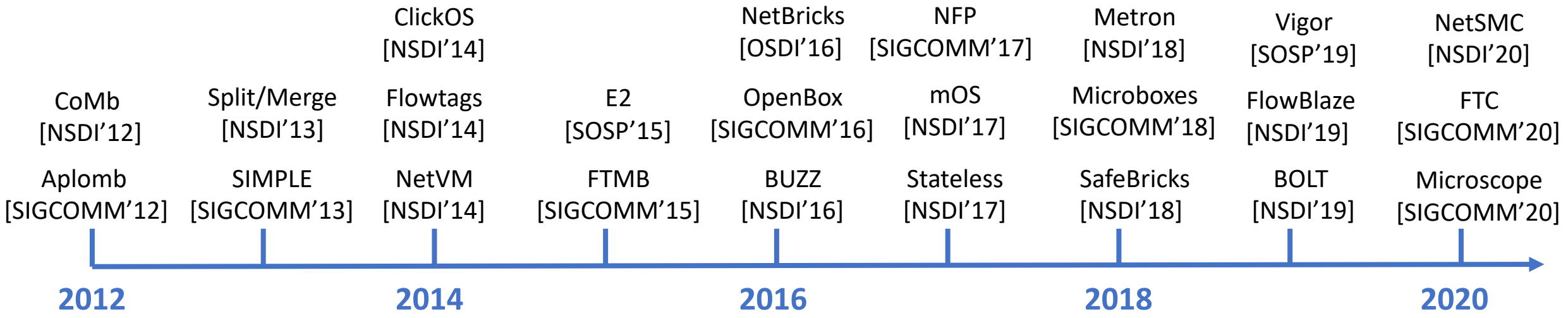
Network Function Virtualization (NFV)



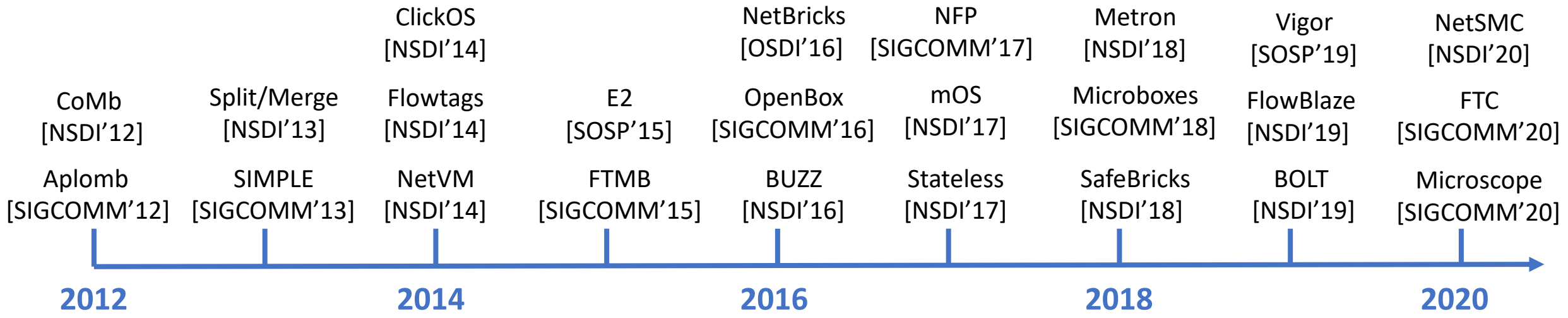
Specialized Appliances

Commodity Server

Academia Efforts To Promote NFV



Cloud-based Network Functions



Load Balancer

Web App Firewall

VPN

Firewall

VPN

Enterprises Are Reluctant To Adopt NFV

NFV

Current NFV Deployments Are Not Auditable

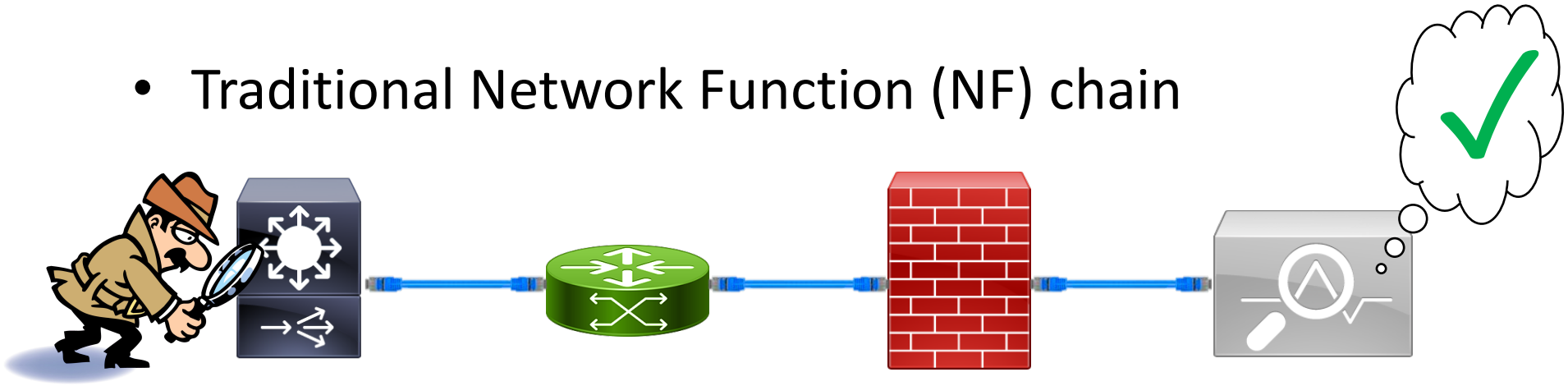
NFV

Why?

Cannot meet government and industrial regulations requirements, e.g., HIPAA, FERPA, GDPR, and PCI.

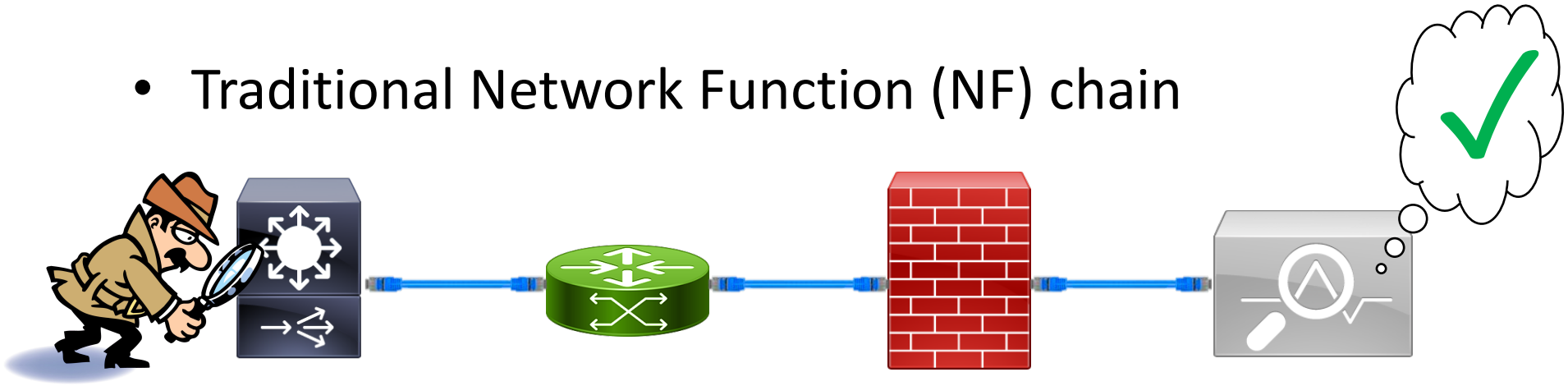
Traditional Auditing Approach

- Traditional Network Function (NF) chain

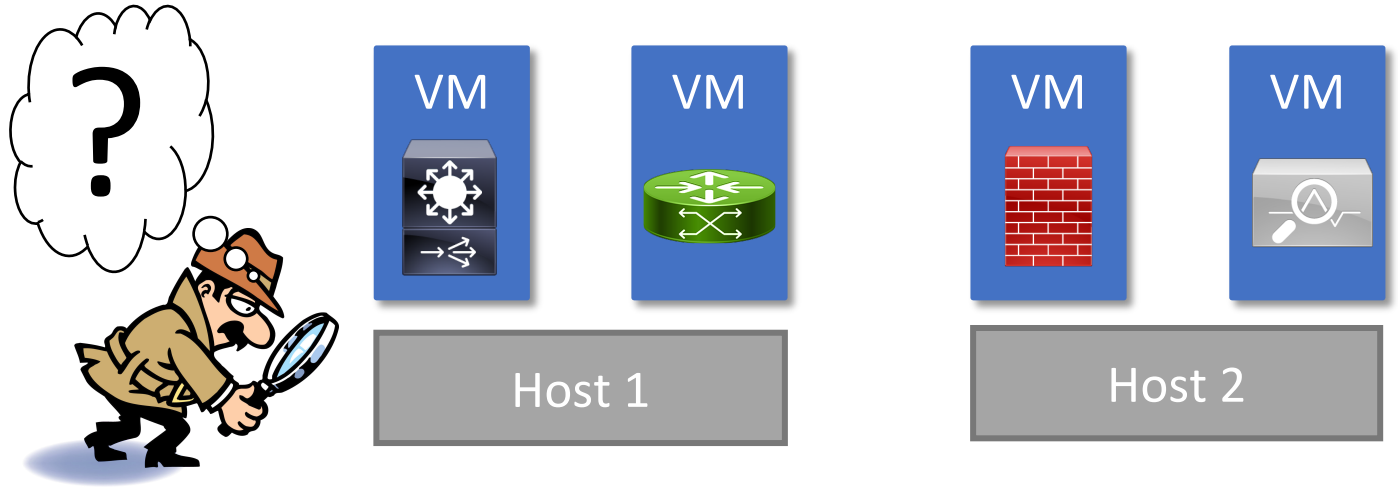


No Existing Tools To Audit Virtualized NFs

- Traditional Network Function (NF) chain



- Modern virtualized NF chain

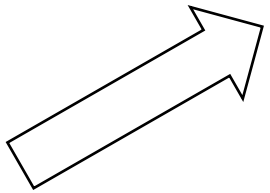


AuditBox Contribution

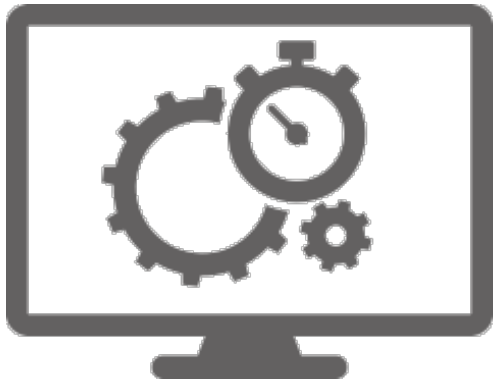
- Offer missing capabilities to audit NFV deployments

Time-of-check-to-time-of-use vulnerabilities

Coarse, manual correctness checks



Provable, continuous assurance of correctness



AuditBox Contribution

- Offer missing capabilities to audit NFV deployments

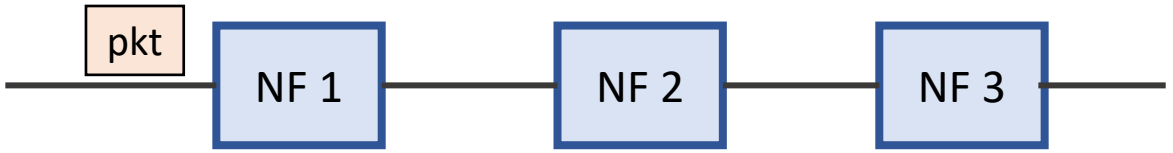
Coarse, manual correctness checks

Provable, continuous assurance of correctness

correctness?

What Does Correctness Mean?

- **Runtime Correctness** = Network implements the intended NF forwarding policies
  - **Packet correctness**
  - **Flow correctness**



- **Offline Auditability** = Must provide a **tamper-proof** ‘audit trail’

Limitations of Prior Work

- Long history of work on verifying Internet paths
  [EPIC USENIX'20, OPT SIGCOMM'14, ICING CoNEXT'11]

- Assumptions:

Immutable Packets

Pre-known Paths

Stateless Processing Nodes

Assumptions Do Not Hold for NFV

- Long history of work on verifying Internet paths
  [EPIC USENIX'20, OPT SIGCOMM'14, ICING CoNEXT'11]

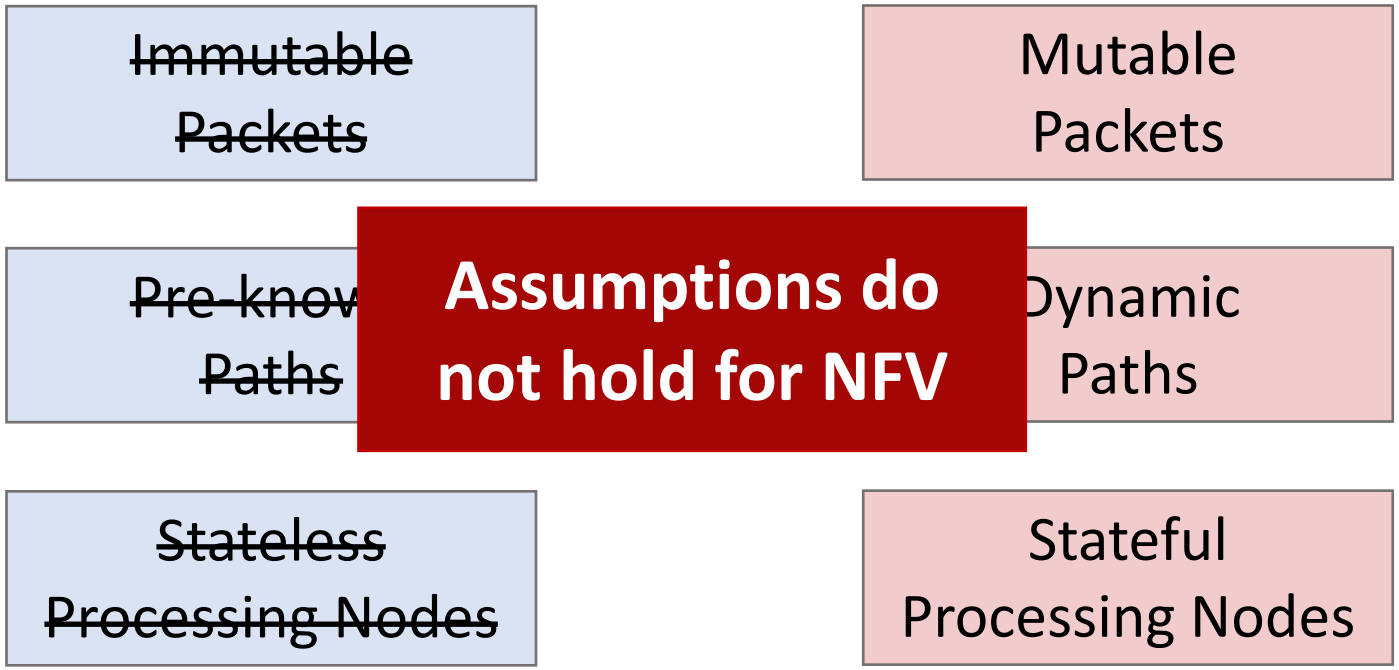
- Assumptions:

Immutable Packets		Mutable Packets
Pre-known Paths	VS	Dynamic Paths
Stateless Processing Nodes		Stateful Processing Nodes

Assumptions Do Not Hold for NFV

- Long history of work on verifying Internet paths
  [EPIC USENIX'20, OPT SIGCOMM'14, ICING CoNEXT'11]

- Assumptions:

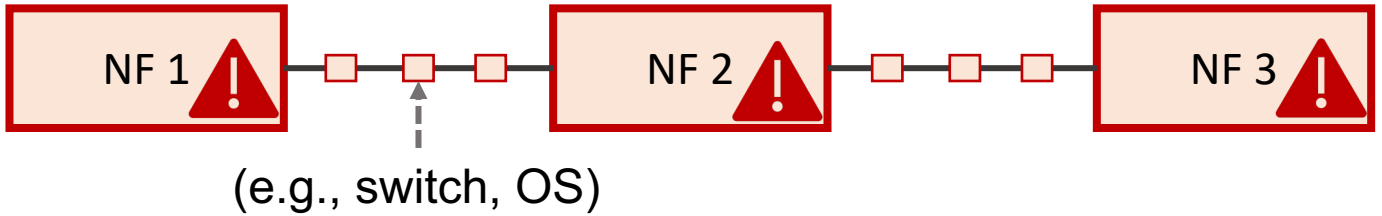


Outline

1. Motivation
2. Our Insight
3. AuditBox Design
4. Evaluation

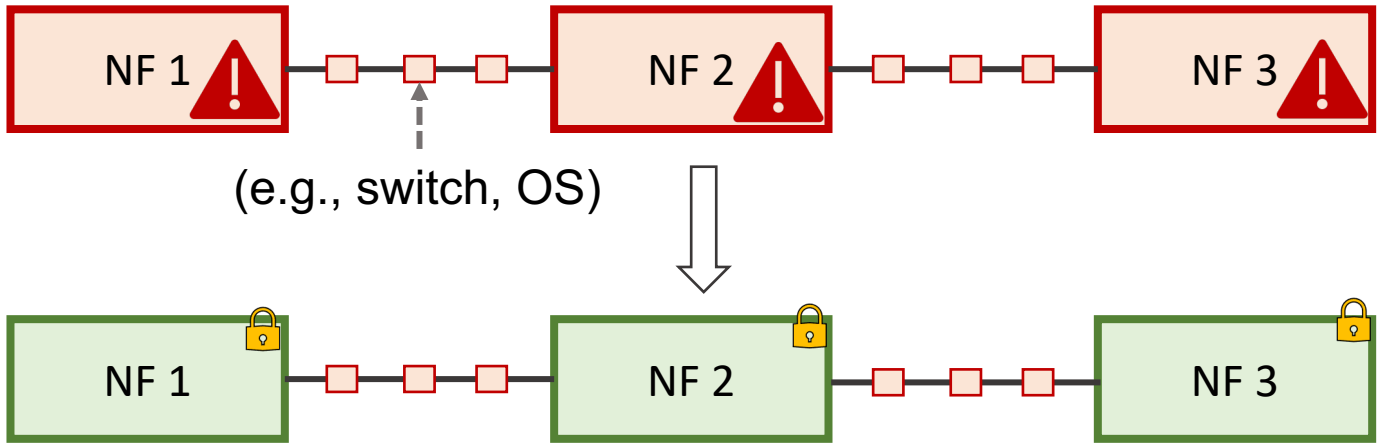
Our Observation

The complexity of auditing comes from NFs' internal processing



Our Insight

The complexity of auditing comes from NFs' internal processing



Run NFs within Trusted Execution Environment (TEEs), and only audit actions between NFs over the untrusted network.

Our Insight

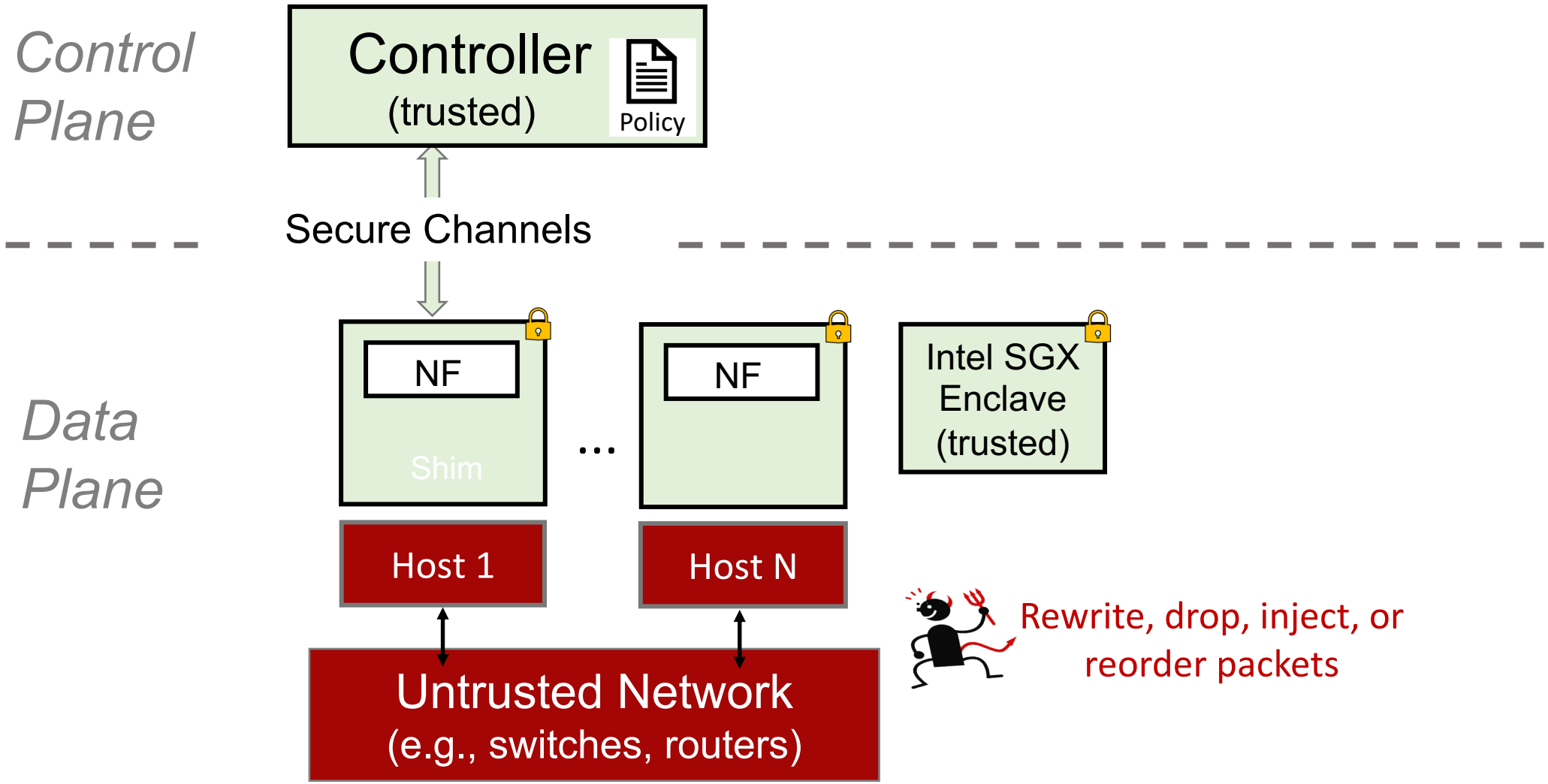
The

Prior Work: SafeBricks [NSDI'18], ShieldBox [SOSR'18], LightBox [CCS'19], S-NFV [SDN-NFV Security'16], etc.

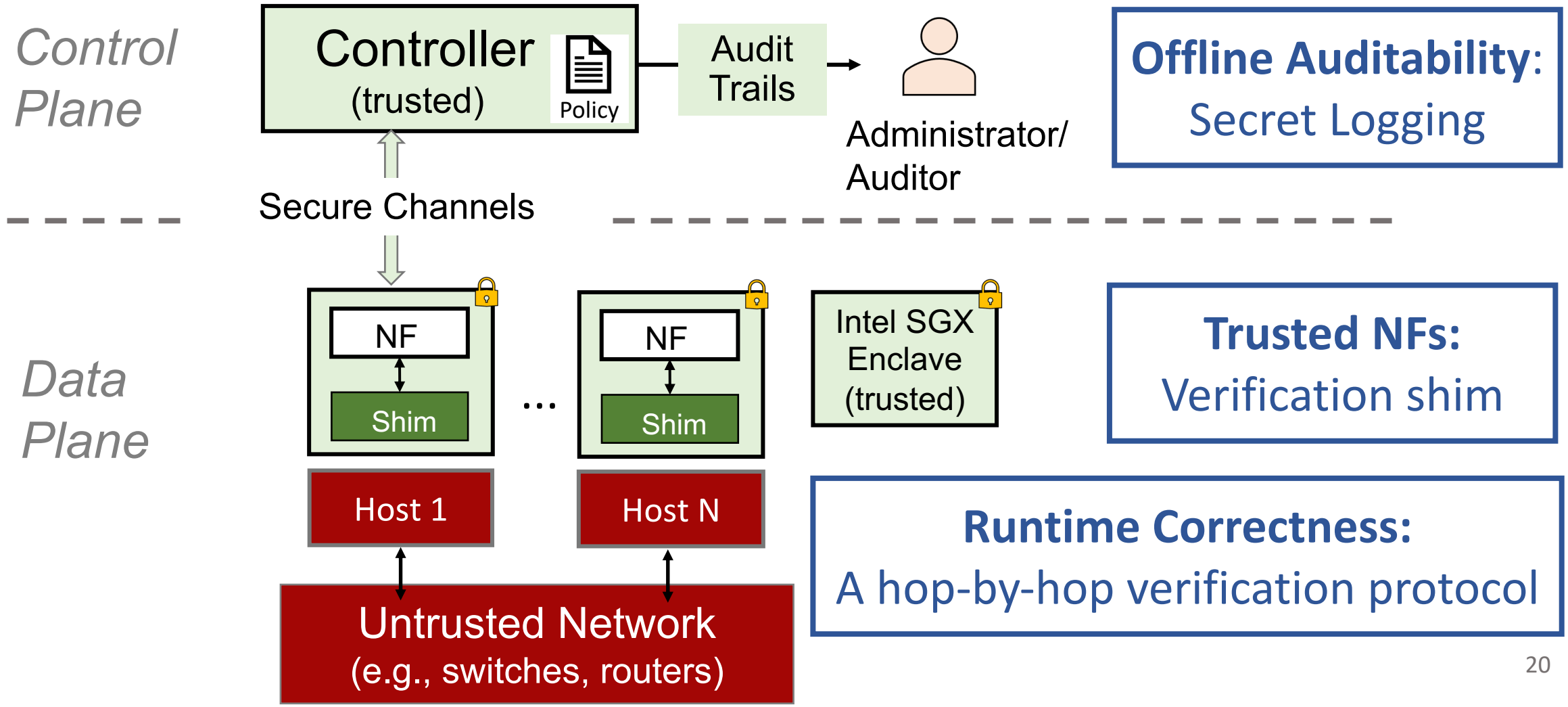
Prior work focuses on securing individual NFs on a single server, not auditing the entire service chain across servers

Run NFs within **Trusted Execution Environment (TEEs)**, and only audit actions between NFs over the untrusted network.

Threat Model



Design Overview

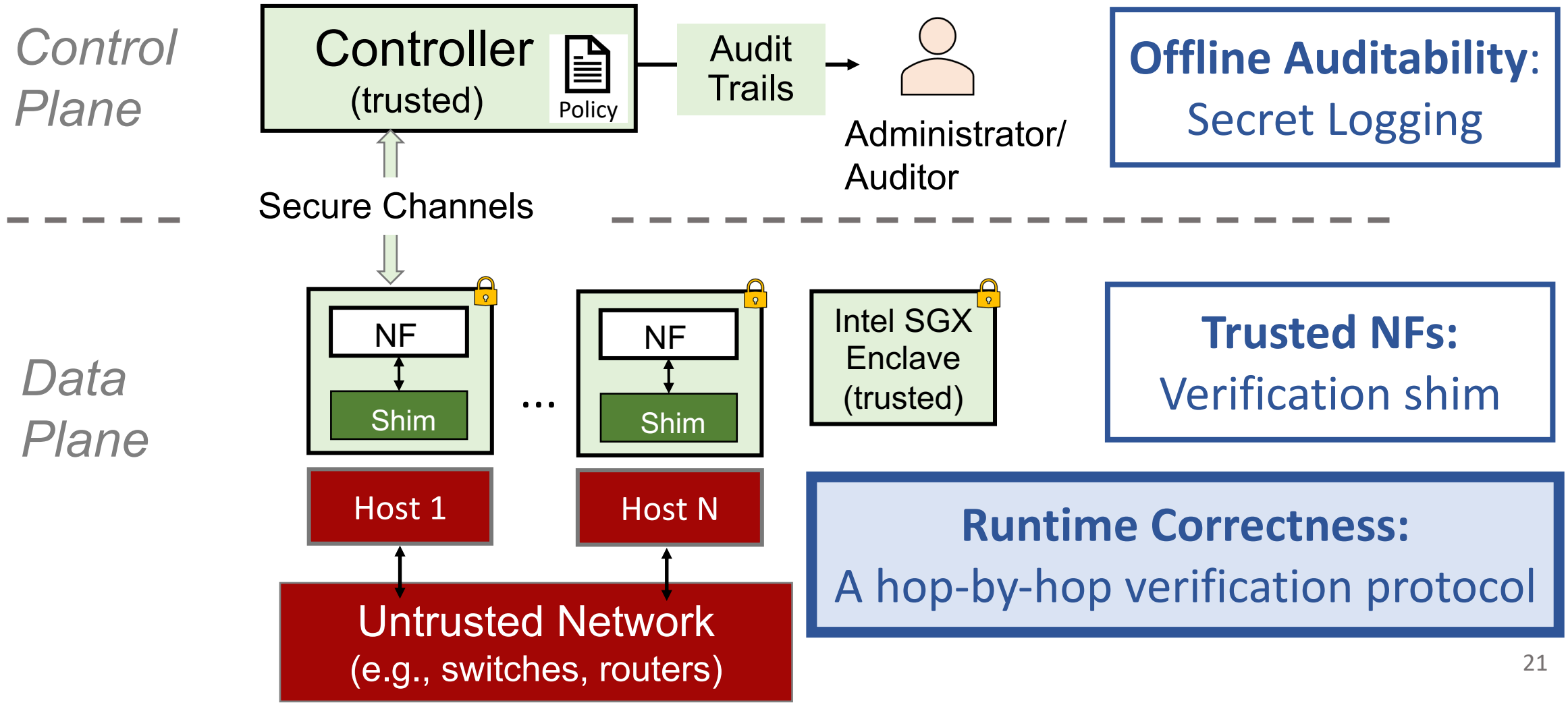


Offline Auditability: Secret Logging

Trusted NFs: Verification shim

Runtime Correctness: A hop-by-hop verification protocol

Design Overview



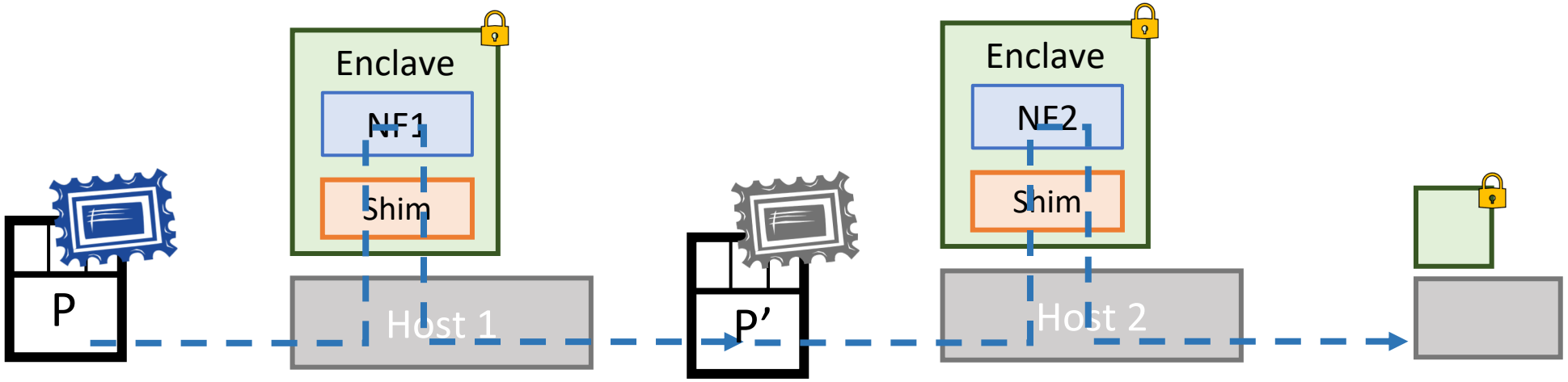
Offline Auditability: Secret Logging

Trusted NFs: Verification shim

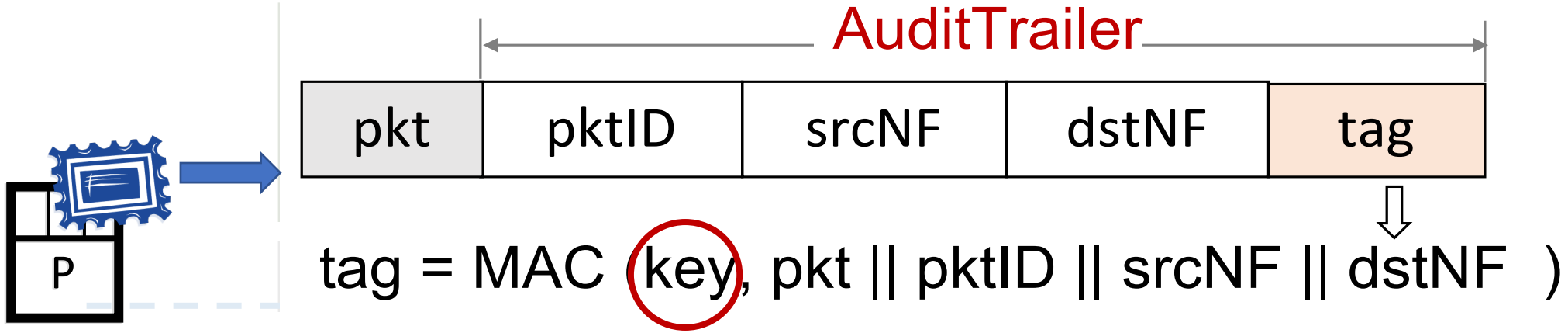
Runtime Correctness: A hop-by-hop verification protocol

NF Hop-by-hop Verification Protocol

- A **shim** in each enclave implements the protocol
- Leverage **transitive trust** to verify packets and enforce policy



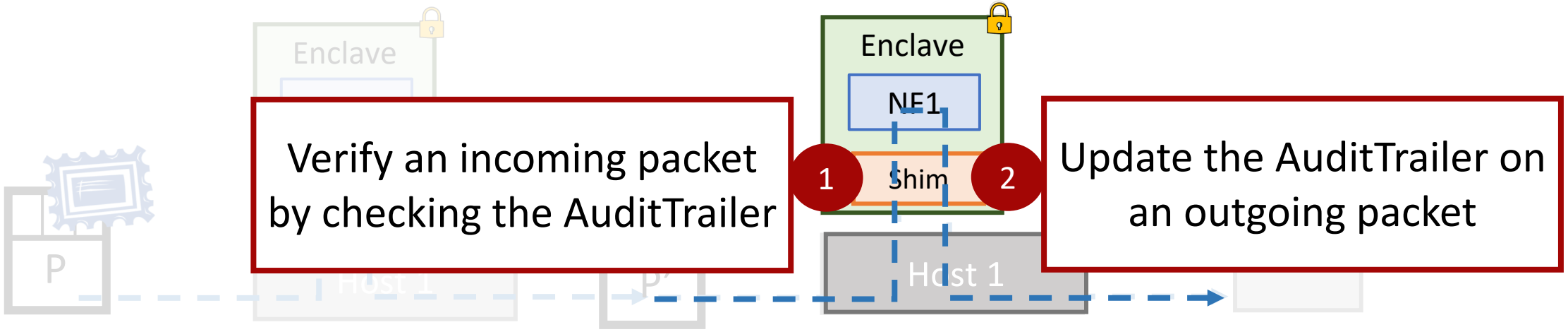
Optimization 1: Simple AuditTrailer



One symmetric key for all NFs in the same policy pipelet

Optimization 2: Updatable GMAC

Reuse the first GMAC when computing the second GMAC to reduce overheads



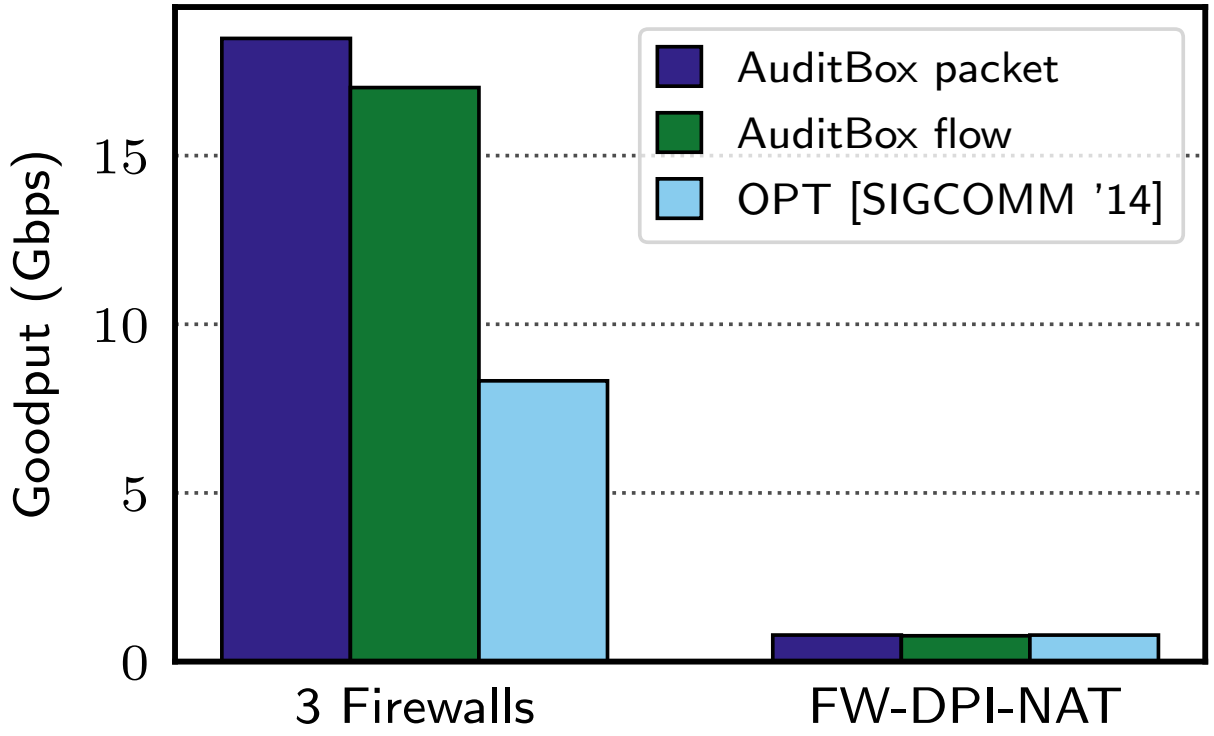
Outline

1. Motivation
2. Our Insight
3. AuditBox Design
4. Evaluation

Evaluation

- **Proofs:** We provide **security proofs** that AuditBox can achieve both runtime correctness and offline auditability
- **Functionality Evaluation:** AuditBox correctly detects a broad class of policy violations
- **Performance Evaluation**: AuditBox enables **auditing** for unmodified NFs with **low overhead**

Evaluation: NF Chain Goodput



Achieves 18 Gbps goodput for a simple NF chain

AuditBox Summary

- **1st NFV auditing system**
- Leverages trusted execution environments to provide
  - **Runtime correctness** guarantees
  - Offline **auditability**
  - And still achieve good performance
- Promotes the adoption of NFV for security sensitive enterprises

nsdi '21

Don't Yank My Chain: Auditable NF Service Chaining

Guyue Liu, Hugo Sadok, Anne Kohlbrenner, Bryan Parno, Vyas Sekar, Justine Sherry*

Carnegie Mellon University **Princeton University*