Don’t Yank My Chain:
Auditable NF Service Chaining

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

Specialized Appliances → NFV → Commodity Server
Academia Efforts To Promote NFV

- CoMb [NSDI’12]
- Aplomb [SIGCOMM’12]
- Split/Merge [NSDI’13]
- SIMPLE [SIGCOMM’13]
- Flowtags [NSDI’14]
- NetVM [NSDI’14]
- ClickOS [NSDI’14]
- E2 [SOSP’15]
- FTMB [SIGCOMM’15]
- OpenBox [SIGCOMM’16]
- BUZZ [NSDI’16]
- NetBricks [OSDI’16]
- NFP [SIGCOMM’17]
- mOS [NSDI’17]
- Stateless [NSDI’17]
- Microboxes [SIGCOMM’18]
- SafeBricks [NSDI’18]
- Metron [NSDI’18]
- Vigor [SOSP’19]
- FlowBlaze [NSDI’19]
- BOLT [NSDI’19]
- FTC [SIGCOMM’20]
- NetSMC [NSDI’20]
- Microscope [SIGCOMM’20]

Years:
- 2012
- 2014
- 2016
- 2018
- 2020
Cloud-based Network Functions

- CoMb [NSDI’12]
- Aplomb [SIGCOMM’12]
- Split/Merge [NSDI’13]
- SIMPLE [SIGCOMM’13]
- Flowtags [NSDI’14]
- NetVM [NSDI’14]
- ClickOS [NSDI’14]
- E2 [SOSP’15]
- FTMB [SIGCOMM’15]
- NetBricks [OSDI’16]
- OpenBox [SIGCOMM’16]
- BUZZ [NSDI’16]
- NFP [SIGCOMM’17]
- mOS [NSDI’17]
- Stateless [NSDI’17]
- SIMPLE [SIGCOMM’13]
- NetVM [NSDI’14]
- ClickOS [NSDI’14]
- E2 [SOSP’15]
- FTMB [SIGCOMM’15]
- NetBricks [OSDI’16]
- OpenBox [SIGCOMM’16]
- BUZZ [NSDI’16]
- NFP [SIGCOMM’17]
- mOS [NSDI’17]
- Stateless [NSDI’17]
- SIMPLE [SIGCOMM’13]
- NetVM [NSDI’14]
- ClickOS [NSDI’14]
- E2 [SOSP’15]
- FTMB [SIGCOMM’15]
- NetBricks [OSDI’16]
- OpenBox [SIGCOMM’16]
- BUZZ [NSDI’16]
- NFP [SIGCOMM’17]
- mOS [NSDI’17]
- Stateless [NSDI’17]
- SIMPLE [SIGCOMM’13]
- NetVM [NSDI’14]
- ClickOS [NSDI’14]
- E2 [SOSP’15]
- FTMB [SIGCOMM’15]
- NetBricks [OSDI’16]
- OpenBox [SIGCOMM’16]
- BUZZ [NSDI’16]
- NFP [SIGCOMM’17]
- mOS [NSDI’17]
- Stateless [NSDI’17]
- SIMPLE [SIGCOMM’13]
- NetVM [NSDI’14]
- ClickOS [NSDI’14]
- E2 [SOSP’15]
- FTMB [SIGCOMM’15]
- NetBricks [OSDI’16]
- OpenBox [SIGCOMM’16]
- BUZZ [NSDI’16]
- NFP [SIGCOMM’17]
- mOS [NSDI’17]
- Stateless [NSDI’17]
- SIMPLE [SIGCOMM’13]
- NetVM [NSDI’14]
- ClickOS [NSDI’14]
- E2 [SOSP’15]
- FTMB [SIGCOMM’15]
- NetBricks [OSDI’16]
- OpenBox [SIGCOMM’16]
- BUZZ [NSDI’16]
- NFP [SIGCOMM’17]
- mOS [NSDI’17]
- Stateless [NSDI’17]
- SIMPLE [SIGCOMM’13]
- NetVM [NSDI’14]
- ClickOS [NSDI’14]
- E2 [SOSP’15]
- FTMB [SIGCOMM’15]
- NetBricks [OSDI’16]
- OpenBox [SIGCOMM’16]
- BUZZ [NSDI’16]
- NFP [SIGCOMM’17]
- mOS [NSDI’17]
- Stateless [NSDI’17]
- SIMPLE [SIGCOMM’13]
- NetVM [NSDI’14]
- ClickOS [NSDI’14]
- E2 [SOSP’15]
- FTMB [SIGCOMM’15]
- NetBricks [OSDI’16]
- OpenBox [SIGCOMM’16]
- BUZZ [NSDI’16]
- NFP [SIGCOMM’17]
- mOS [NSDI’17]
- Stateless [NSDI’17]
- SIMPLE [SIGCOMM’13]
- NetVM [NSDI’14]
- ClickOS [NSDI’14]
- E2 [SOSP’15]
- FTMB [SIGCOMM’15]
- NetBricks [OSDI’16]
- OpenBox [SIGCOMM’16]
- BUZZ [NSDI’16]
- NFP [SIGCOMM’17]
- mOS [NSDI’17]
- Stateless [NSDI’17]
- SIMPLE [SIGCOMM’13]
- NetVM [NSDI’14]
- ClickOS [NSDI’14]
- E2 [SOSP’15]
- FTMB [SIGCOMM’15]
- NetBricks [OSDI’16]
- OpenBox [SIGCOMM’16]
- BUZZ [NSDI’16]
- NFP [SIGCOMM’17]
- mOS [NSDI’17]
- Stateless [NSDI’17]
- SIMPLE [SIGCOMM’13]
- NetVM [NSDI’14]
- ClickOS [NSDI’14]
- E2 [SOSP’15]
- FTMB [SIGCOMM’15]
- NetBricks [OSDI’16]
- OpenBox [SIGCOMM’16]
- BUZZ [NSDI’16]
- NFP [SIGCOMM’17]
- mOS [NSDI’17]
- Stateless [NSDI’17]
- SIMPLE [SIGCOMM’13]
- NetVM [NSDI’14]
- Cloud-based Network Functions

2012  2014  2016  2018  2020
Enterprises Are Reluctant To Adopt NFV
Current NFV Deployments Are Not Auditable

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

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

Assumptions do not hold for NFV
Outline

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

The complexity of auditing comes from NFs’ internal processing (e.g., switch, OS)
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

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

Control Plane

Data Plane

Controller (trusted)

Secure Channels

Controller Policy

Intel SGX Enclave (trusted)

Rewrite, drop, inject, or reorder packets

Untrusted Network (e.g., switches, routers)
Design Overview

Control Plane

Controller (trusted) → Secure Channels → Audit Trails

Audit Trails → Administrator/Auditor

Data Plane

NF Shim → Host 1

Intel SGX Enclave (trusted) → Host N

Untrusted Network (e.g., switches, routers)

Offline Auditability: Secret Logging

Trusted NFs: Verification shim

Runtime Correctness: A hop-by-hop verification protocol
Design Overview

**Control Plane**
- Controller (trusted)
- Secure Channels

**Data Plane**
- NF
- Shim
- Host 1
- Host N
- Untrusted Network (e.g., switches, routers)

**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

![Diagram of AuditTrailer structure]

- **pkt**
- **pktID**
- **srcNF**
- **dstNF**
- **tag**

\[
tag = MAC(\text{key}, \text{pkt} || \text{pktID} || \text{srcNF} || \text{dstNF})\]

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.

1. Verify an incoming packet by checking the AuditTrailer.
2. Update the AuditTrailer on an outgoing packet.
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

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