SVLAN: Secure & Scalable Network Virtualization

Jonghoon Kwon, Taeho Lee, Claude Hähni, Adrian Perrig
ETH Zürich, Network Security Group
Current Inter-domain Network Virtualization: VLAN

Virtual LAN (IEEE 802.1q)

Layer-2 bridging
Supporting apx. 4 K virtual networks with a 12-bit VID value
Current Inter-domain Network Virtualization: VXLAN

Virtual eXtensible LAN

Supporting 16 M virtual networks with a 24-bit VNI value
Interconnecting layer-2 networks over an underlying layer-3 network
Adversarial Model and Desired Properties

Compromise Network Isolation

Disrupt Virtual Network

Security

Scalability

Flexibility
VXLAN: Insufficient Security

Attackers may manipulate VNIs and forward malicious traffic.
VXLAN: Scalability Constraints
VXLAN: Insufficient Flexibility
VXLAN: Insufficient Flexibility
Challenges and Countermeasures

Intra-domain Properties
- Host-level granularity
- Limited number of VNI
- Frequent VNI update

Inter-domain Properties
- Insecure overlay tunneling
- ARP broadcast
- State routing

Intra-domain network slicing
(Destination-driven connectivity)
- Application-level granularity
- Unlimited virtual group
- Centralized management

Verifiable Inter-domain routing
(Packet-carrying forwarding state)
- Crypto-based protection
- Separation of control & data plane
- Stateless routing
Our Vision on Secure and Scalable Network Virtualization

Jonghoon Kwon, Ph.D

Untrusted Network

Mobile Slice

IoT Slice

Mission critical Slice

Edge network

Core network

Mobile Slice

IoT Slice

Mission critical Slice

Untrusted Network
SVLAN (Secure & Scalable Virtual LAN) Overview

Sender
Hypervisor
VM
VM
SVTEP

Authorization Delegate

Receiver
Hypervisor
VM
VM
SVTEP

SVLAN tunnel
Verifier
Express Receiver’s Consent

Sender

Hypervisor

VM VM

SVTEP

Receiving Policy

Receiver

Hypervisor

VM VM

SVTEP
Acquiring Receiver’s Consent

Sender

Hypervisor

VM
VM
SVTEP

Authorization request

Receiver

Hypervisor

VM
VM
SVTEP
Acquiring Receiver’s Consent

Sender

Hypervisor

VM

VM

SVTEP

Authorization Proof

Path Segments + Authorization Proof

Receiver

Hypervisor

VM

VM

SVTEP

Jonghoon Kwon, Ph.D

25.02.2020
SVLAN Packet Forwarding

Sender
Hypervisor

VM
VM

SVTEP

Path Segment + Authorization Proof + Data

Receiver
Hypervisor

VM
VM

SVTEP
Verifying the Validity of Packets

Sender
Hypervisor
VM
VM
SVTEP

Path Segment + Authorization Proof + Data

Receiver
Hypervisor
VM
VM
SVTEP
Proof-of-Concept Implementation in SCIONLab

SCIONLab: Global Future Internet Testbed

Secure and fine-grained inter-domain segment routing
Testbed distributed across the world

https://github.com/scionproto/scion
https://www.scionlab.org
Cracking the Authorization Proof is Impractical

Brute-force attack would require 60000 years on 100 Gbps line to break 64-bit MAC
No Significant Bandwidth Overhead

TABLE II: Comparison of the header sizes, maximum payload, and network performance on a 1Gbps link. The SVLAN header contains three segment labels and one authorization proof.

<table>
<thead>
<tr>
<th></th>
<th>Ethernet</th>
<th>VXLAN</th>
<th>SVLAN</th>
<th>SR-MPLS</th>
<th>SCION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extra header (bytes)</td>
<td>-</td>
<td>50</td>
<td>36</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>Max payload (bytes)</td>
<td>1460</td>
<td>1410</td>
<td>1424</td>
<td>1400</td>
<td></td>
</tr>
<tr>
<td>Max goodput (Mbps)</td>
<td>949</td>
<td>916</td>
<td>926</td>
<td>910</td>
<td></td>
</tr>
</tbody>
</table>

- **SR-MPLS**
  - 36 bytes of additional header
  - 12 bytes of MPLS labels (three labels)
  - 24 bytes of proof

- **SCION**
  - 60 bytes of additional header
  - 24 bytes of forwarding paths (three labels)
  - 32 bytes of extra header
Small Forwarding Performance Overhead

iMIX profiles the proportion of packets of a certain size based on statistical sampling from actual Internet traces.
Latency Inflation Measurements in Cloud

14 Amazon EC2 instances
Select 3 instances as the sender, receiver, and authorization delegate
Measure the latency for TTFP (Time to First Packet)
Latency Inflation with AD on Amazon Cloud

< 75% of latency inflation
Large-scale Simulation
SVLAN, Expected Benefits

### Scalability
- Highly scalable network virtualization
  - Unlimited number of VNI
  - Stateless VTEP

### Security
- Secure isolation from unwanted traffic
  - Only authorized packets get forwarded
  - Adversaries cannot impersonate authorized senders

### Flexibility
- Flexible network management
  - Receiving policy at different granularity
  - Easy update for virtual network

### Performance
- Reducing network overhead
  - No ARP flooding
  - Negligible latency influence
Thank you!

SVLAN: Secure & Scalable Network Virtualization

Jonghoon Kwon, Taeho Lee, Claude Hähni, Adrian Perrig
(jong.kwon@inf.ethz.ch)

ETH Zurich
Network Security Group
Universitätstrasse 6
8092 Zürich

https://netsec.ethz.ch
Backup Slides
### Implementation Example

#### SVLAN header format on SCION

<table>
<thead>
<tr>
<th>0</th>
<th>7</th>
<th>15</th>
<th>23</th>
<th>31</th>
<th>63</th>
</tr>
</thead>
<tbody>
<tr>
<td>NextHdr</td>
<td>HdrLen</td>
<td>ExtType</td>
<td>SecType</td>
<td>Path Segment ($R_{seg}$)</td>
<td>ExpTime</td>
</tr>
<tr>
<td>Authorization Delegate Addr. ($A_{addr}$)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MAC (continued)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **NextHdr**: Next header type
- **HdrLen**: Header length
- **ExtType**: Extension type
- **SecType**: Security type
- **Path Segment ($R_{seg}$)**: Path segment
- **ExpTime**: Expiration time
- **MAC**: Media access control
- **Common header**, **Addresses**, **Forwarding Path (segments)**, **SVLAN Extension**, **Layer 4 and Data**

---

*ETH Zürich*

Jonghoon Kwon, Ph.D. | 25.02.2020 | 27
Practical Consideration

Location of Authorization Delegates

Sender
Hypervisor
VM
VM
SVTEP

Receiver
Hypervisor
VM
VM
SVTEP

Receiver’s AS
Third party entity (Cloud)
Practical Consideration

Location of Verifiers

Receiver
Receiver’s AS
Sender’s AS
Third party entity (Cloud)