Programmable data planes for network security

Roland Meier
nsg.ee.ethz.ch
HotSec 2019
if (packet_is_evil):
    packet.ipv4.evil_bit = 1
else:
    packet.ipv4.evil_bit = 0

<table>
<thead>
<tr>
<th>Version</th>
<th>Header length</th>
<th>Type of service</th>
<th>Total length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identifier</td>
<td>Flags</td>
<td>Fragment offset</td>
<td></td>
</tr>
<tr>
<td>Time to live</td>
<td>Protocol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source address</td>
<td>Destination address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The Security Flag in the IPv4 Header

Evil  DF  MF
if (packet_is_evil):
    packet.ipv4.evil_bit = 1
else:
    packet.ipv4.evil_bit = 0

50 GB

60 milliseconds

hours

60 milliseconds
There has always been hardware to process packets. What has changed?

This hardware is programmable.
It is now possible to write programs for the control plane and the data plane of a network

**Data plane**
- fixed-function hardware
- fast but restricted

**Control plane**
- vendor-specific software
- slow but versatile
It is now possible to write programs for the control plane and the data plane of a network.
Programmable data planes are heavily used in the networking community.
Programmable data planes are heavily used in the networking community.
Programmable data planes are heavily used in the networking community

Google Scholar search results:
- About 408,000 results (0.08 sec)
- Cited by 927

NSDI: 23 papers
SIGCOMM: 20 papers
Programmable data planes are barely used in the security community

NSDI | 23 papers
SIGCOMM | 20
NDSS | 3
S&P | 1
USENIX Sec | 1
CCS | 0
Programmable data planes are barely used in the security community.

NetHide: Secure and Practical Network Topology Obfuscation

Roland Meier(1), Petar Tsankov(1), Vincent Lenders(2), Laurent Vanbever(1), Martin Vechev(1)
nethide.ethz.ch

USENIX Security 2018

Cited by 927

USENIX Security

23 papers

NSDI 20

SIGCOMM 20

NDSS 3

S&P 1

CCS 0
Programmable data planes are barely used in the security community.

<table>
<thead>
<tr>
<th>Conference</th>
<th>Papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSDI</td>
<td>23</td>
</tr>
<tr>
<td>SIGCOMM</td>
<td>20</td>
</tr>
<tr>
<td>NDSS</td>
<td>3</td>
</tr>
<tr>
<td>USENIX Sec</td>
<td>1</td>
</tr>
<tr>
<td>CCS</td>
<td>0</td>
</tr>
</tbody>
</table>
Programmable data planes are barely used in the security community. 

<table>
<thead>
<tr>
<th>Conference</th>
<th>Papers</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSDI</td>
<td>23</td>
</tr>
<tr>
<td>SIGCOMM</td>
<td>20</td>
</tr>
<tr>
<td>NDSS</td>
<td>3</td>
</tr>
<tr>
<td>S&amp;P</td>
<td>1</td>
</tr>
<tr>
<td>USENIX Sec</td>
<td>1</td>
</tr>
<tr>
<td>CCS</td>
<td>0</td>
</tr>
</tbody>
</table>
Programmable data planes are barely used in the security community

Why?
Programmable data planes allow processing **all packets at line rate**

- no sampling
- no impact on performance
P4 is a domain-specific programming language
Possibilities and limitations of programmable data planes

- simple operations on all packets
- extract information from packets
- custom headers and protocols

- complex operations
- maintain (large) state
- modify the payload
Let’s discuss these 2 topics (and more)

- Which network security applications can benefit from programmable data planes and how?

- Which dangers does this new technology impose? e.g. related to attacks against data-plane programs