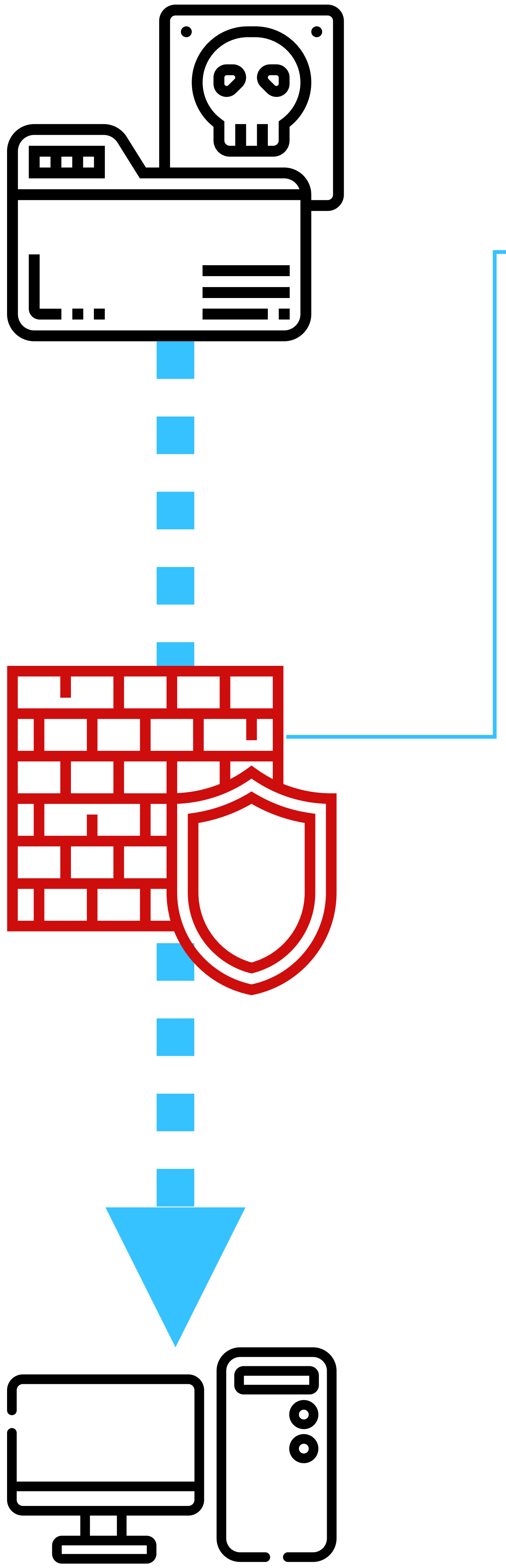
Programmable data planes for network security

Roland Meier

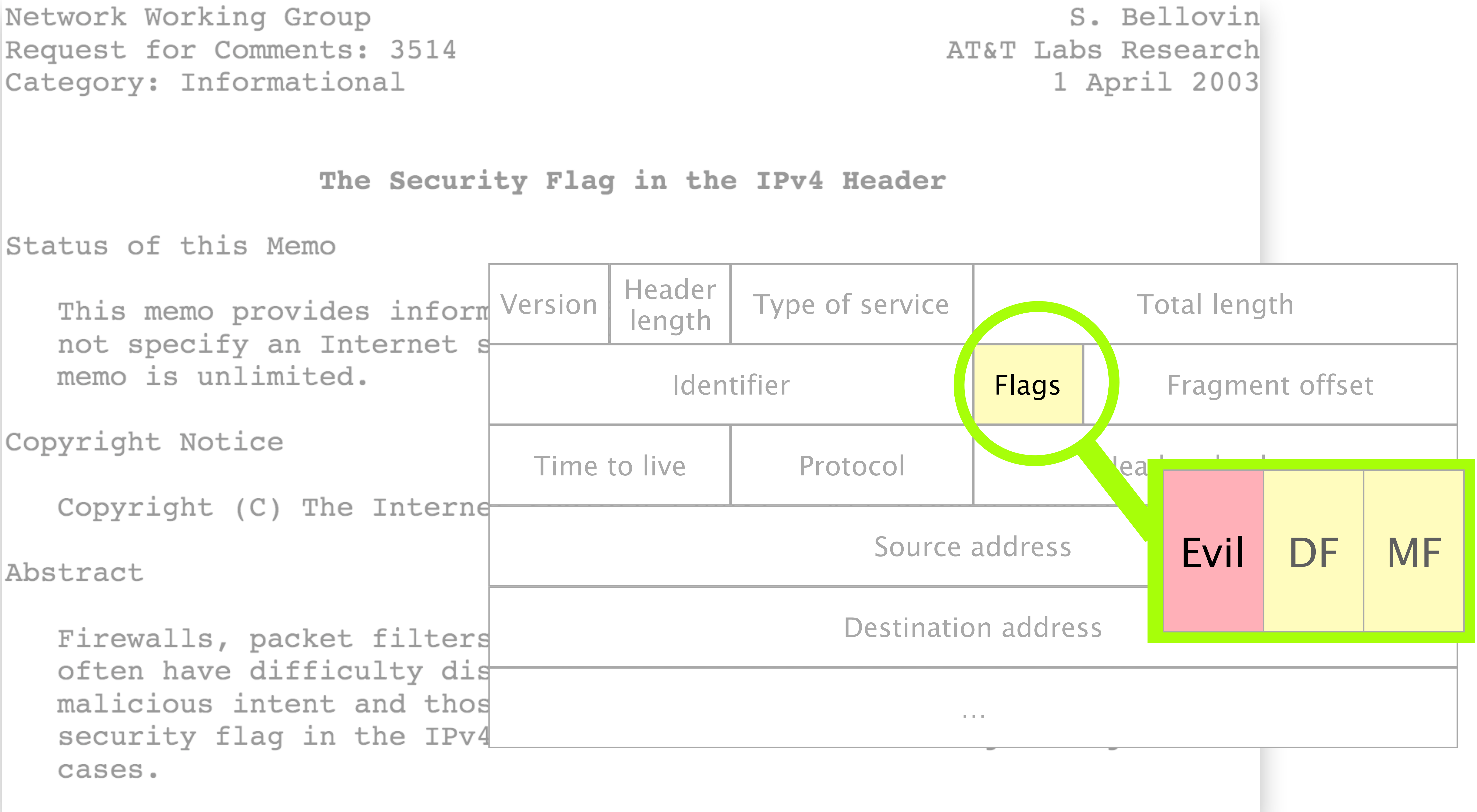
nsg.ee.ethz.ch

HotSec 2019

ETH zürich



```
if (packet_is_evil):
    packet.ipv4.evil_bit = 1
else:
    packet.ipv4.evil_bit = 0
```



```
Network Working Group                                      S. Bellovin
Request for Comments: 3514                          AT&T Labs Research
Category: Informational                                   1 April 2003


                The Security Flag in the IPv4 Header

Status of this Memo

   This memo provides inform
   not specify an Internet s
   memo is unlimited.

Copyright Notice

   Copyright (C) The Interne

Abstract

   Firewalls, packet filters
   often have difficulty dis
   malicious intent and thos
   security flag in the IPv4
   cases.
```

Version | Header length | Type of service | Total length

Identifier | Flags | Fragment offset

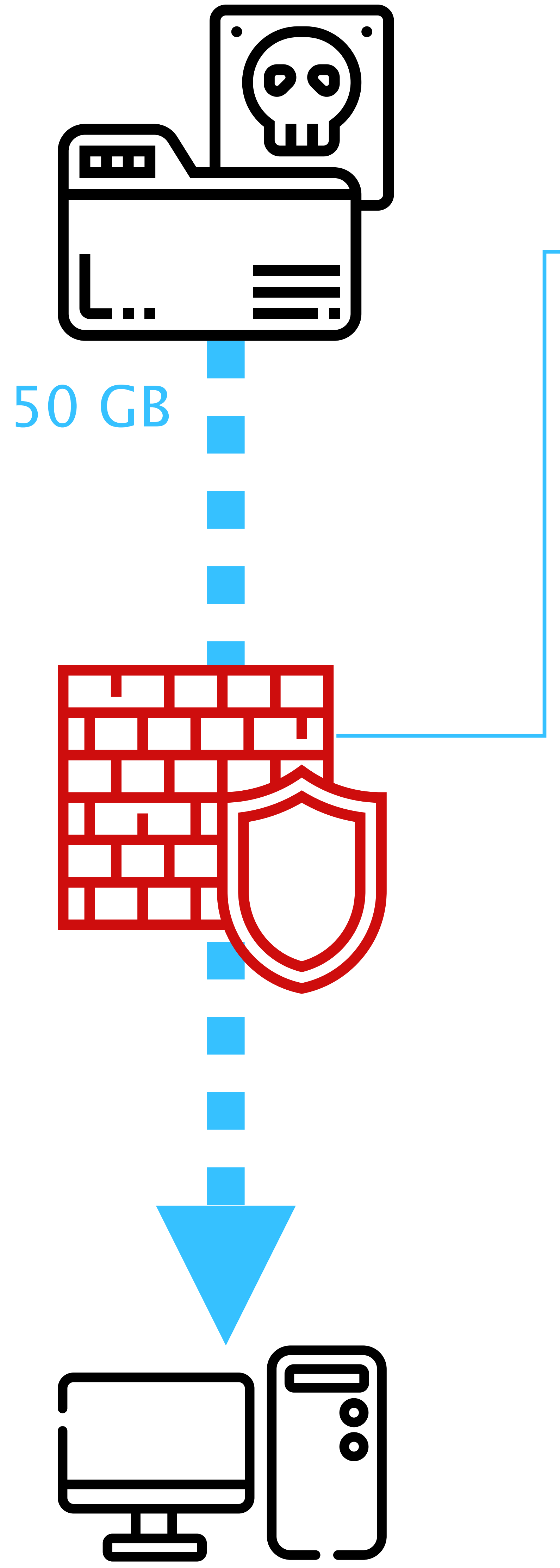
Time to live | Protocol | Hea

Source address

Destination address

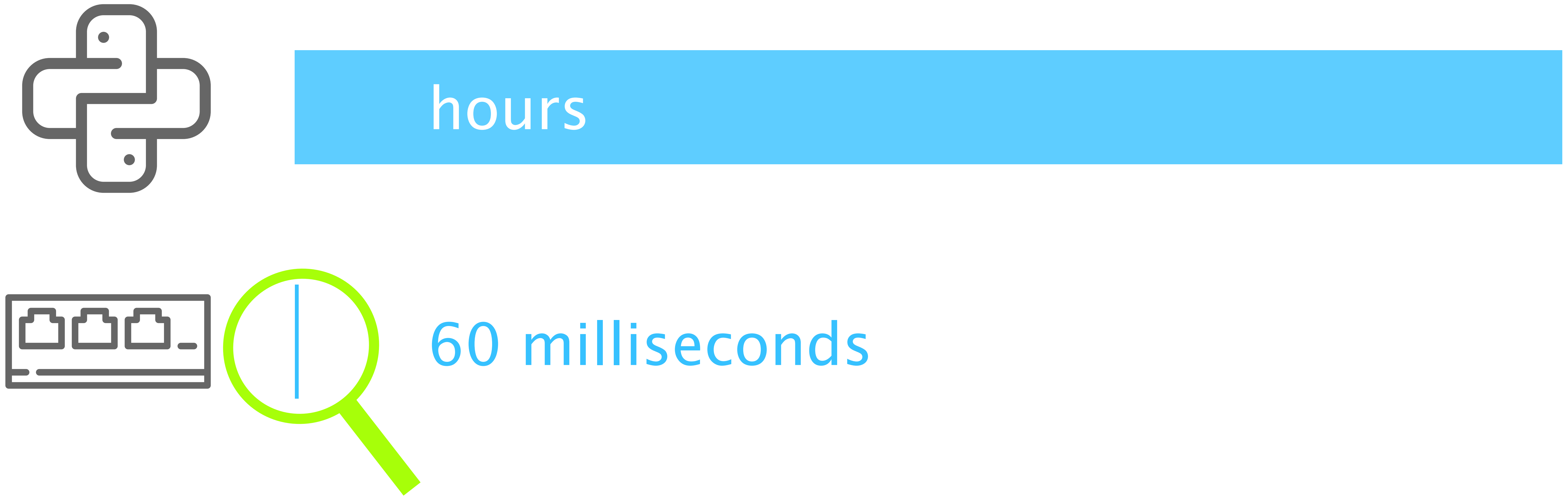
...

Evil | DF | MF



50 GB

```
if (packet_is_evil):
    packet.ipv4.evil_bit = 1
else:
    packet.ipv4.evil_bit = 0
```



hours

60 milliseconds

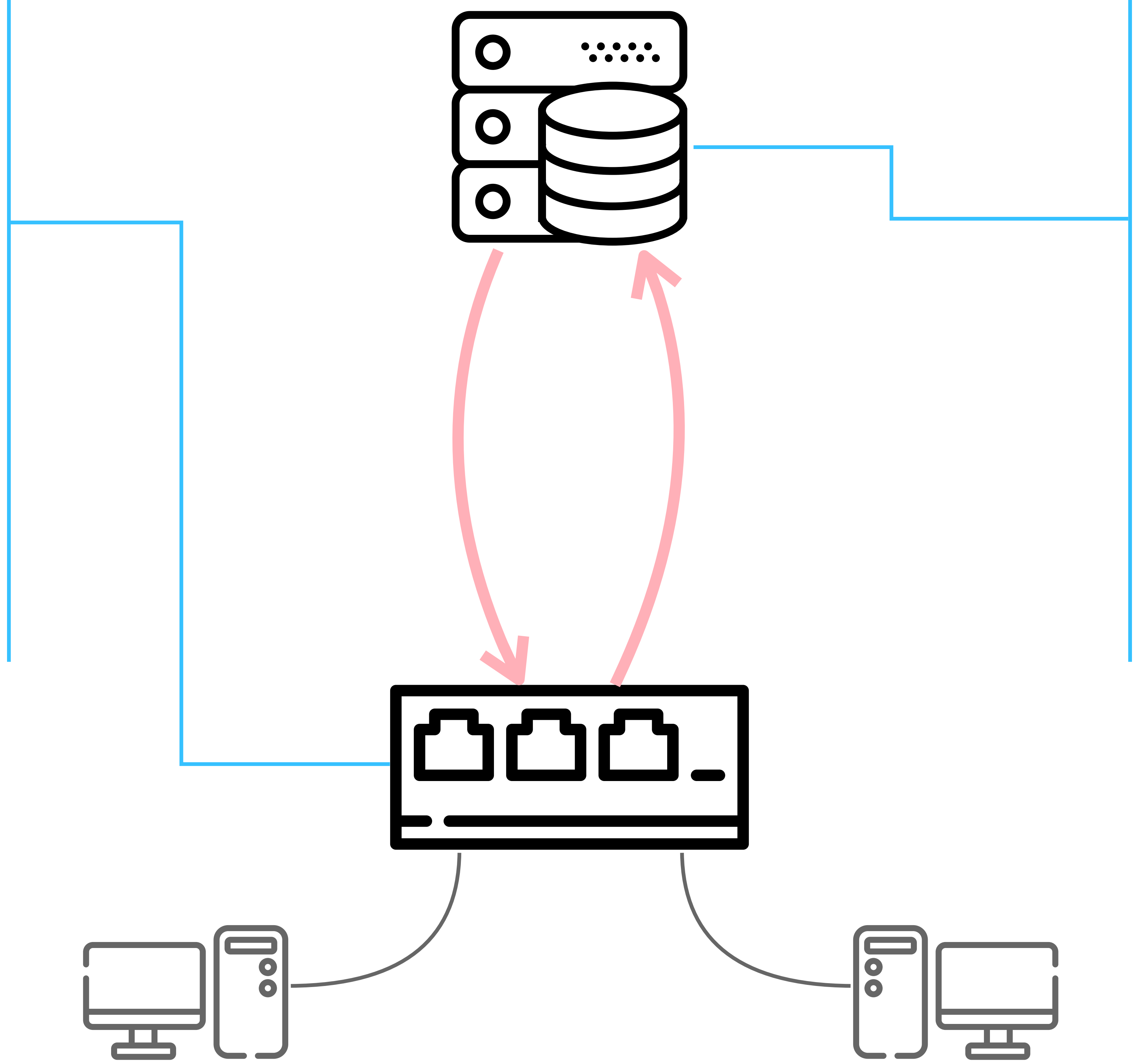
There has always been hardware to process packets.
What has changed?

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

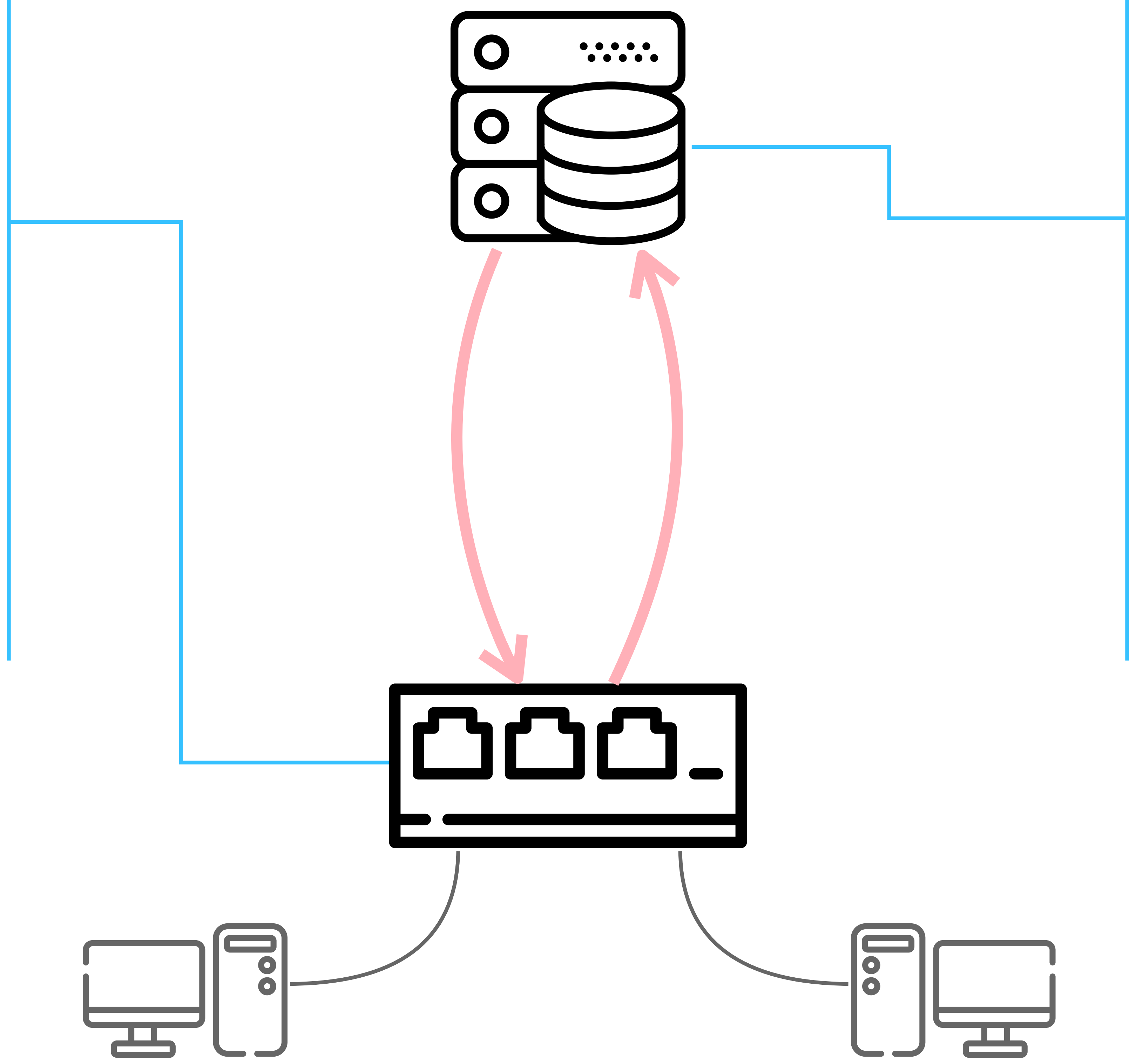
- vendor-specific software
- slow but versatile

It is now possible to write programs for the control plane *and* the data plane of a network

Data plane

programmable

- ~~fixed-function~~ hardware
- fast but restricted

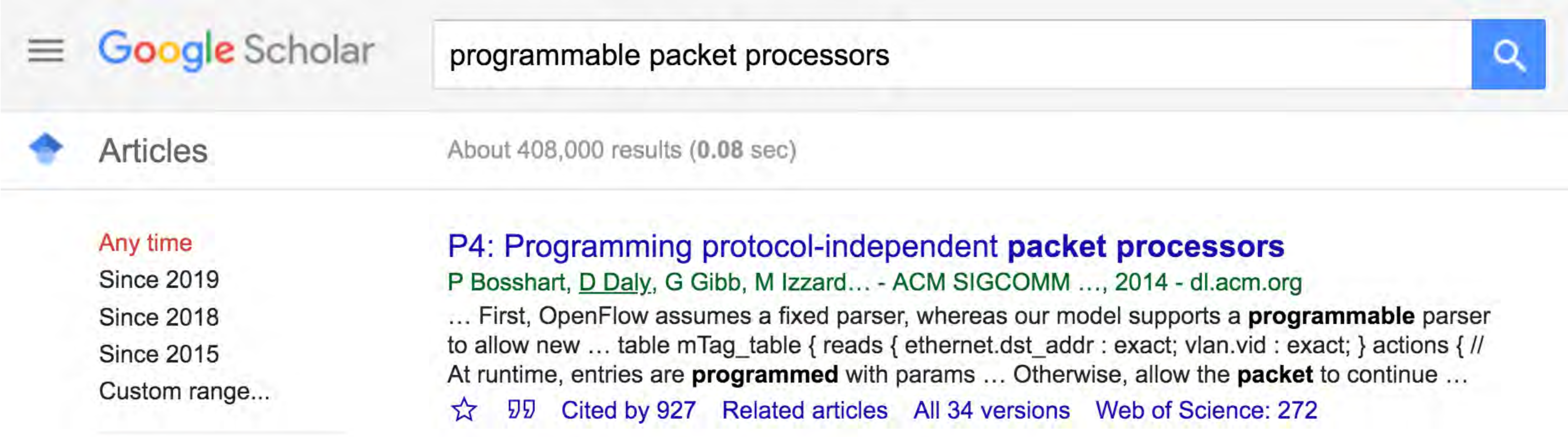


Control plane

custom

- ~~vendor-specific~~ software
- slow but versatile

Programmable data planes are heavily used in the networking community



programmable packet processors

About 408,000 results (**0.08** sec)

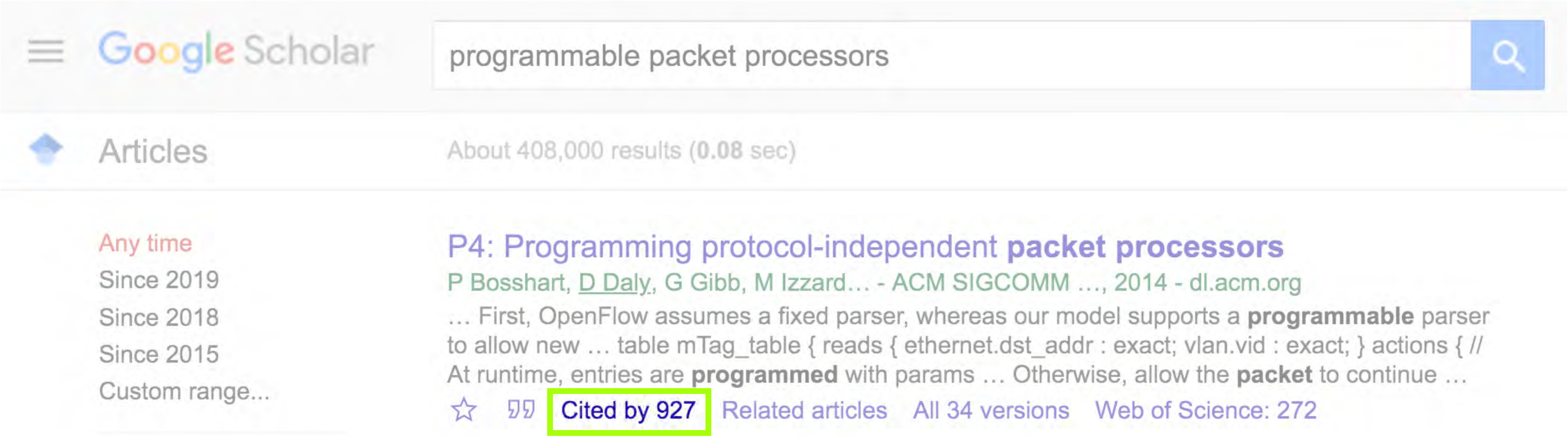
P4: Programming protocol-independent **packet processors**

P Bosshart, D Daly, G Gibb, M Izzard… - ACM SIGCOMM …, 2014 - dl.acm.org

… First, OpenFlow assumes a fixed parser, whereas our model supports a **programmable** parser to allow new … table mTag_table { reads { ethernet.dst_addr : exact; vlan.vid : exact; } actions { // At runtime, entries are **programmed** with params … Otherwise, allow the **packet** to continue …

☆ 99 Cited by 927 Related articles All 34 versions Web of Science: 272

Programmable data planes are heavily used in the networking community



programmable packet processors

About 408,000 results (**0.08** sec)

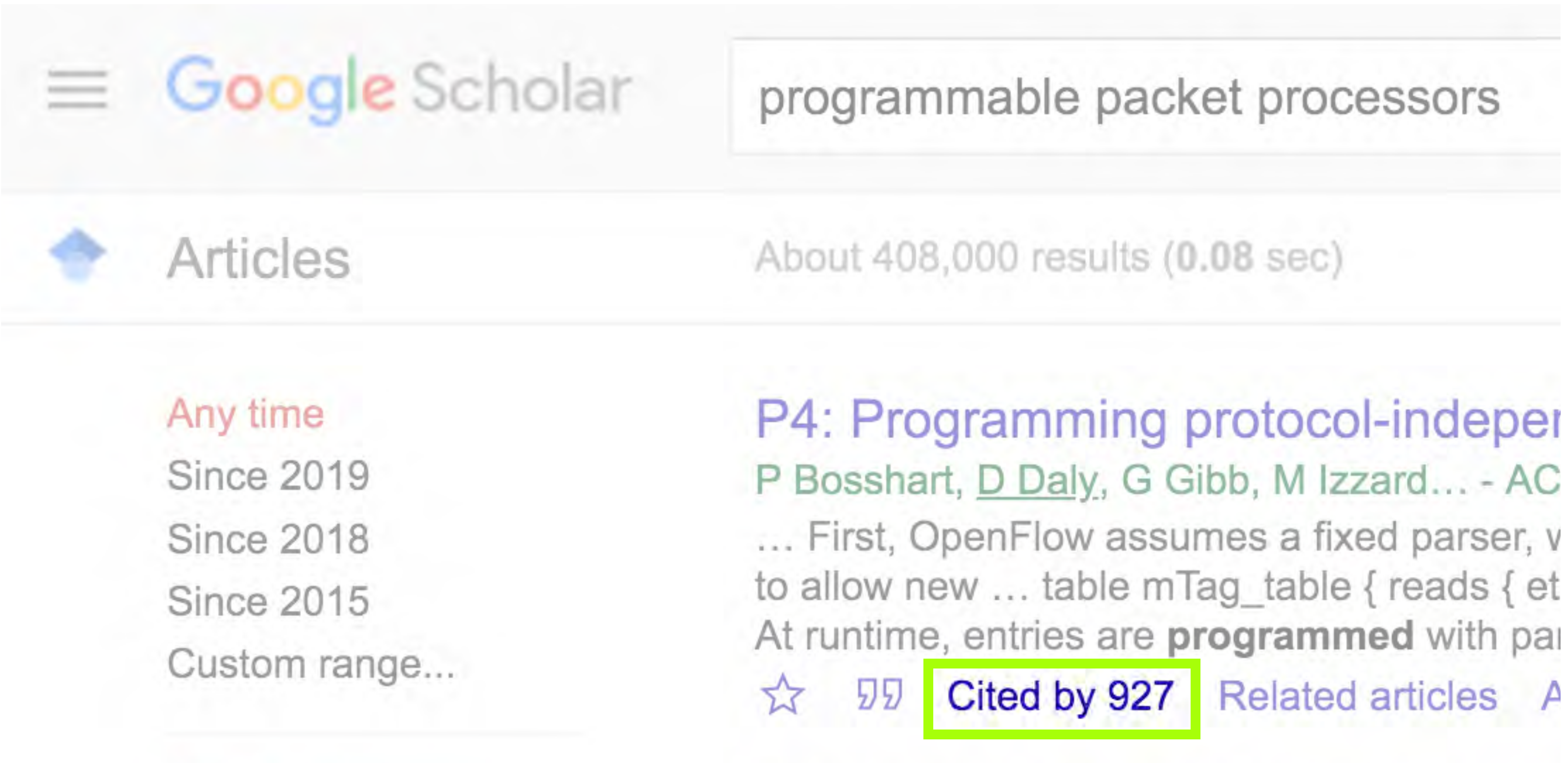
P4: Programming protocol-independent **packet processors**

P Bosshart, D Daly, G Gibb, M Izzard… - ACM SIGCOMM …, 2014 - dl.acm.org

… First, OpenFlow assumes a fixed parser, whereas our model supports a **programmable** parser to allow new … table mTag_table { reads { ethernet.dst_addr : exact; vlan.vid : exact; } actions { // At runtime, entries are **programmed** with params … Otherwise, allow the **packet** to continue …

☆ 99 Cited by 927 Related articles All 34 versions Web of Science: 272

Programmable data planes are heavily used in the networking community

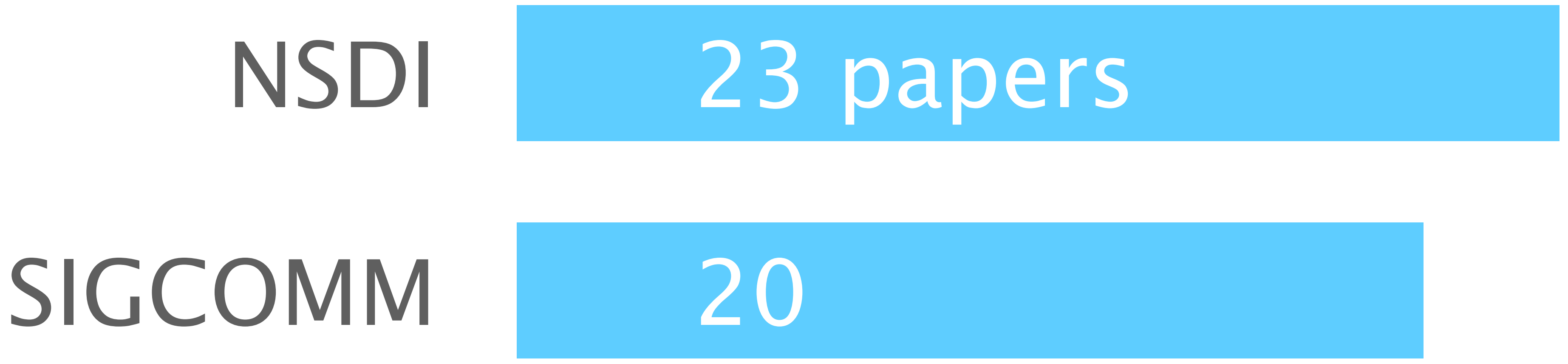


Google Scholar | programmable packet processors

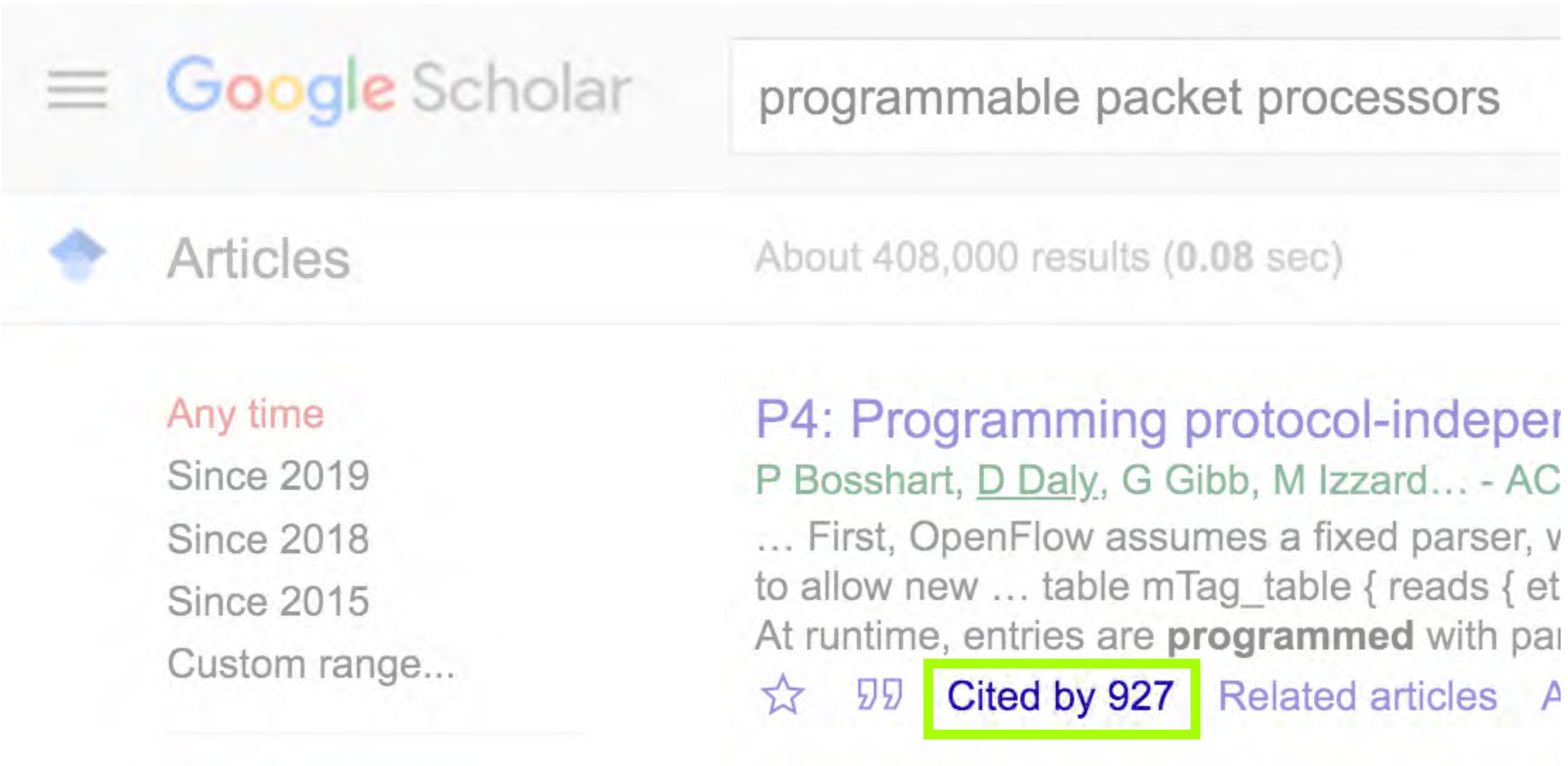
Articles | About 408,000 results (**0.08** sec)

Any time
Since 2019
Since 2018
Since 2015
Custom range...

P4: Programming protocol-indepe
P Bosshart, D Daly, G Gibb, M Izzard… - AC
… First, OpenFlow assumes a fixed parser, v
to allow new … table mTag_table { reads { et
At runtime, entries are **programmed** with pa
☆ 99 Cited by 927 Related articles A



Programmable data planes are barely used in the security community



Google Scholar

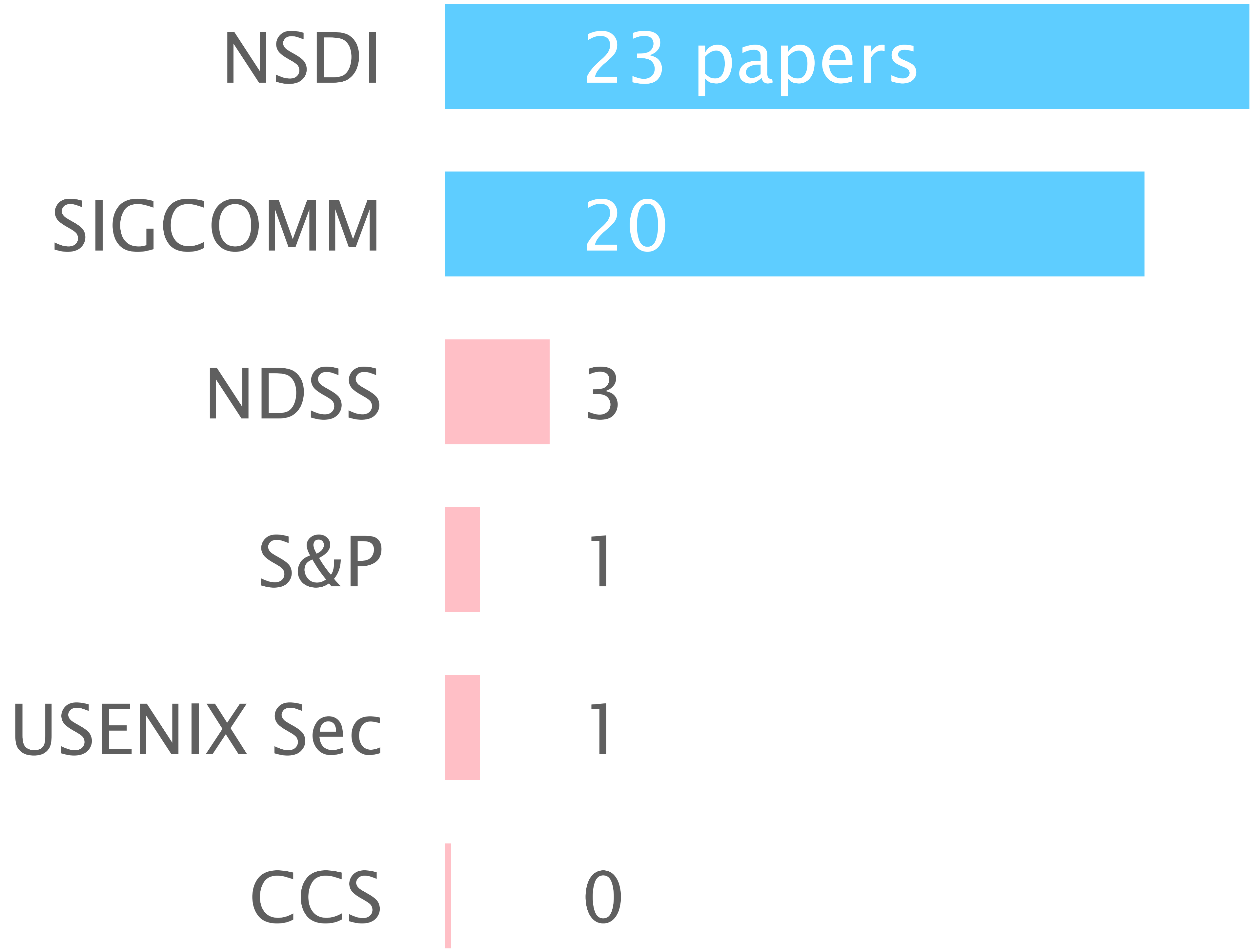
programmable packet processors

Articles

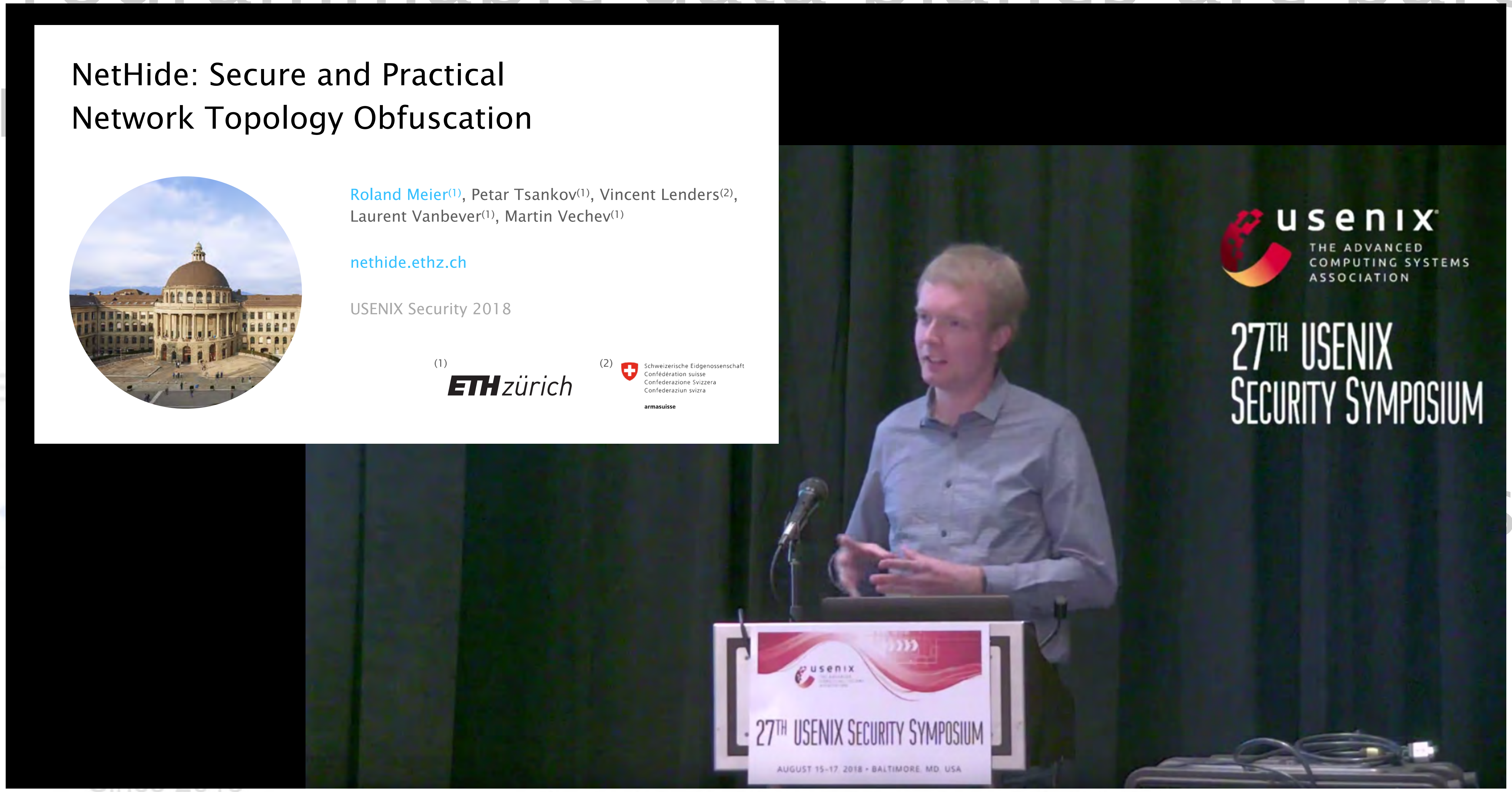
About 408,000 results (**0.08** sec)

Any time
Since 2019
Since 2018
Since 2015
Custom range...

P4: Programming protocol-indeper
P Bosshart, D Daly, G Gibb, M Izzard… - AC
… First, OpenFlow assumes a fixed parser, v
to allow new … table mTag_table { reads { et
At runtime, entries are **programmed** with pa



Programmable data planes are barely used
i



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

(1) ETH zürich

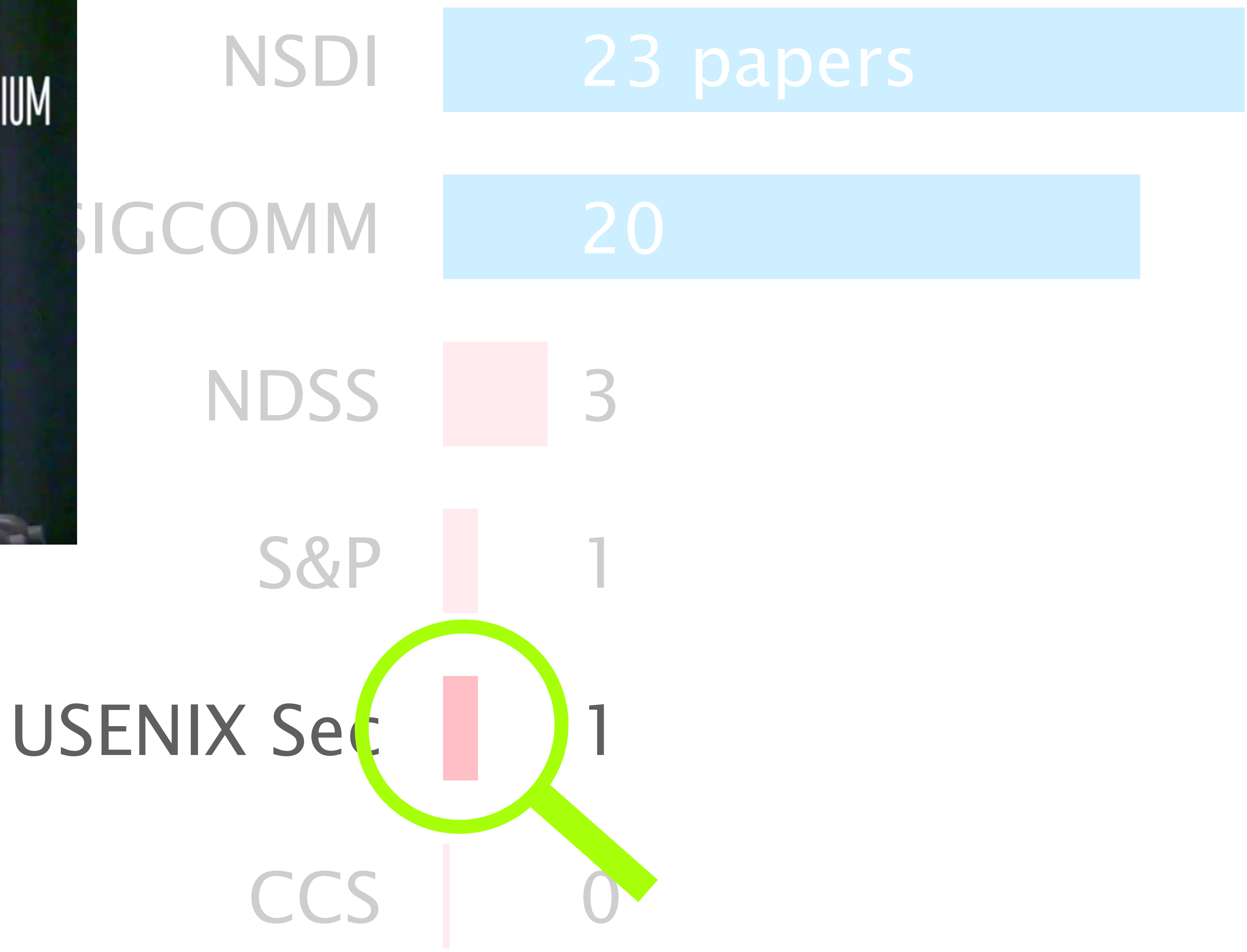
(2) Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
armasuisse

usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION
27TH USENIX SECURITY SYMPOSIUM
usenix
27TH USENIX SECURITY SYMPOSIUM
AUGUST 15-17, 2018 • BALTIMORE, MD, USA

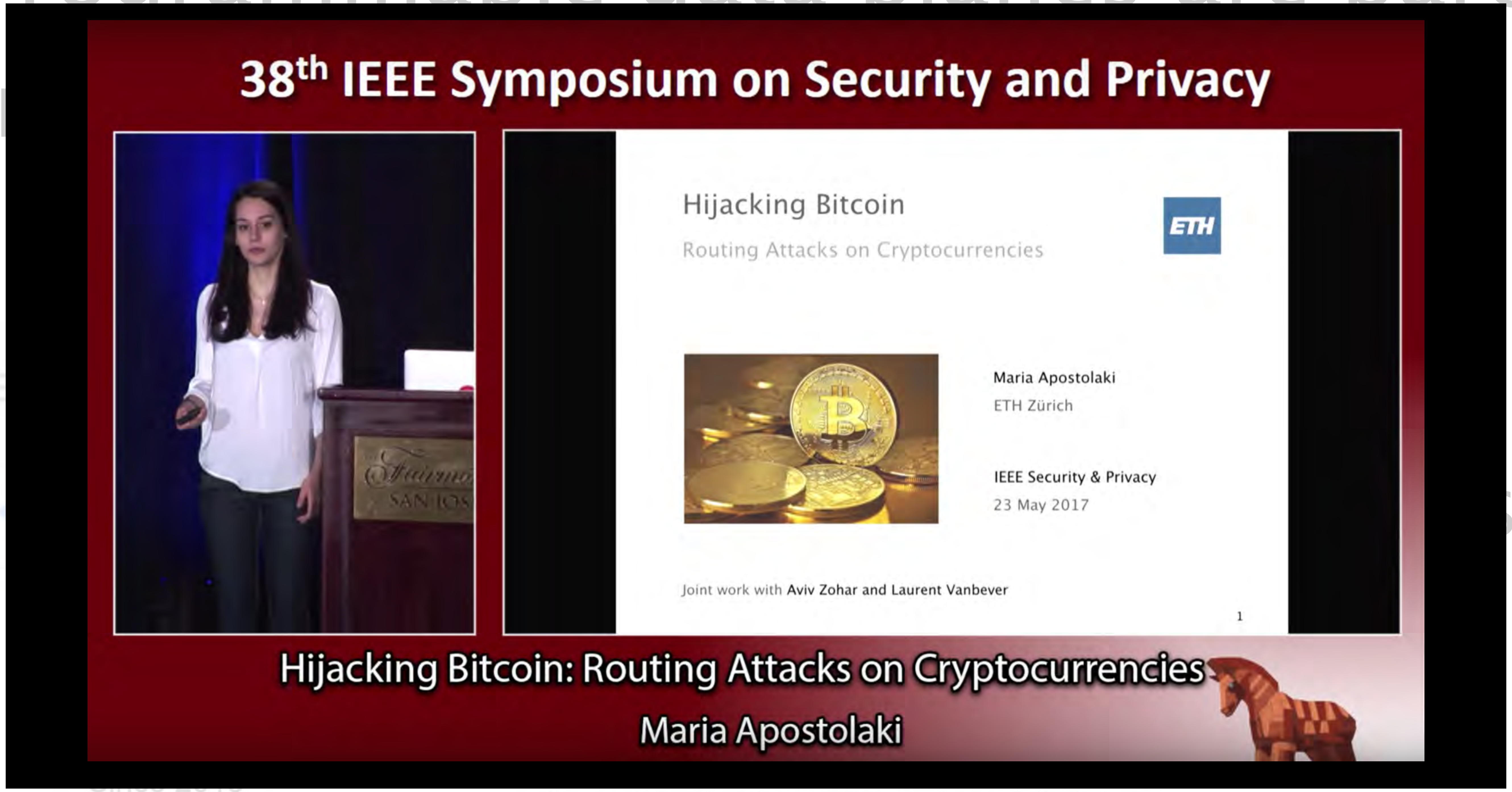
Custom range...

At runtime, entries are **programmed** with pa

☆ 99 Cited by 927 Related articles



Programmable data planes are barely used i



38th IEEE Symposium on Security and Privacy

Hijacking Bitcoin

Routing Attacks on Cryptocurrencies

Maria Apostolaki
ETH Zürich

IEEE Security & Privacy
23 May 2017

Joint work with Aviv Zohar and Laurent Vanbever

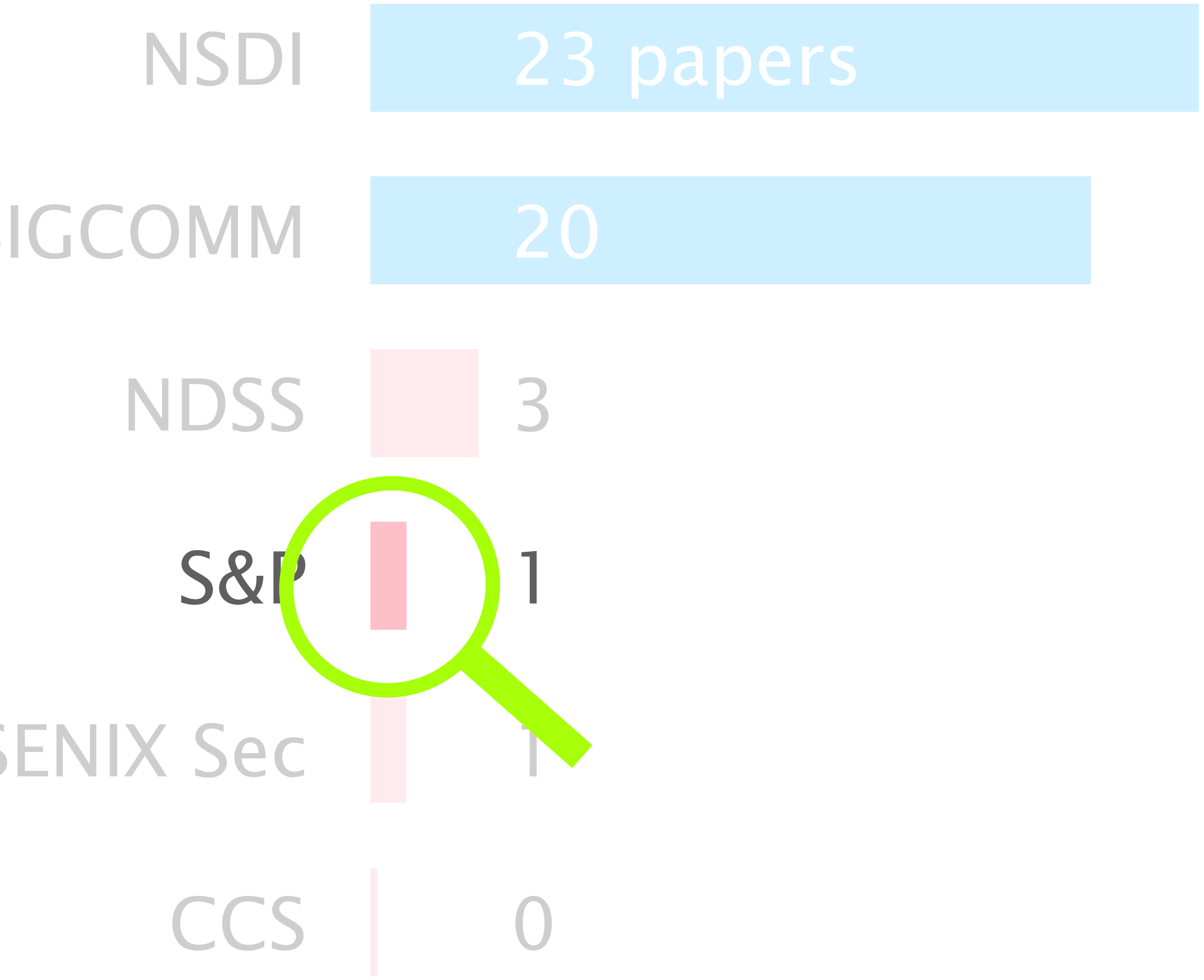
Hijacking Bitcoin: Routing Attacks on Cryptocurrencies

Maria Apostolaki

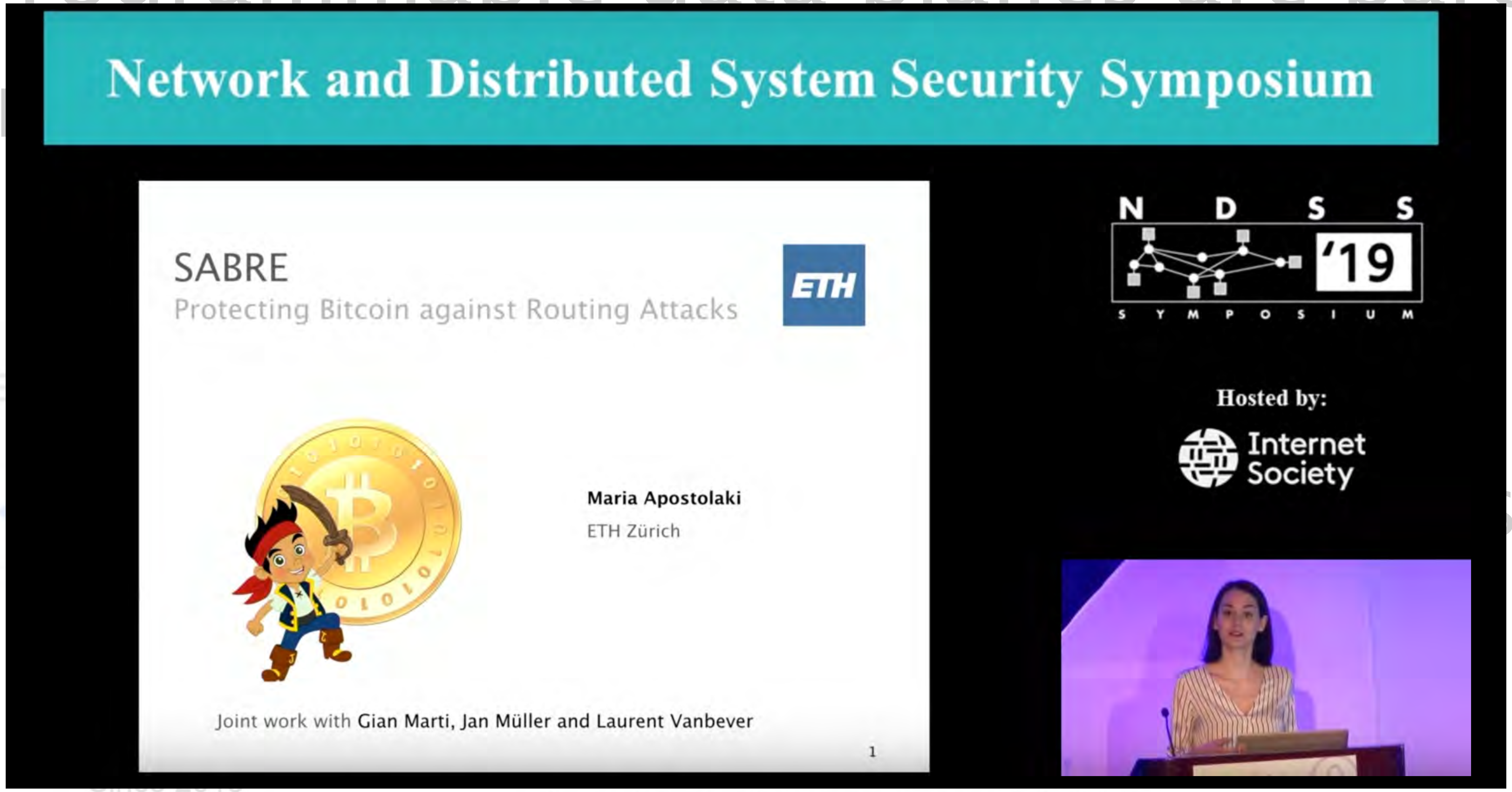
Custom range...

At runtime, entries are **programmed** with pa

☆ 99 Cited by 927 Related articles



Programmable data planes are barely used i



Network and Distributed System Security Symposium

SABRE

Protecting Bitcoin against Routing Attacks

Maria Apostolaki

ETH Zürich

Joint work with Gian Marti, Jan Müller and Laurent Vanbever

1

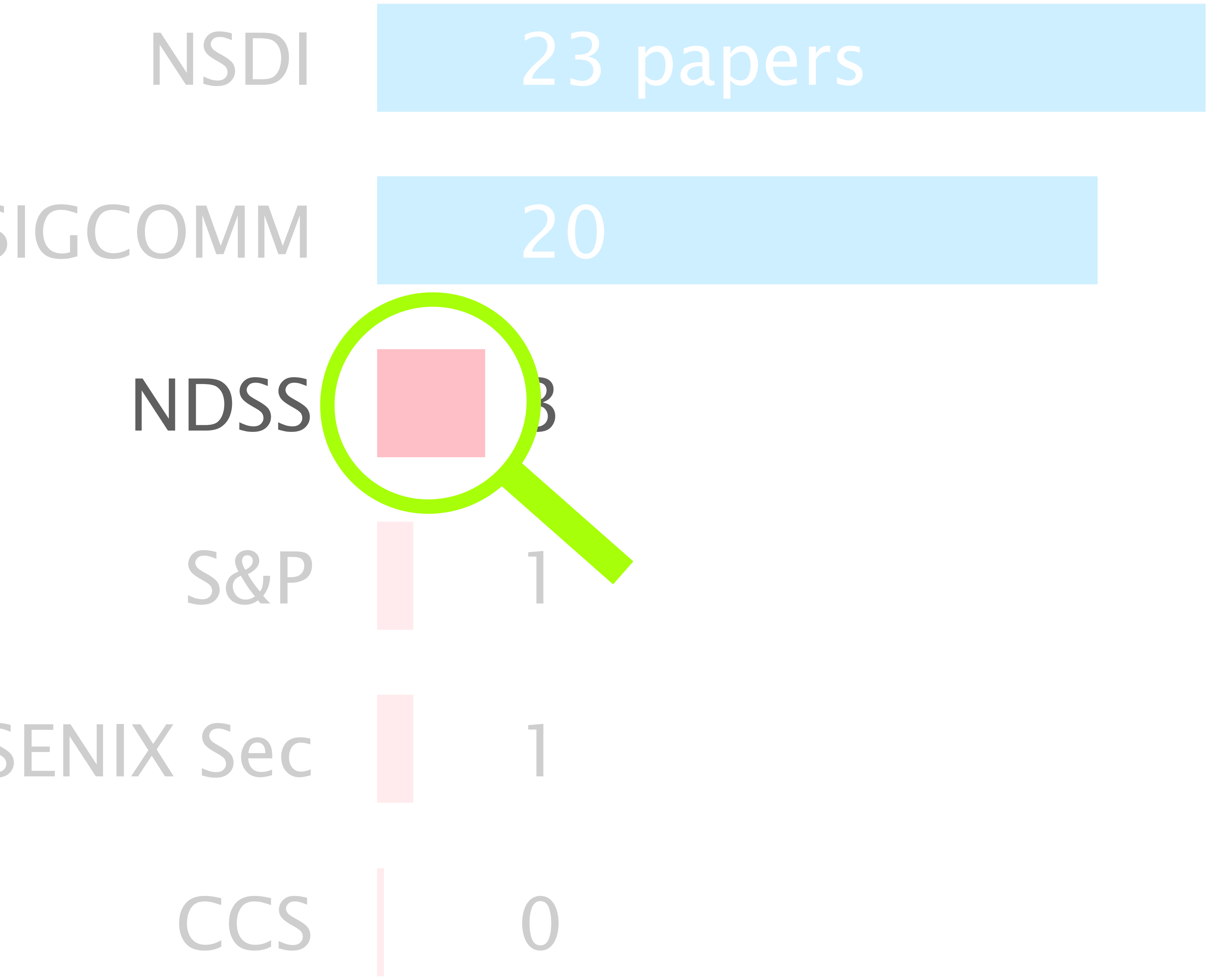
NDSS '19 SYMPOSIUM

Hosted by: Internet Society

Custom range...

At runtime, entries are programmed with pa

Cited by 927 Related articles



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

C

− loops

− recursive calls

− pointers

− malloc

− free

+ parsers

+ tables

+ architectures

P4

[Andy Fingerhut: P4 in 500 words]

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

Roland Meier
meierrol@ethz.ch
nsg.ee.ethz.ch

ETH zürich