Krejzy věci s SSH

Adam Kalisz

adam.kalisz@notnullmakers.com

5 years since

IF2019: Advanced misuse of (mostly) OpenSSH
https://www.youtube.com/watch?v=UpXqW2DFfMI

LD2019: SSH nejen pro vzdálenou správu Linuxu
(Petr Krčmář)
https://www.youtube.com/watch?v=mWB2ralMAG0

GUES
HESLO
CZ.NIC
fest.cz
Adam Kalisz

V minulých dílech jste viděli...

-L Local Port Forwarding

-R Remote Port Forwarding

-D Dynamic Port Forwarding/ SOCKS Proxy

-w TUN/ "VPN"

(SSH over TOR, SSH over DNS)

```
/etc/services
```

```
%WINDIR%\system32\drivers\etc\services
```

Anything over HTTP(S)

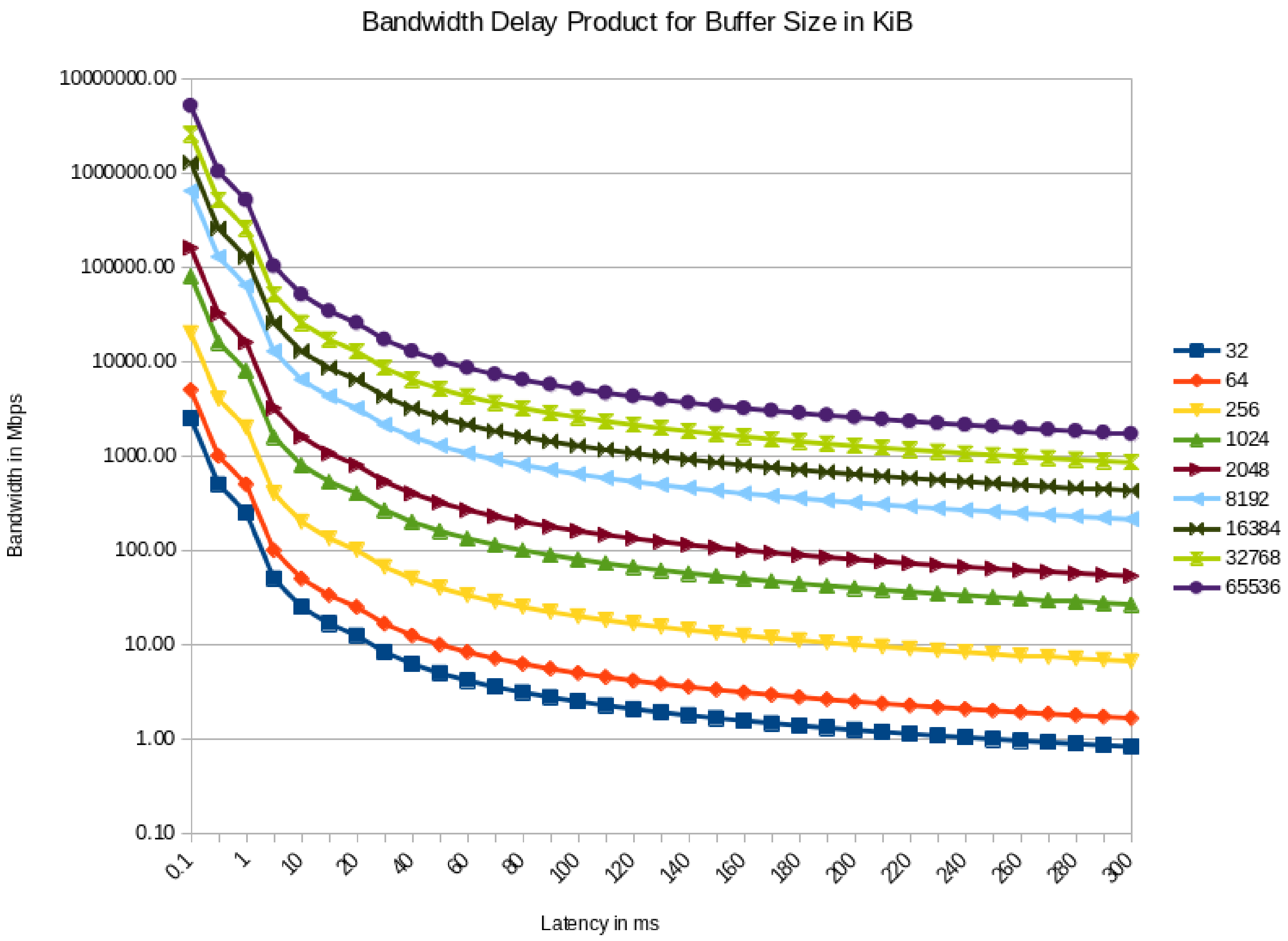
- Chisel (https://github.com/jpillora/chisel)
- Teleport https://goteleport.com/
- Guacamole https://guacamole.apache.org/
- SSH over HTTP/3 or QUIC
  https://github.com/francoismichel/ssh3
- WS tunnel https://github.com/erebe/wstunnel

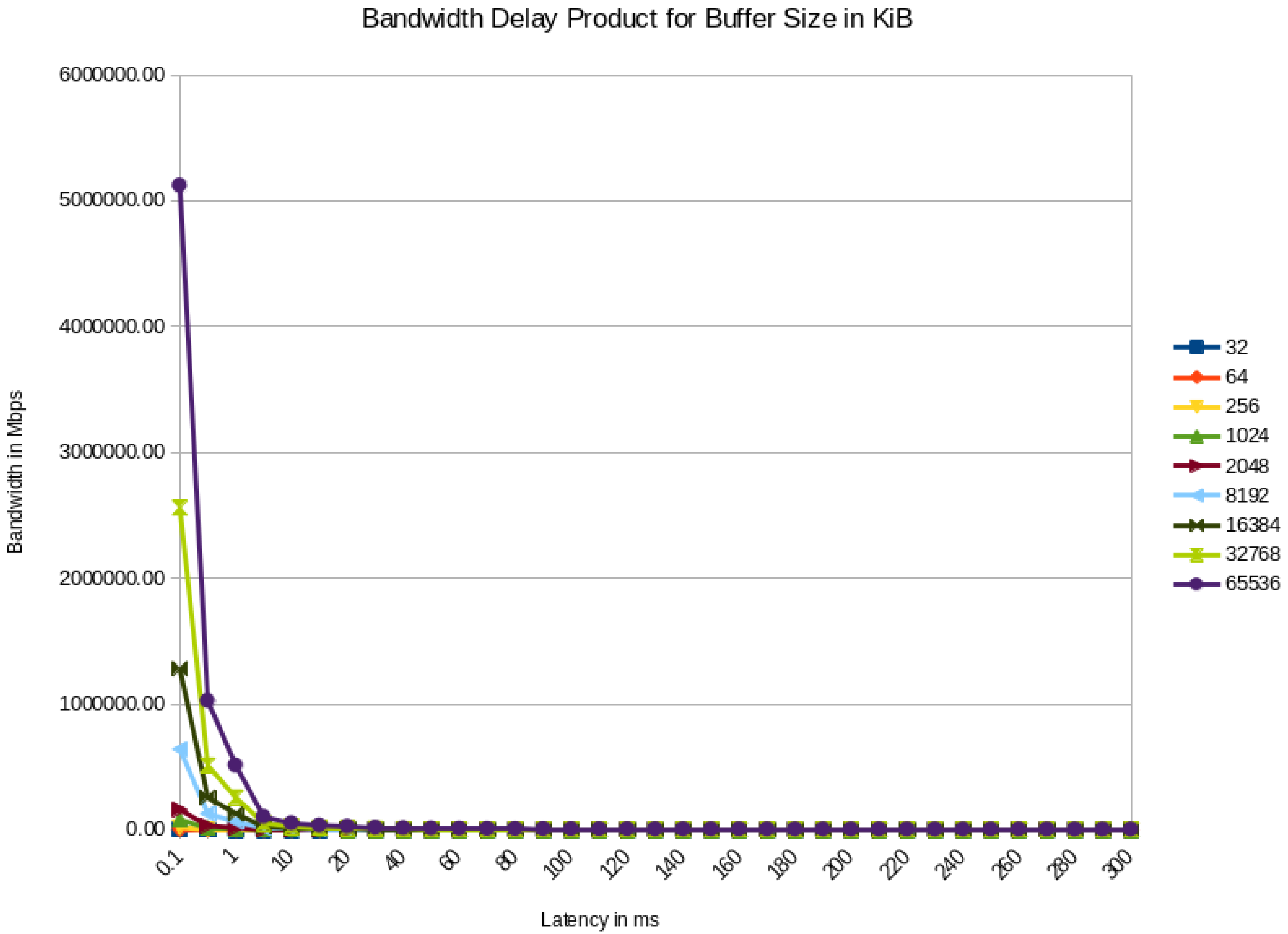
What is left?

- WebRTC https://github.com/rtctunnel/rtctunnel
- ICMP (https://github.com/DhavalKapil/icmptunnel)
- RDP (https://rdp2tcp.sourceforge.net/)
- FTP
- NTP
- Exchange ActiveSync
- SMTP/ Submission/ IMAP/ POP3

Performance

Bandwidth Delay Product


Bandwidth Delay Product for Buffer Size in KiB
Bandwidth in Mbps
10000000.00
1000000.00
100000.00
10000.00
1000.00
100.00
10.00
1.00
0.10
0.1
1
10
20
40
60
80
100
120
140
160
180
200
220
240
260
280
300
Latency in ms
32
64
256
1024
2048
8192
16384
32768
65536


Bandwidth Delay Product for Buffer Size in KiB
Bandwidth in Mbps
6000000.00
5000000.00
4000000.00
3000000.00
2000000.00
1000000.00
0.00
0.1
1
10
20
40
60
80
100
120
140
160
180
200
220
240
260
280
300
Latency in ms
32
64
256
1024
2048
8192
16384
32768
65536

Growing Latency, Falling Bandwidth

- Be smarter
- AQM (e.g. using CAKE, fq_codel)
- Congestion Control (BBRv2/v3?)
- Prioritization of ACKs (ToS, DiffServ, ECN)
- Appropriate buffer size
- LASER/ MW links

Problems With SSH

- Buffers at max 2 MB
- Slow establishment of connections
- Security vs performance

```
ip netns add ns-bad
ip link add veth-good type veth peer \
  name veth-bad
ip link set veth-bad netns ns-bad
ip netns exec ns-bad ip link set dev \
  veth-bad up && ip netns exec ns-bad ip \
  address add 172.16.0.1/24 dev veth-bad
ip link set dev veth-good up && \
  ip addr add 172.16.0.2/24 dev veth-good
ip netns exec ns-bad tc qdisc add dev \
  veth-bad root netem delay 25ms
tc qdisc add dev veth-good root netem delay 25ms
```

stunnel

```
ip netns del ns-bad
ip link del veth-good
```

KexAlgorithms, Ciphers, (MACs)

Thank You

For later questions, feedback:

adam.kalisz@notnullmakers.com