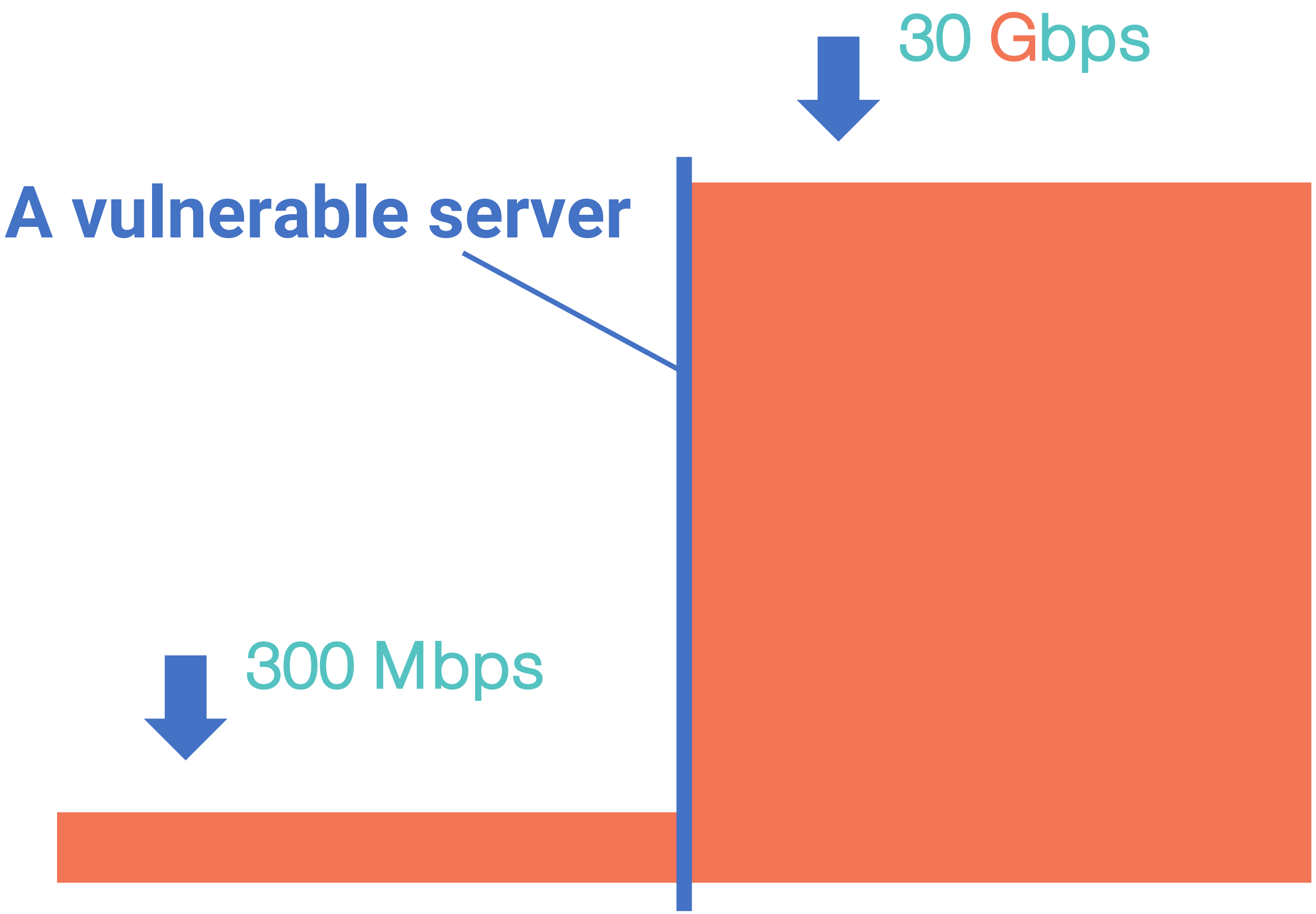
Memcached amplification

Artyom Gavrichenkov <ag@qrator.net>

Typical amplification attack

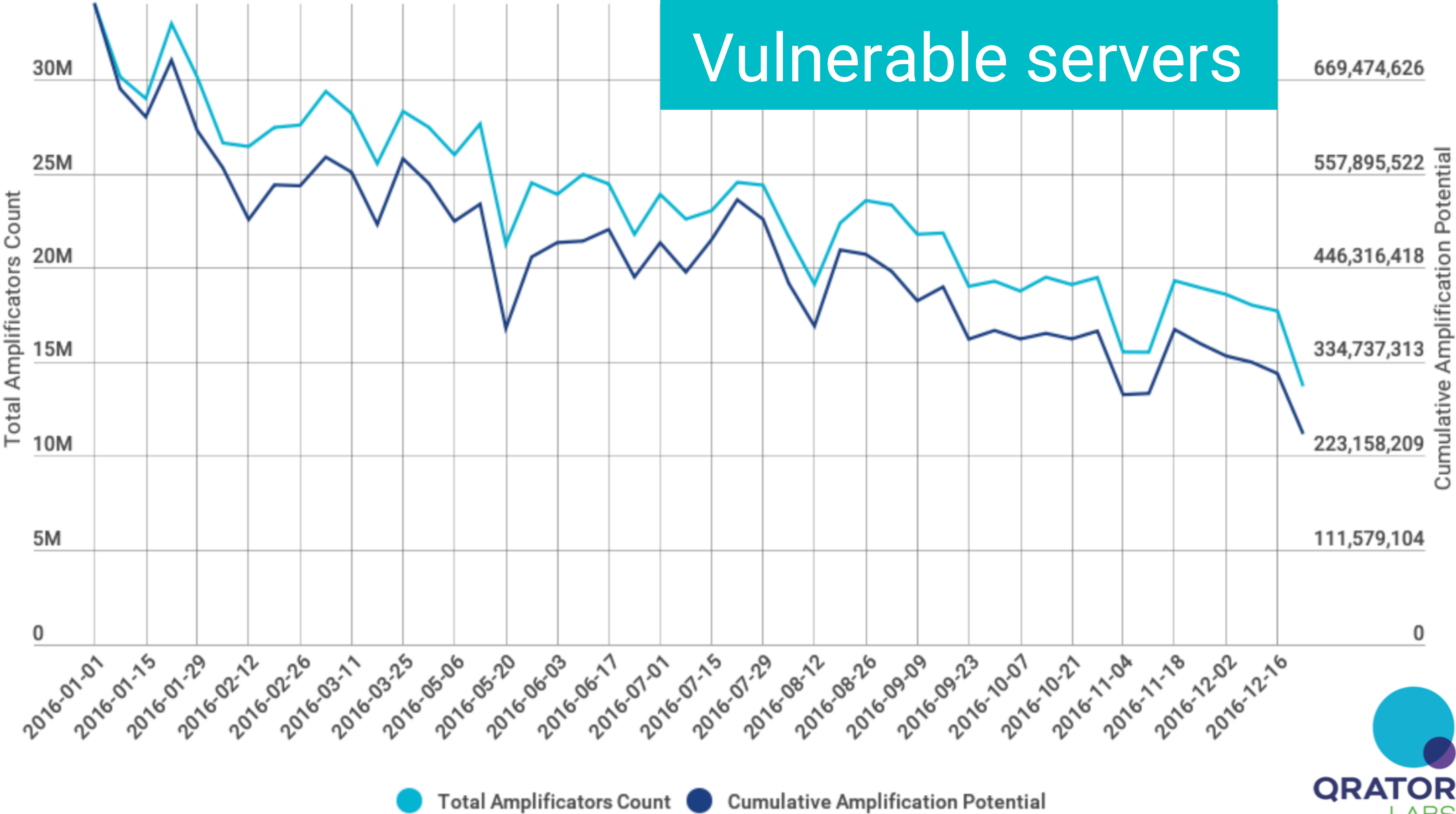
- Most servers on the Internet send more data to a client than they receive
- UDP-based servers generally do not verify the source IP address
- This allows for amplification DDoS



Vulnerable protocols

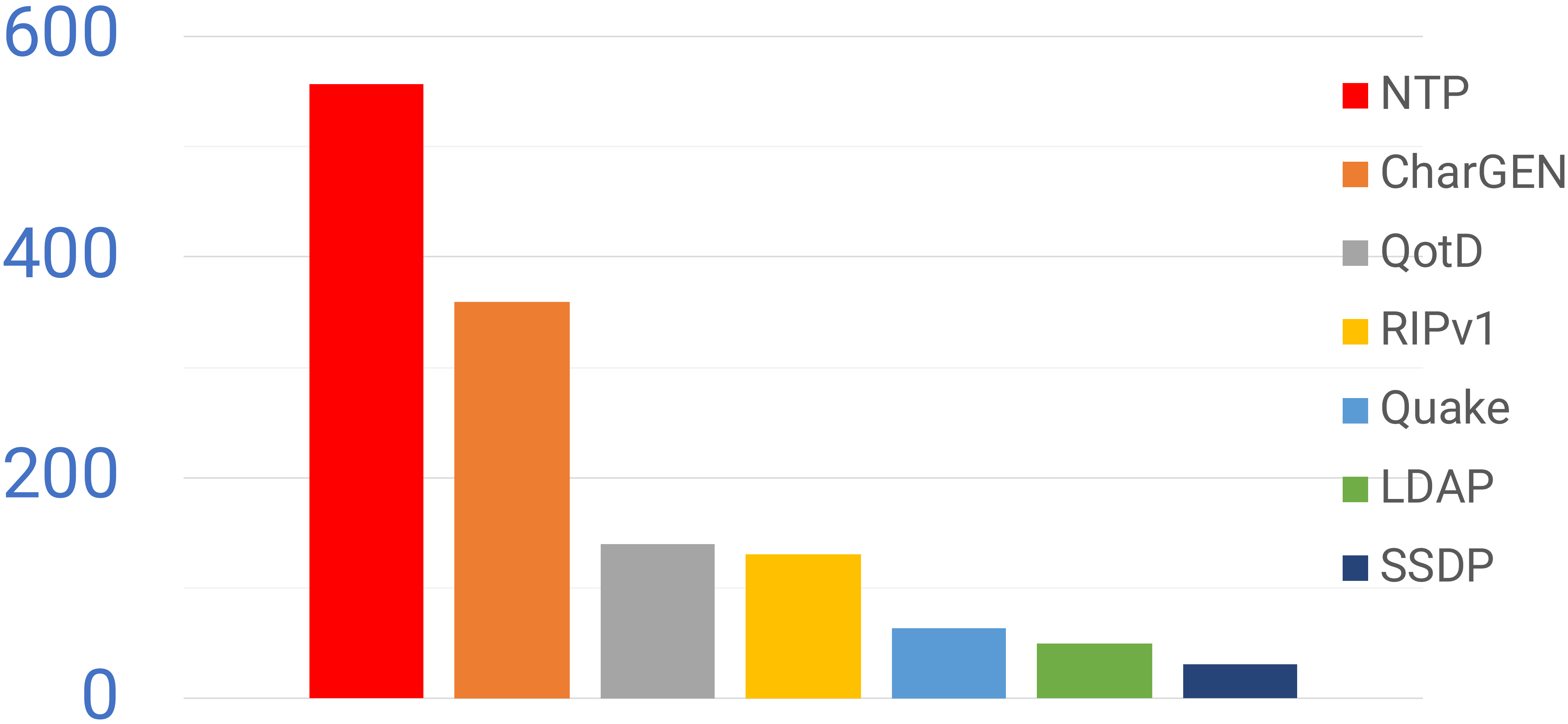
- NTP
- DNS
- SNMP
- SSDP
- ICMP
- NetBIOS
- RIPv1
- PORTMAP
- CHARGEN
- QOTD
- **Quake**
- …

Vulnerable servers



QRATOR LABS

Amplification factor



QRATOR LABS

memcached

- A **fast** in-memory cache
- Heavily used in Web development

memcached

- A **fast** in-memory cache
- Heavily used in Web development

- Listens on all interfaces, port 11211, by default

memcached

- Basic ASCII protocol doesn’t do authentication
- 2014, **Blackhat USA**:
  “An attacker can inject arbitrary data into memory”

memcached

- Basic ASCII protocol doesn’t do authentication
- 2014, **Blackhat USA**:
  “An attacker can inject arbitrary data into memory”

- **2017, Power of Community:**

  “An attacker can send data from memory to a third party via spoofing victim’s IP address”

```
import memcache
m = memcache.Client([
    ‘reflector.example.com:11211’
])
m.set(’a’, value)
```

– to inject a value of an arbitrary size under key “a”

```
print ’\0\x01\0\0\0\x01\0\0gets a\r\n’
```

– to retrieve a value

```
print ’\0\x01\0\0\0\x01\0\0gets a a a a a\r\n’
```

– to retrieve a value **5 times**

```
print ’\0\x01\0\0\0\x01\0\0gets a a a a a\r\n’
```

– to retrieve a value **5 times.**

Or 10 times.

Or a hundred.

memcached

- Theoretical amplification factor is **millions**

memcached

- Theoretical amplification factor is **billions**

- Fortunately, all the packets aren’t sent at once
- In practice, the amplification factor is 9000-10000

- **Still 20 times the NTP Amplification does.**

- Current incidents range between 200 and 500 Gbps
- Up to 1,5 Tbps can be expected

Mitigation

- Again, BCP 38.

- Make sure you don’t have open `memcached` port `11211/udp` on your network

- Use firewalls or FlowSpec to filter `11211/udp`

Mitigation

- Again, BCP 38.

- Make sure you don’t have open `memcached` port `11211/udp` on your network

- Use firewalls or FlowSpec to filter `11211/udp`

- **More news as events warrant**

Q&A

mailto: Artyom Gavrichenkov <ag@qrator.net>

https://medium.com/@qratorlabs/