Deep Packet Inspection Challenges in a Transport Network

Artyom Gavrichenkov <ag@qrator.net>

GPG: 2deb 97b1 0a3c 151d b67f 1ee5 00e7 94bc 4d08 9191

Qrator Traffic Filtering Network

A global **anycast network** for traffic filtering and **DDoS** mitigation

Each point of presence:

- A properly chosen **generic hardware**
- A custom-built **DPI software**

Qrator Traffic Filtering Network

A **8 years** experience in:

- **DPI** appliance **design**
- **DPI R&D**
- Deployment and integration:
  - **ISP** networks
  - **Enterprise** networks

Qrator Traffic Filtering Network

The main purpose is **availability**

- Traffic analysis
- Monitoring and provisioning
- DDoS mitigation

DDoS Mitigation

A full OSI stack traffic analysis

L3: simple traffic **filtering**,
complex **network scanning** and mapping

L4-6: simple **flow assessment**,
complex aspects of **TCP/TLS edge cases**

L7: complex **session analysis**,
simple **Big Data** tooling

(haha, *not really*)

“L7 Packet Filtering”

An assumption:

“a simple packet-based analysis is just enough to tell malicious intent from a legitimate one, L3-L7-wise”

“L7 Packet Filtering”

This is **convenient.**

- Computational complexity
- Implied unreliability of sec. appliances
- SPAN, Netflow/IPFIX

“L7 Packet Filtering”

This is **convenient approach**,
contradicting the nature of **TCP/IP layering.**

It was theoretically vulnerable
even in the age of **cleartext.**

“L7 Packet Filtering”

This is **convenient approach**,
contradicting the nature of **TCP/IP layering.**

It was ~~theoretically~~ vulnerable
even in the age of **cleartext.**

GoodbyeDPI

https://github.com/ValdikSS/**GoodbyeDPI**

GoodbyeDPI

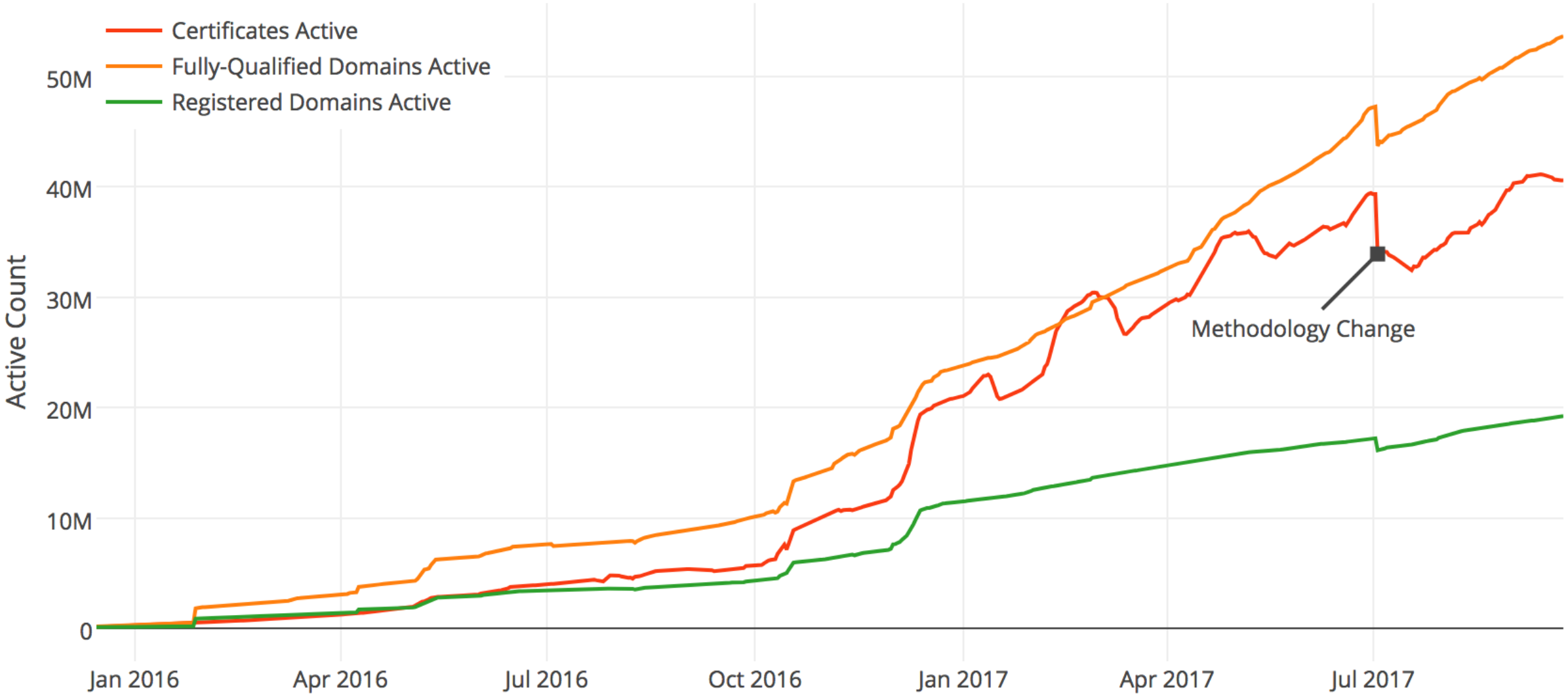
- **IP ID** Analysis
- TCP **Fragmentation**
- HTTP **Header Mangling**

GoodbyeDPI

- **IP ID** Analysis
- TCP **Fragmentation**
- HTTP **Header Mangling**

- **Game over** for most of DPI deployed by ISP

Let's Encrypt Growth



Percentage of Web Pages Loaded by Firefox Using HTTPS

(14-day moving average, source: Firefox Telemetry)

“L7 Packet Filtering”

This is **convenient approach**,
contradicting the nature of **TCP/IP layering.**

It was ~~theoretically~~ vulnerable
even in the age of **cleartext.**

With heavy **TLS** and **PFS** deployment happening recently,

packet-based approach is **helpless** even for the means of DDoS mitigation.

Perfect Forward Secrecy

- Present in ephemeral Diffie-Hellman ciphers
- **Mandatory in TLS v1.3**
- Makes **out-of-path** analysis **impossible**
- Makes **historic data** analysis **impossible**

Perfect Forward Secrecy

Good catch for an out-of-path DPI and/or WAF

70% HTTPS requests come and go without analysis

Perfect Forward Secrecy

Good catch for an out-of-path DPI and/or WAF

70% { 60% legitimate
90% malicious } HTTPS requests come and go without analysis

The Purpose of DPI

The Purpose of DPI

- DDoS mitigation
  (enough said already)
- General QoS and shaping
- Parental control

The Purpose of DPI

- DDoS mitigation (enough said already)
- General QoS and shaping
- Parental control
- Targeted advertisement
- Copyright abuse countermeasures
- Lawful interception and filtering of unwanted content

(no matter the definition of “unwanted”)

The Purpose of DPI

- DDoS mitigation (enough said already)
- General QoS and shaping
- Parental contr[illegible]
- Targeted advertisement
- Copyright abuse measures
- Lawful interception and filtering of unwanted content

Within an IP transport network

(no matter the definition of "unwanted")

The Purpose of DPI

- DDoS mitigation (enough said already)
- General QoS and shaping
- Parental contr…
- Targeted advertisement
- Copyright abuse
- …measures
- Lawful inter… filt… …wanted …tent

Within an IP transport network

With comp. complexity of conn/sess. tracking

(no matter the definition of "unwanted")

Catastrophic backtracking

- **RegEx** over every single packet

Catastrophic backtracking

- **RegEx** over every single packet

```
(x+x+)+y
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx...x
```

$O(n^2)$ behaviour!

https://blog.codinghorror.com/regex-performance/

DPI Caveats

A DPI is commonly believed to be **a silver bullet**,

a sort of products, supposedly available
for purchase and deployment,

designed to handle **every** DPI goal out there.

DPI Caveats

A DPI is commonly believed to be **a silver bullet**,

designed to handle **every** DPI goal out there.

In reality, DPI is just a **common** characteristics
of a broad range of solutions,
each designed to handle a **single** DPI goal

A DPI is commonly believed to be **a silver bullet**,

designed to handle **every** DPI goal out there.

In reality, DPI is just a **common** characteristics
of a broad range of solutions,
each designed to handle a **single** DPI goal

A **single** piece of equipment
won't cope with **every** DPI goal

Even with a single goal,

there's a ***trade-off***
between the packet processing ***speed***

and the expected ***functionality***
to a certain extent.

Network design: transparent IP network

- VoIP
- Gaming
- Overlay networks

Network design: transparent IP network

- VoIP
- Gaming
- Overlay networks

- Enterprise VPN
- Modern Web:
  HTTP/2, MPTCP, QUIC…
- Modern Net:
  TLS v1.3, DNSSEC, CAA…

Network design: transparent IP network

DPI **breaks** this transparency.

The outcome

The outcome

- Several important applications **suffer**

Placeholder: NAT/Middleboxes

- TLS 1.3 shows increased connection failure rates in the field
  - Hard to get clear measurements, but probably the 1-10% range
  - Problem seems to be middleboxes
- Currently studying various approaches
  - Make connection look less like TLS 1.2 (PR#1051)
  - Make flight look more like TLS 1.2 (maybe like resumption?)
  - Fallback paired with middlebox fixing
  - More data needed.
- More soon (next few months)

(slides by Eric Rescorla, http://tinyurl.com/tls13ietf99)

The outcome

- Several important applications **suffer**
- Others **adapt**

Placeholder: NAT/Middleboxes

- TLS 1.3 shows increased connection failure rates in the field
  - Hard to get clear measurements, but probably the 1-10% range
  - Problem seems to be middleboxes
- Currently studying various approaches
  - Make connection look less like TLS 1.2 (PR#1051)
  - Make flight look more like TLS 1.2 (maybe like resumption?)
  - Fallback paired with middlebox fixing
  - More data needed.
- More soon (next few months)

An Arms Race

- ENOG 13: the **ISP Security Roundtable**
- It takes up to **4-6 months**
  to deploy an updated network firmware
  even in case of a vulnerability discovered

4-6 months

- 2-3 months
  on the vendor side
  alone.

Илья Медведовский
17 августа ·

С одной стороны:
- 252 000 уязвимых роутеров в Интернете;
- главный приз pwn-конкурса в Гонконге в мае.
С другой:
- "Вероятно мы закроем эту уязвимость в октябре".

Циско, прекрати, зачем так быстро.

Нравится Комментарий Поделиться

4-6 months

- 2-3 months
  on the vendor side
  alone.

- 2-3 months **more** to roll out the update all across the IP network.

An Arms Race

- It takes up to **4-6 months**
  to deploy an updated network firmware.

- A modern application
  (including, but not limited to IoT and malware)

  makes heavy use of the **CI/CD** approach,
  enabling it to roll out a new release **several times a day.**

An Arms Race

- It takes up to **4-6 months** to deploy an updated network firmware.

- A modern application (including, but not limited to IoT and malware)

  makes heavy use of the **CI/CD** approach, enabling it to roll out a new release **several times a day.**

An Arms Race → is lost at that point.

- It takes up to **4-6 months** to deploy an updated network firmware.

- A modern application (including, but not limited to and malware)

makes heavy use of the **CI/CD** approach, enabling it to roll out a new release **several times a day.**

The Day after Tomorrow

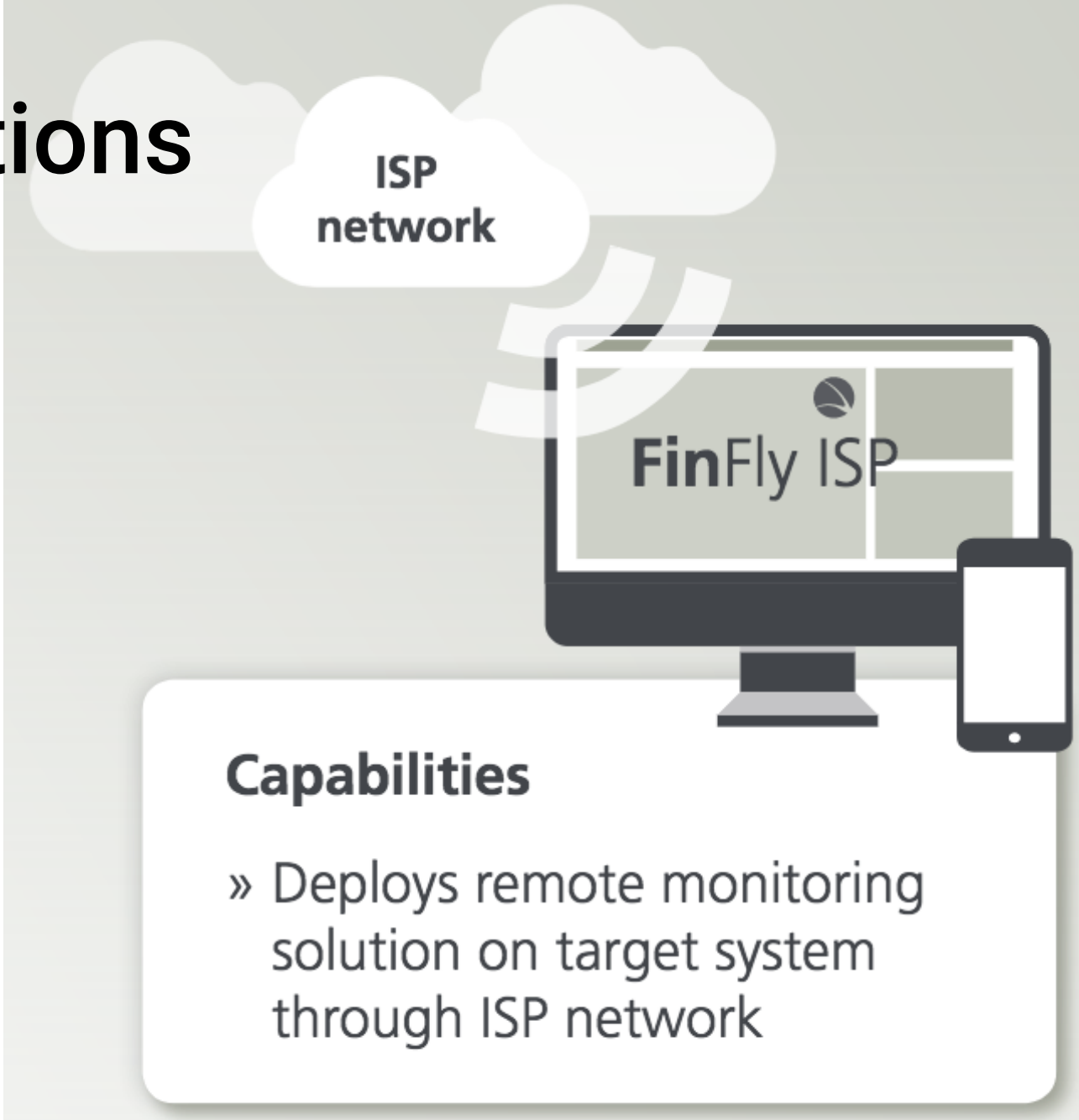
- A packet-based DPI is **unsufficient**

  It has its regions of applicability though – it's **when you're fine with 80/20 rule**:
  - Parental control
  - Simple QoS
  - Targeted advertisement
  - **General** lawful interception and copyright enforcement
- A session-based DPI is **vulnerable**
  when neither a client nor a server is under the DPI vendor control

  The implied heavy computational complexity
  renders a DPI unable to transparently handle
  every new network activity in time, as it goes.

Security Considerations

- DPI: complex solution
- Security awareness of vendors?
- FinFisher spyware as a PoC
- The risk and the implied loss potential are beyond imagination
  (i.e. a “futurological congress” scale)



The right way for a network entity,
destined to build some non-transparent solutions
in a middle of IP transport network,

The right way for a network entity,
destined to build some non-transparent solutions
in a middle of IP transport network,
is to join **RIPE, IETF**, and **ICANN** activities
in order to clarify the requirements
and to build a network solution that will survive
the day after tomorrow.

The right way for a network entity,
destined to build some non-transparent solutions
in a middle of IP transport network,
is to join **RIPE, IETF**, and **ICANN** activities
in order to clarify the requirements
and to build a network solution that will survive
the day after tomorrow.

Either this, or an **unreliable IP transport**,
ad-hoc applications,
and **an inherent instability** of the **core** infrastructure.

Q&A

Artyom Gavrichenkov <ag@qrator.net>