APPLICATION-AWARE FLOW MONITORING

Thursday 11th April, 2019

Petr Velan

MUNI
ICS

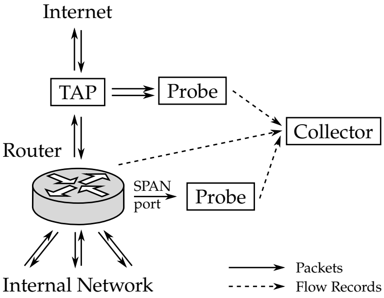
CSIRT-MU

Motivation

Basic Flow Monitoring

Flow monitoring is widely used for:

- Accounting
- Security (IDS, forensics)
- Data retention
- Network diagnostics



Basic flow record example:

```
Flow start    Duration Proto     Src IP Addr:Port          Dst IP Addr:Port    Flags   Packets   Bytes
09:41:21.763    0.101  TCP      172.16.96.48:15094 ->  209.85.135.147:80      .AP.SF        4     715
09:41:21.893    0.031  TCP    209.85.135.147:80     ->    172.16.96.48:15094  .AP.SF        4    1594
```

Flow creation process is complex

- Flow vs. connection, fragmented traffic, flow termination conditions, flow keys from multiple layers
- ⇒ Definition of flow is necessary

Application Layer Information

Application visibility, such as provided by DPI, improves security and network diagnostics.

- Application identification (not relying on well-known ports)
- Encapsulating application protocols (HTTP used for audio/video streaming)
- Information about tunnels (e.g., MPLS, VLAN, IPv6 transition mechanisms)

Basic flow contains only selected information from packet headers.

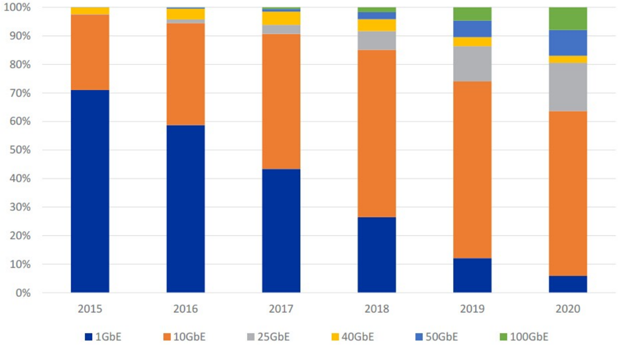
- Gather more information available from the headers (L2 layer)
- Analyze application layer information (application identification and visibility)

Application flow record example:

```
Flow start   L3,4        HTTP Host             HTTP URL                          HTTP User Agent   Rsp. Code
09:41:21.763 ....  www.example.com  /requested/endpoint  ’Mozilla/5.0 AppleWebKit/531.21.10 ...’
09:41:21.893 ....                                                                                        200
```

Growing Network Speeds

10 G, 25 G, 40 G and 100 G: Seeing Broad Adoption in Data Center



http://techblog.comsoc.org/tag/25-100g-ethernet/

Growing Network Speeds

- Very short time to process individual packets
- Large number of concurrent flows increase memory utilization

	10 G		100 G	
	pps	CPU cycles*	pps	CPU cycles*
Smallest frame size	14.88 M	201	148.81 M	20
800 B packets	1.49 M	2011	14.92 M	201

* On a 3 GHz CPU core

Multiple concepts must be combined:

- Multi-core and multi-processor systems
- Specialized NICs (FPGA-based)
- Software (user and kernel space) optimizations

Traffic Encryption

Increasing amount of encrypted traffic (SSL/TLS, DTLS, IPsec, . . .):

- Privacy becomes increasingly important
- Free certificates (Let’s Encrypt)

DPI fails for encrypted traffic:

- No precise application identification (back to port numbers)
- No application layer visibility

Some information still available:

- Encryption protocol headers (e.g., certificates, ciphers)
- Statistical information ⇒ machine learning

Thesis Goals

- Propose application flow monitoring which utilises application layer information to facilitate flow analysis and threat detection.
- Evaluate performance of flow monitoring and propose optimisations to facilitate monitoring of high-speed networks.
- Analyse options for monitoring of encrypted traffic, survey common encryption protocols and methods for encrypted traffic classification.

Application Flow Monitoring

Flow Definition

IPFIX and NetFlow v9 flow definitions have a few shortcomings:

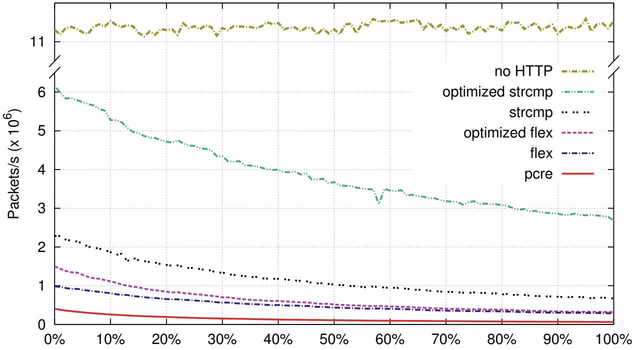
- Limited to IP flows
- Do not account for fragmented packets
- Unclear definition of packet characteristics

Proposed a new definition which addresses these problems:

> *A flow is defined as a sequence of packets passing an observation point in the network during a certain time interval. All packets that belong to a particular flow have a set of common properties derived from the data contained in the packet, previous packets of the same flow, and from the packet treatment at the observation point.*

Formalization of the definition avoids misinterpretation.

HTTP Parser Design



Parser Performance Comparison with Respect to HTTP Proportion (0 % - No HTTP, 100 % - Only HTTP Headers) in the Traffic - Full Packets 1500 B.

Use of Application Information

Security monitoring of HTTP traffic:

- Classification of HTTP traffic
- Repeated requests (proxies and brute-force attacks)
- HTTP scans
- Web crawlers

IPv6 transition mechanisms:

- Teredo, protocol 41 (e.g., 6to4, 6in4), ISATAP, AYIYA
- Detection of tunnel endpoints
- Geolocation of endpoints, optimization of traffic routes
- Anomalies, misconfiguration (forwarding of local-link packets inside tunnels)
- OS fingerprinting

Flow Monitoring Performance

Flow Acceleration

Hardware acceleration	Software acceleration
Receive Side Scaling	Multithreading
Packet trimming	NUMA awareness
Packet header preprocessing	Flow state in parsers
Flow processing offloading	Flow cache design
Application identification	Per-flow expiration timeout
	Delayed packet processing
	Bidirectional flow records

Flow Acceleration Techniques (Novel Proposals).

Novel Flow Acceleration Techniques

Packet header preprocessing:

- Extraction of information from packet headers by the NIC
- Only necessary information sent to software
- Minimizes data transfers, lowers utilization of memory controller

Application identification:

- Only small portion of packets carry important application protocol information
- Packets containing important headers can be identified by NIC

Flow state in parsers:

- Flows with application information are usually processed by only single parser
- Apply parsers from the most common to the least common one
- Skip application parsers after important information is extracted

High-Density Flow Monitoring

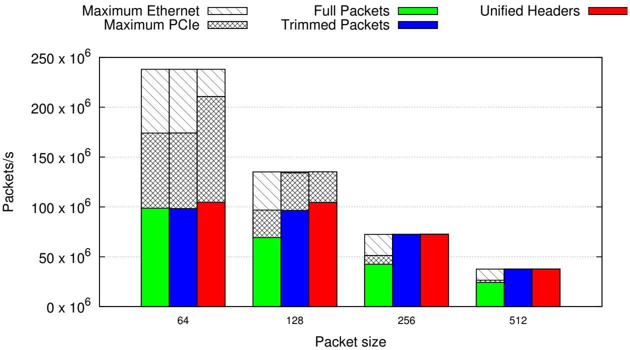
Aggregate measurement of multiple 10 G links in a single box.

- 2 NICs (2x40 G ports configured as 8x10 G)
- Theoretical throughput: 160 Gbps
- Test impact of packet trimming and packet header preprocessing in NIC
- Different flow counts, packet sizes
- Test impact of CPU choice (6 vs 8 cores, 2 GHz vs 2.6 GHz)

Results:

- Line-rate is achievable for 128 B packets with hardware acceleration
- Impact of flow count is significant for short packet lengths
- Choice of CPU (especially frequency and number of cores) is very important

Impact of Packet Trimming and Preprocessing



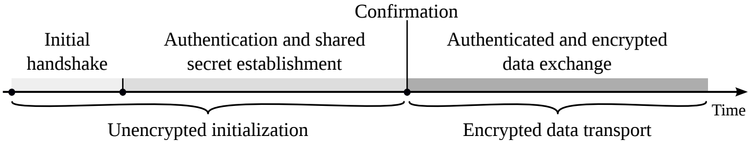
Packet Processing Performance Comparison in Packets/s for 16,384 Flows per Interface.

Measurement of Encrypted Traffic

Information Extraction From Encrypted Traffic

Some information remains disclosed even for encrypted traffic:

- Initialisation of the encrypted connection is usually unencrypted
- TLS up to version 1.3 discloses certificates
- SNI still available, but propositions are being made to encrypt it
- Combination with DNS monitoring is possible
- These information can be used directly by flow monitoring system
- Information about offered cryptographic algorithms can be used to fingerprint clients


Confirmation
Initial handshake
Authentication and shared secret establishment
Authenticated and encrypted data exchange
Time
Unencrypted initialization
Encrypted data transport

Encrypted Traffic Classification

Identification of encrypted protocols is not always possible.

- Machine learning and statistical methods can be used
- Surveyed works published in the top related conferences and journals from 2004 to 2015

Payload-based classification techniques:

- Mostly ready-to use tools
- Utilized in practice for DPI

Feature-based classification techniques:

- Intensive research area
- Most authors use private datasets
- Incomparable results

Future Work

Concepts for Next Generation Flow Monitoring

EventFlow

- Group flows based on actions
- Proof of concept implemented on HTTP and DNS protocols

MetaFlow

- Hierarchical structure for flows
- Useful for monitoring of layered traffic
- Helps to reduce number of flow data templates

Application Events

- Similar to MetaFlow
- Do not create application flows (can disrupt basic flow creation process)
- Attach application information to basic flow in separate record

THANK YOU FOR YOUR ATTENTION!

https://is.muni.cz/th/a2fxd/

@csirtmu

Petr Velan

velan@ics.muni.cz

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MŠMT
MINISTRY OF EDUCATION,
YOUTH AND SPORTS

MUNI
ICS

CSIRT-MU