MUNI
C4E

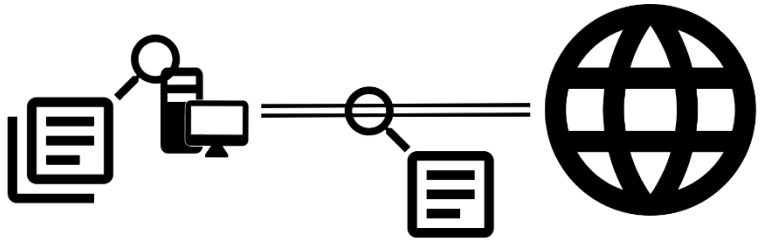
Event-Flow Correlation of the HTTP/3 Web Traffic

Stanislav Špaček, Petr Velan, Martin Holkovič, Tomáš Plesník

Motivation

- Web traffic is currently mostly encrypted
- Analysis of encrypted traffic is inaccurate and costly
  - Unecrypted handshakes
  - Statistical features
  - Reencryption proxies
- HTTP/3 fundamentally changes its web traffic
- Enrich network monitoring by data from host-based monitoring

Host-Based and Network Monitoring



	timestamp	server	message
1	10:21:01.154	10.0.0.1	client 10.0.0.5#44630 (www.yahoo.com):...
2	10:21:13.278	10.0.0.1	client 10.0.0.2#42543 (intel.com): query: ...
3	10:21:21.004	10.0.0.1	client 10.0.0.5#35721 (www.google.com):...
4	10:21:22.152	10.0.0.1	client 10.0.0.3#32849 (example.com): qu...

start_t	end_t	src	dst	bytes	proto	application data	
10:21:00	10:21:01	10.0.0.5	10.0.0.1	16	QUIC		A
10:21:12	10:21:13	10.0.0.2	10.0.0.1	15	QUIC		B
10:21:20	10:21:21	10.0.0.5	10.0.0.1	18	QUIC		C
10:21:20	10:21:22	10.0.0.3	10.0.0.1	25	QUIC		D

Event-Flow Correlation: 1A, 2B, 3C, 4D

MUNI C4E

Benefits and Restrictions

- Benefits of event-flow correlation
  - Enrichment of encrypted network traffic monitoring
  - Consistency check for event logs
  - Improvement of situational awareness for incident handlers
- Restrictions of event-flow correlation
  - Time synchronization of monitoring infrastructure
  - Monitoring of custom features necessary
  - Usable only for „internal“ web services

Research Topic

- Correlation of HTTP/3 events and IP flows
- Research questions:
  - *How does event-flow correlation perform in a controlled environment?*
  - *How accurately can we correlate HTTP/3 events and flows compared to HTTP/2?*

MUNI C4E

Common Feature Set

Feature		HTTP	
Event	**Flow**	**HTTP/2**	**HTTP/3**
time-generated	[START_NSEC, END_NSEC]	✓	✓
s-ip	L3_IPV4_DST	✓	✓
s-port	L4_PORT_DST	✓	✓
c-ip	L3_IPV4_SRC	✓	✓
c-port	L4_PORT_SRC	✓	✓
cs-host	HTTP_REQUEST_HOST	✓	⊘

Correlation Method

- A single method based on the common feature set
- Evaluated on both HTTP/2 and HTTP/3 web traffic
- Input filters to eliminate prematurely terminated IP flows (maligned, crawlers)

Dataset

- Six days of web traffic of a single web server in a controlled environment
- Approximately 30 000 events and 1 000 IP flows
- HTTP/2 and HTTP/3 web traffic
- Events and IP flows captured directly on the server

Evaluation

	HTTP/2		HTTP/3	
	Single Events	Single Flows	Single Events	Single Flows
No Filter	0 %	64.13 %	0 %	25.04 %
HTTP Error Filter	0 %	62.07 %	8.93 %	25.78 %
Handshake Filter	0 %	27.54 %	0 %	16.03 %
All Filters	0 %	26.39 %	-	-

MUNI C4E

Conclusion

- 100 % of HTTP/3 and HTTP/2 events were assigned to IP flows
- The share of correlated IP flows remained lower (74 % HTTP/2, 84 % HTTP/3)
- Precision of time measurement was an issue in Windows Server
- Event-Flow Correlation remains viable for HTTP/3 web traffic

MUNI
C4E

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

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

C4E.CZ