CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

HTTPS Event-Flow Correlation: Improving Situational Awareness in Encrypted Web Traffic

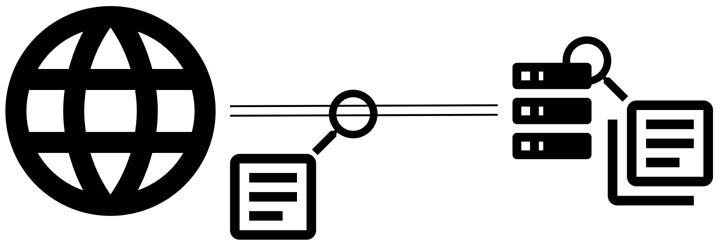
Stanislav Špaček, Petr Velan, Pavel Čeleda, Daniel Tovarňák

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 830927.

Motivation

- Web traffic is currently mostly encrypted
- Analysis of encrypted traffic is inaccurate and costly
  - Unecrypted handshakes
  - Statistical features
  - Reencryption proxies
- Enrich network monitoring by data from host-based monitoring

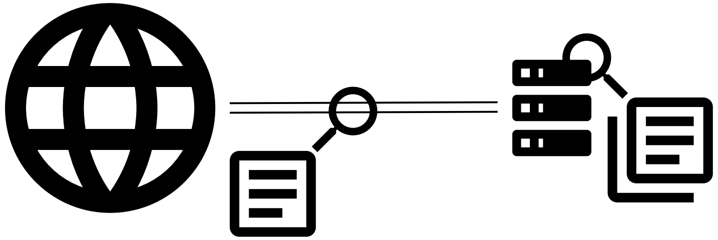
Host-Based and Network Monitoring I



Flows						
start_t	end_t	src	dst	bytes	proto	application data
10:21:00	10:21:25	10.0.0.5	10.0.0.1	1643	TLS	
10:21:19	10:24:03	10.0.0.2	10.0.0.1	1554	TLS	

Events		
timestamp	server	message
10:21:01.154	10.0.0.1	GET example.com 200 Mozilla/5.0+iPhone+OS
10:21:13.278	10.0.0.1	GET edu.example.com 200 Mozilla/5.0+iPhone
10:21:21.004	10.0.0.1	POST example.com 200 Mozilla/5.0+iPhone+O
10:21:22.152	10.0.0.2	GET example.com 200 Chromium/64.2+Windo

Host-Based and Network Monitoring II



	Flows						
	start_t	end_t	src	dst	bytes	proto	application data
1	10:21:00	10:21:25	10.0.0.5	10.0.0.1	1643	TLS	
2	10:21:19	10:24:03	10.0.0.2	10.0.0.1	1554	TLS	

Events			
timestamp	server	message	
10:21:01.154	10.0.0.1	GET example.com 200 Mozilla/5.0+iPhone+OS	A
10:21:13.278	10.0.0.1	GET edu.example.com 200 Mozilla/5.0+iPhone	B
10:21:21.004	10.0.0.1	POST example.com 200 Mozilla/5.0+iPhone+O	C
10:21:22.152	10.0.0.2	GET example.com 200 Chromium/64.2+Windo	D

Event-Flow Correlation: 1ABC, 2D

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 the HTTPS events and network flows
- Research questions
  - *How accurately can be events recorded on a web server correlated to the network flows that caused them?*
  - *What impact will future web traffic encryption technologies have on the accuracy of the correlation process?*

Common Features

Feature		HTTP			
Event	Flow	Plain	TLS 1.2	TLS 1.3	QUIC
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	✓	✓	✗	✗
cs-uri-stem	HTTP_REQUETS_URL	✓	✗	✗	✗
cs-user-agent	HTTP_USER_AGENT	✓	✗	✗	✗

Correlation Methods

- Four methods based on different sets of common features:
  - All-params – for TLS 1.2 encrypted flows
  - No-sni – TLS 1.3 and QUIC encrypted flows
  - No-port – environment does not allow custom features monitoring
  - No-port-sni – scenario with the least available data

Dataset

- Seven days of web traffic from a large campus network
- Approximately 3 000 000 flows and 6 000 000 events
- TLS 1.2 network flows and Windows Server events
- All devices time-synchronized with millisecond precision
- Webservers unable to log client port disqualified
- Dataset and all tools are public

Evaluation

	All-params	No-sni	No-port	No-port-sni
Accuracy	1,0000	0,9999	0,9999	0,9999
Precision	1,0000	0,9999	0,4055	0,3555
Recall	1,0000	1,0000	1,0000	1,0000
F1-Score	1,0000	0,9999	0,5770	0,5245

Conclusion

- Event-flow correlation may enrich encrypted web traffic monitoring with content and client data
- *How accurately can be events recorded on a web server correlated to the network flows that caused them?*
  - Event-flow correlation is suitable if client port can be monitored
- *What impact will future web traffic encryption technologies have on the accuracy of the correlation process?*
  - Lack of SNI in TLS 1.3 and QUIC has only marginal effect on correlation accuracy

Contact

Research Institute CODE
Carl-Wery-Straße 22
81739 Munich
Germany

contact@concordia-h2020.eu

Follow us

www.concordia-h2020.eu

www.twitter.com/concordiah2020

www.facebook.com/concordia.eu

www.linkedin.com/in/concordia-h2020

www.youtube.com/concordiah2020