Contribution ID : **17** Type : **not specified**

Real-Time Analytics of DNS packets

Thursday, 31 March 2016 11:30 (30)

In OARC 22 (Amsterdam) we gave a lightning talk about the possibilities and prospects of using Apache Storm for real-time analytics of DNS packets.

Now, after a year of work, we are glad to present RaTA-DNS, our modular system for realtime analytics. RaTA-DNS was designed as a set of self-contained modules aiming to an easy integration with existing systems such as DSC and Hedgehog, and new systems such as SIDN Lab's ENTRADA.

The main components of our system are three: Fievel, a packet monitor responsible for capturing network traffic and perform a preliminary processing (for reducing the data rate in order to be transmitted to aggregators); Gopher, which is responsible for aggregate the captured data received from multiple servers (Gopher was developed in Go language instead using the Apache Storm framework for modularity reasons); and Remy, the dashboard (data visualisations), which is connected to several Gopher modules to provide real time displays.

The idea is to provide a programmable framework for real-time monitoring of DNS. Thus, Fievel has been developed as a scriptable module, where preprocessing is programmable and adaptable to the needs of different users, producing a monitoring system fully customisable.

Additionally, as Fievel provides the tcp-replay function and Remy the play-pause-rewind functions, RaTA-DNS can be also seen as a very useful tool for forensic analysis of DNS traces.
Actually, RaTA-DNS is connected to 2 NIC Chile DNS servers, processing in a normal operations day around 1200 (queries-responses)/sec per server, and aggregating statistical information such as queries/sec, non-rfc-conformant queries (queries using underscores), top-K queries by source, destiny, and geolocation. Further information can be seen in http://ratadns.niclabs.cl

Summary

Primary author(s) : Dr. BUSTOS-JIMÉNEZ, Javier (NIC Chile Research Labs (NICLabs). Universidad de Chile)

Co-author(s) : Mr. CIFUENTES, Francisco (NIC Chile Research Labs)

Presenter(s) : Dr. BUSTOS-JIMÉNEZ, Javier (NIC Chile Research Labs (NICLabs). Universidad de Chile)

Session Classification : Public Workshop: First Session

Track Classification : Public Workshop