Dear all,
please please find enclosed my research proposal for the IAB M-TEN workshop. Hope this triggers your attention/

Regards Luca

Introduction
nDPI is an open source Dpi (Deep Packet Inspection) toolkit designed for:
• Detecting application protocol in both clear-text and encrypted traffic
• Extracting relevant metadata (e.g. TLS SNI) for enabling applications sitting on top of it to make traffic decisions (e.g. dropping or steering) as well further characterise traffic.
• Providing users an implementation of several speed-optimised streaming algorithms for classifying traffic, detecting communication similarities in encrypted traffic, or anomalies in traffic.

As nDPI is widely used in cybersecurity, it implements the concept of flow risk: nDPI labels a communication flow with a bitmap, where each bit is an indication of a specific issue named flow risk. To date nDPI support over 40 flow risks that belong to the following families:
• Suspicious Data Transfer (e.g. binary application trans- fer).
• Data Exfiltration (e.g. over ICMP and DNS).
• Unexpected Traffic (e.g. DNS packets larger than 512 bytes, TLS traffic with no SNI).
• Alerts based on communication with a remote host present on a third-party blacklist.
• Suspicious Traffic (e.g. suspicious SNI or unidirectional unicast UDP traffic).
• Elephant (i.e. large uploads/downloads) or Long-Lived Flows.
  • Insecure or Obsolete Protocol versions (e.g. TLSv1 or obsolete SSH client version).

Proposal
As nDPI maintainer I am open to join a collaborative effort whose goal is to improve traffic (including malicious traffic) classification by means of DPI techniques and traffic analysis. In particular:
• Define methods for classifying (unknown) encrypted traffic similar to what nDPI does with DoH that by means of binning techniques it can reliably detect this type of traffic.
• Improve fingerprinting techniques such as JA3 (nDPI also implements JA3+ that is an improvement of the original technique) for finding traffic similarities that can help to spot and eventually block encrypted flows produce by malware applications.
• Improve and extend flow risk to further classify communication flows to assist cybersecurity applications to carry-on their job.

Research Papers

Videos and Presentations
• Using nDPI for Monitoring and Security
• Network Traffic Classification for Cybersecurity and Monitoring

Code
• https://github.com/ntop/nDPI

--
Mten-workshop-pc mailing list
Mten-workshop-pc@iab.org
https://www.iab.org/mailman/listinfo/mten-workshop-pc