Network flows exporter supporting application information

Jiri Havranek
Faculty of Information Technology, Czech Technical University in Prague
Thakurova 9, 160 00 Prague 6, Czech Republic

havraji6@fit.cvut.cz

Keywords. exporter, network flow, application protocol, optimization, NEMEA, OpenWrt, IPFIX, HTTP, DNS

Abstract

Network traffic monitoring is a necessary part of nowadays computer networks administration. Gathered information is not only used to provide basic network functionality and problem detection, but also for security analysis.

Due to user privacy and reduction of data volume, approaches based on network flows are used. This work focuses on exporting flow records with application protocol extension. Contribution of this work is a new version of existing open source flow exporter from NEMEA project. This software module was optimized and successfully ported to embedded devices with OpenWrt system. It is possible to create network monitoring probe from low performance cheap home routers and enhance awareness of traffic on network including malicious traffic detection.

Besides memory and performance optimizations, the module is extended of capability reading packets from network interface with the libpcap library. Flow cache, that is used to store flow records during the computation, was improved in order to handle application protocol information. The implemented version of the flow exporter contains two new example plugins for parsing HTTP and DNS protocols. In addition, the exporter is now able to export data in the IPFIX format.

Acknowledgment

Ing. Tomas Cejka