HISTORY – High-Speed Network Monitoring and Analysis

Falko Dressler
Autonomic Networking, Dept. of Computer Science 7
University of Erlangen-Nuremberg
Erlangen, Germany
dressler@informatik.uni-erlangen.de

Georg Carle
Computer Networks and Internet
University of Tübingen
Tübingen, Germany
carle@informatik.uni-tuebingen.de

***Abstract*—In this paper we demonstrate the potentials of a new network monitoring architecture named HISTORY (High Speed Network Monitoring and Analysis). The basis of this approach is a high-speed monitoring probe allowing to process up to one gigabit per second on a standard PC. The complete architecture relies on standardized protocols such as IPFIX and PSAMP for transmission of monitoring data between the monitoring elements and successive traffic analysis. Especially the employed statistical methodologies allow the usage of History for various applications in network security such as intrusion detection and traceback. In this paper we introduce two tools developed in History for high-speed network monitoring (Vermont) and analysis (Nasty).**

Keywords—Network Monitoring, Traffic Analysis, Statistical Evaluation, Network Security

I. INTRODUCTION

The aim of the HISTORY project is to build an architecture, methods, and tools for distributed analysis of network traffic. In cooperation between the autonomic networking group and the computer networks and internet group, we work on new methodologies for high-speed network monitoring, which build a basis for intrusion detection and traceback mechanisms even in high-speed core networks. The network monitoring and analysis environment makes it possible to collect information about network traffic and its behavior in distributed network environments capable to operate on high-speed network links. The employment of standardized protocols, i.e. IPFIX (IP flow information export, [11]) and PSAMP (packet sampling, [4]), results in an extensible architecture. Additionally, we ensure the interoperability of our tools by contributing to the standardization process in these areas in the IETF working groups IPFIX, PSAMP, and NSIS.

The main objective is to develop methodologies for handling high amounts of statistics and packet data even with cheap low-end components. Visualization techniques and anonymization methods round off the big picture of a visionary environment for all challenges in network monitoring and analysis. Developed tools will be available under an open source license. The applicability was already verified by employing the monitoring equipment in research projects focusing on efficient intrusion detection, accounting, and traceback mechanisms.

Research Goals and Objectives

- Cooperative autonomous entities with distributed functioning
- Emergent behavior through adaptive self-organization
- Operation in high-speed networks while utilizing standard PC components
- Wide application range from accounting up to traffic engineering, intrusion detection and traceback
- Anonymization techniques for wide applicability

II. ARCHITECTURE

The complete architecture is depicted in Figure 1. Multiple distributed monitoring probes, in IPFIX terminology called exporters, are monitoring network traffic using different methodologies as described in the following subsection. The collected packets and statistics are transferred to a central collector for further processing. In general, this can even form a distributed architecture in a higher hierarchy. Such highly distributed architectures are our current research objectives and described in the further work. The Netflow.v9 [3], the IPFIX protocol [1, 2], and the corresponding PSAMP protocol [4, 6] are employed for encoding and transmitting the monitored data. In addition to the standard functionality of IPFIX or netflow accounting, we developed an aggregation technique that dramatically reduces the amount of monitoring data [9].

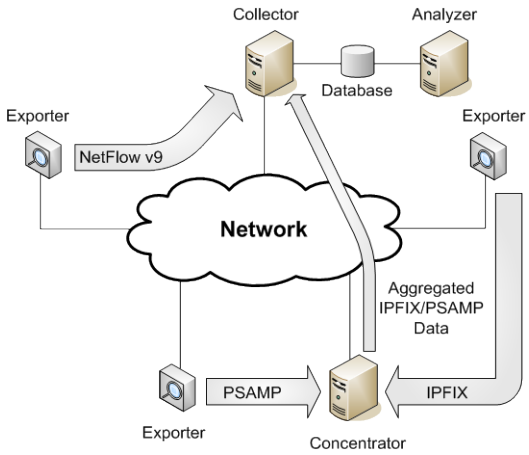

Figure 1. HISTORY architecture

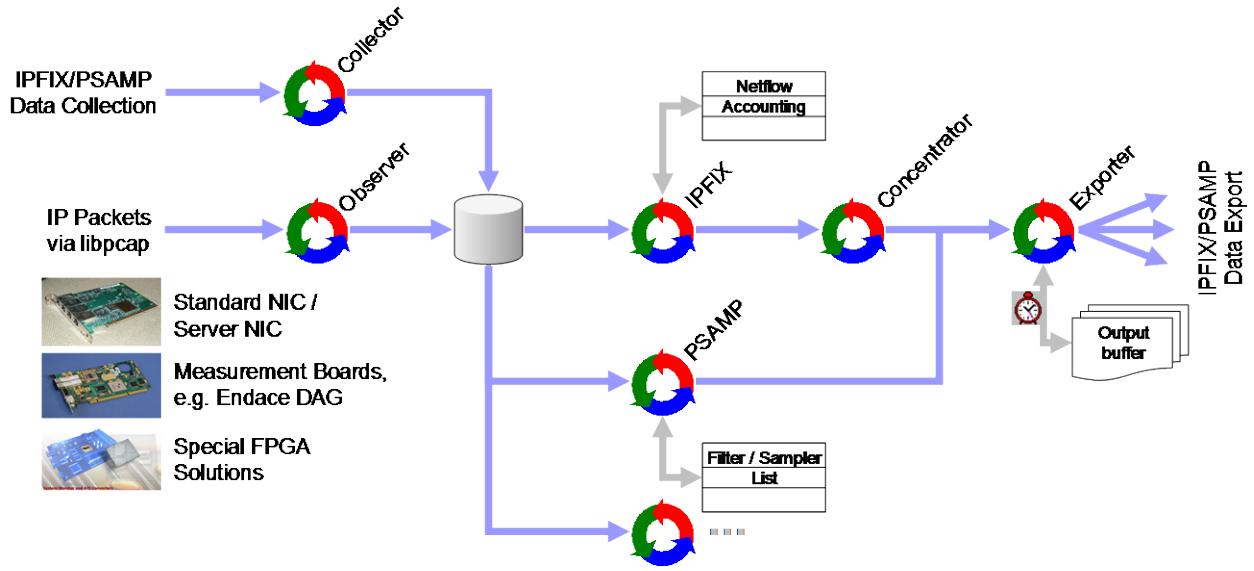

Figure 2. VERMONT monitoring probe

For the configuration of the monitoring probes, a path-oriented signaling protocol developed by the IETF NSIS working group, the metering NSLP [8] can be used.

A. *Monitoring*

We developed a monitoring toolkit, named VERMONT (VERsatile MONitoring Toolkit), for high-speed network monitoring. The main criteria in the development of VERMONT are:

- Standardized accounting (IPFIX/PSAMP)
- Policy-based data aggregation
- Data collection using libpcap (HW abstraction layer)
- Efficient, decoupled data processing
- Multiprocessor support
- High-performance based on optimized hash tables

The toolkit allows to employ different hardware modules for network access such as standard NICs up to special FPGA-based solutions. Internally, multiple threads work on the captured packets interconnected by various queues and buffers to cope with bursts of small packets. The captured data can be processed in two ways. First, netflow accounting can be accomplished. In this mode of operation, statistics of single IP flows are accumulated such as the total number of transmitted bytes and packets. Secondly, the PSAMP module can apply filters and sampling algorithms to select single packets that need to be forwarded for post-analysis. Such filters allow to look for packets of particular interest, e.g. for packet traceback, whereas the sampling algorithms reduce the number of packets of be processed and transmitted to a value depending on the capabilities of the overall system. Depending on the application, IPFIX/netflow accounting, packet sampling, or both can be employed. Finally, the concentrator functionality as described by IPFIX is embedded by including IPFIX a collector for data input and an aggregation module. The complete architecture of VERMONT is shown in Figure 2.

B. *Analysis*

The tool NASTY (Network Analysis and STatistics Yielding) was developed to collect and analyze monitoring data monitored received via Netflow, IPFIX, or PSAMP. The architecture is shown in Figure 3.

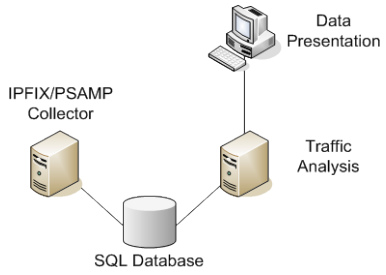

Figure 3. NASTY architecture

Using a SQL database, collected data are stored for further high-performance SQL-based data analysis. This DBMS-centric operation allows a fine-granular data selection, pre-analysis, and statistics. Based on a web-based architecture, the graphical traffic analysis of the network utilization becomes easy to achieve. The flexible architecture of NASTY allows to differentiate between end systems and applications. Additionally, data export to script-languages (PERL) is supported. An example of the traffic analysis is provided in Figure 4. Similar evaluations can be executed for all stored information.

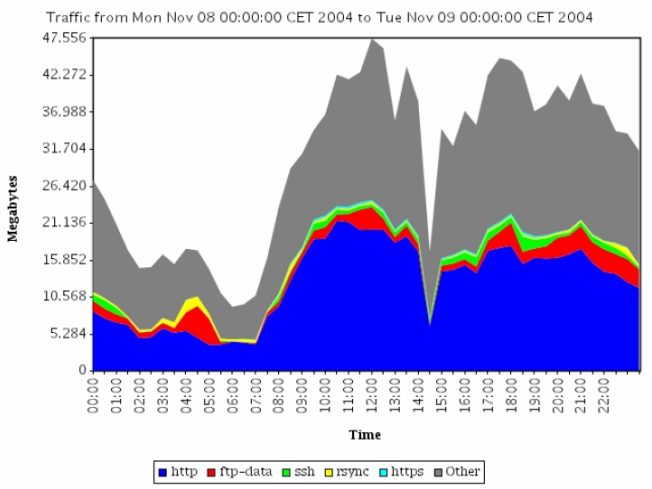

Figure 4. Sample analysis output

III. Applicability and Conclusions

The methodologies and tools developed in the context of HISTIORY are already in use in several projects and applications. For example, it shows its potential in application for network security mechanisms such as distributed intrusion detection [7] and a new kind of traceback mechanisms called probabilistic traceback. Additionally, the applicability to accounting mechanisms is shown in [10].

Other tools have been developed in the networking community to provide Netflow accounting, e.g. nProbe by Deri [5]. Nevertheless, such tools only concentrate on very limited issues of the demonstrated architecture. Due to the flexible approach and the standardized protocols, such tools can be employed in the HISTORY architecture as well. Additionally, VERMONT is the first available tool that supports packet sampling and flow aggregation as described by IPFIX.

In conclusion, it can be said that we developed a unique monitoring architecture which is extensible and flexible in terms of used modules and mechanisms. We implemented a high-speed monitoring probe capable of exporting IPFIX and PSAMP data. Additionally, the complete environment does not stop with the monitoring part. For real-time transport and analysis of the monitored information, we provide aggregation and transport mechanisms.

IV. Outlook and Further Work

The continuing research on the analysis of network traffic leads to distributed data storage and analysis. We address this objective by providing a standardized monitoring architecture and extend is to distributed data storage and suitable data storage and re-location mechanisms. The most challenging issues are the efficient data localization and transmission, anonymization, and access control. By working out a policy-based lookup language for accessing and modifying data we turn to distributed analysis with the following goals:

- Evaluation of traffic characteristics, short and long range dependencies
- Analysis of traffic flows for efficient traffic engineering
- Detection of traffic anomalies and forensic evaluations

References

[1] P. Calato, J. Meyer, and J. Quittek, "Information Model for IP Flow Information Export," draft-ietf-ipfix-info-03.txt, February 2004.

[2] B. Claise, "IPFIX Protocol Specification," Internet-Draft, draft-ietf-ipfix-protocol-07.txt, December 2004.

[3] B. Claise, "Cisco Systems NetFlow Services Export Version 9," RFC 3954, October 2004.

[4] B. Claise, "Packet Sampling (PSAMP) Protocol Specifications," draft-ietf-psamp-protocol-01.txt, February 2004.

[5] L. Deri, "Passively Monitoring Networks at Gigabit Speeds Using Commodity Hardware and Open Source Software," Proceedings of Passive and Active Measurement Workshop (PAM 2003), La Jolla, CA, USA, April 2003.

[6] T. Dietz, F. Dressler, G. Carle, and B. Claise, "Information Model for Packet Sampling Exports," Internet-Draft, draft-ietf-psamp-info-02.txt, July 2004.

[7] F. Dressler, G. Münz, and G. Carle, "Attack Detection using Cooperating Autonomous Detection Systems (CATS)," Proceedings of 1st IFIP TC6 WG6.6 International Workshop on Autonomic Communication (WAC 2004), Berlin, Germany, October 2004.

[8] F. Dressler, G. Carle, C. Fan, C. Kappler, and H. Tschofenig, "NSLP for Metering Configuration Signaling," Internet-Draft, draft-dressler-nsis-metering-nslp-00.txt, October 2004.

[9] F. Dressler, C. Sommer, and G. Münz, "IPFIX Aggregation," Internet-Draft, draft-dressler-ipfix-aggregation-00.txt, January 2005.

[10] U. Foell, C. Fan, G. Carle, F. Dressler, and M. Roshandel, "Service-Oriented Accounting and Charging for 3G and B3G Mobile Environments," Proceedings of 9th IFIP/IEEE International Symposium on Integrated Network Management (IM 2005), May 2005.

[11] G. Sadasivan, N. Brownlee, B. Claise, and J. Quittek, "Architecture for IP Flow Information Export," Internet-Draft, draft-ietf-ipfix-architecture-05.txt, January 2005.