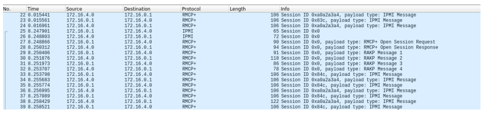
Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Thesis B.Sc.

IDP

Efficient Processing of Large Network Captures

Motivation



No.	Time	Source	Destination	Protocol	Length	Info
22	0.015441	172.16.4.0	172.16.0.1	RMCP+	106	Session ID 0xa0a2a3a4, payload type: IPMI Message
23	0.015561	172.16.0.1	172.16.4.0	RMCP+	106	Session ID 0x83c, payload type: IPMI Message
24	0.016961	172.16.4.0	172.16.0.1	RMCP+	106	Session ID 0xa0a2a3a4, payload type: IPMI Message
25	8.247901	172.16.0.1	172.16.4.0	IPMI	65	Session ID 0x0
26	8.248803	172.16.4.0	172.16.0.1	IPMI	72	Session ID 0x0
27	8.248866	172.16.0.1	172.16.4.0	RMCP+	90	Session ID 0x0, payload type: RMCP+ Open Session Request
28	8.250312	172.16.4.0	172.16.0.1	RMCP+	94	Session ID 0x0, payload type: RMCP+ Open Session Response
29	8.250406	172.16.0.1	172.16.4.0	RMCP+	91	Session ID 0x0, payload type: RAKP Message 1
30	8.251876	172.16.4.0	172.16.0.1	RMCP+	118	Session ID 0x0, payload type: RAKP Message 2
31	8.251973	172.16.0.1	172.16.4.0	RMCP+	86	Session ID 0x0, payload type: RAKP Message 3
32	8.253707	172.16.4.0	172.16.0.1	RMCP+	78	Session ID 0x0, payload type: RAKP Message 4
33	8.253798	172.16.0.1	172.16.4.0	RMCP+	106	Session ID 0x84c, payload type: IPMI Message
34	8.255683	172.16.4.0	172.16.0.1	RMCP+	106	Session ID 0xa0a2a3a4, payload type: IPMI Message
35	8.255774	172.16.0.1	172.16.4.0	RMCP+	106	Session ID 0x84c, payload type: IPMI Message
36	8.256995	172.16.4.0	172.16.0.1	RMCP+	106	Session ID 0xa0a2a3a4, payload type: IPMI Message
37	8.257089	172.16.0.1	172.16.4.0	RMCP+	106	Session ID 0x84c, payload type: IPMI Message
38	8.258429	172.16.4.0	172.16.0.1	RMCP+	122	Session ID 0xa0a2a3a4, payload type: IPMI Message
39	8.258521	172.16.0.1	172.16.4.0	RMCP+	106	Session ID 0x84c, payload type: IPMI Message

The uncountable numbers of devices in networks pose a new challenge for monitoring tools: they generate large amounts of network data. This data needs to be processed to generate meaningful insights into a monitored network. Standard methods for processing large amounts of network data take long and are therefore not sufficient. This fosters the need for highly efficient network data (pre-) processing mechanisms.

Topic

The goal of this thesis is to develop and implement a pipeline for efficiently parsing and processing network-data at large scale. Therefore, an analysis about existing parsing methods needs to be conducted with respect to their efficiency. Further, a common denominator in network data needs to be found such that data from different sources can be processed and stored in a standardized way. Finally, after processing data, it needs to be stored in an accessible way such that different applications can benefit from the preprocessing and further process the data.

Your Task

- Analysis of network data processing methods
- Comparison of existing approaches
- Implementation of an own data-parsing pipeline
- Comparison of the developed approach to naive methods.

Requirements

- Basic network knowledge
- Ability to write efficient and maintainable code
- Experience in Go is a plus

Sources

Contact

Lars Wüstrich wuestrich@net.in.tum.de
Johannes Zirngibl zirngibl@net.in.tum.de
Christian Lübben luebben@net.in.tum.de
http://go.tum.de/080755