COMPUTER NETWORK TRAFFIC ANALYSIS TECHNOLOGIES

Department of information and technical support TFOMS Sverdlovsk region
Aleksandr S. Suslov
Applied tasks of traffic analysis

- Information security event monitoring;
- Monitoring the state of information flows in the computer network;
- Network software debugging;
- Computer science education.
Traffic analysis workflow
Syslog protocol
Principle of SNMP Communication
NetFlow protocol
Network packet capture
Manual packet analysis

Wireshark screen showing a packet analysis with columns for Time, Source, Destination, Protocol, and Info.
Signature based analysis

String matching methods:
• Exhaustive Search;
• Decision Tree;
• Decomposition;
• Tuple Space.

RegExp matching:
• Nondeterministic finite automaton;
• Deterministic finite automaton.
Statistical analysis of network packets

• Online/Offline analysis;
• Parametric/nonparametric;
• One-dimensional/multidimensional analysis.
Machine learning methods

- Classification (supervised learning);
- Clustering (unsupervised learning);
- Association;
- Numerical prediction.
Conclusion

• Manual packet analysis with using a packet analyzer is the cheapest and most effective method of traffic analysis in computer science education.
References


5. Carlos Vega, Javier Aracil, Eduardo Magana: KISS methodologies for network management and anomaly detection. SOFTCOM 2018
http://dx.doi.org/10.23919/SOFTCOM.2018.8555785.

Thanks for your attention!