Technische Universität München, Department of Informatics

Chair for Network Architectures and Services

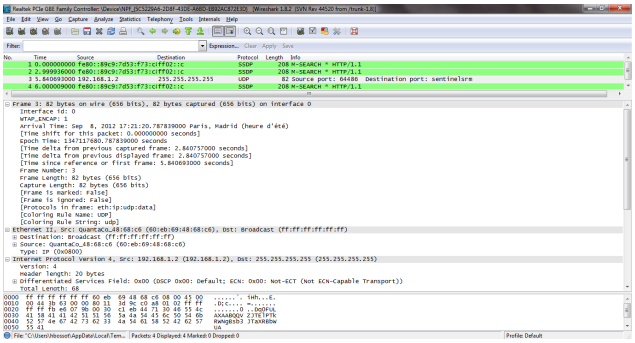
Prof. Dr.-Ing. Georg Carle

Thesis M.Sc.

IDP, Guided Research

Protocol inference of multi-session network protocols

Motivation



Understanding the protocol format and the sequence of messages of network protocols gives you the possibility to detect unwanted or malicious behaviour in your network. This protocol inference is possible when done on relatively simple and single-session protocols [1, 2, 3, 5] or when manual intervention is done [4]. However, automatic protocol inference with correlation of multiple different protocols (e.g. XMPP and DNS) is still an open challenge. In this thesis you will develop a technique to do protocol inference of multi-session protocols.

Your Task

- Research state of the art of protocol inference
- Develop a tool to do protocol inference on network traces
- Evaluate your tool with protocols such as WhatsApp

Bibliography

[1] Joao Antunes, Nuno Neves, and Paulo Verissimo. Reverx: Reverse engineering of protocols. 2011.

[2] Paolo Milani Comparetti, Gilbert Wondracek, Christopher Kruegel, and Engin Kirda. Prospex: Protocol specification extraction. In *Security and Privacy, 2009 30th IEEE Symposium on*, pages 110–125. IEEE, 2009.

[3] Weidong Cui, Jayanthkumar Kannan, and Helen J Wang. Discoverer: Automatic protocol reverse engineering from network traces. In *USENIX Security*, pages 199–212, 2007.

[4] Qun Huang, Patrick PC Lee, Caifeng He, Jianfeng Qian, and Cheng He. Fine-grained dissection of wechat in cellular networks.

[5] TUM I8. ProtoX GitHub. https://github.com/tumi8/Protocol-Informatics.

Contact

Oliver Gasser gasser@net.in.tum.de

http://go.tum.de/306574