Protocol inference of multi-session network protocols

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.

- 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


Contact

Oliver Gasser  gasser@net.in.tum.de

http://go.tum.de/306574