Control Protocols for Network Covert Channels

Steffen Wendzel
FernUniversität in Hagen
D-58097 Hagen
SteffenWendzel{at}web.de

Covert channels are security policy breaking communication techniques based on channels which were not designed for a communication. Applied to today's computer networks, covert channels provide a means to i) exfiltrate confidential information of organizations, ii) to control botnets, as well as they iii) enable the unrestricted communication of political parties and journalists in monitored networks, just to mention the most important use-cases.

Within the last years, first ideas for the improvement of network covert channels arose, such as autonomous covert channels, self-adapting covert channels and covert channels with internal control protocols (so called *micro protocols*).

This work presents protocol engineering techniques which help to optimize the micro protocol design in a way that the covert channel raises as little attention as possible.

We demonstrate that covert channel overlays can utilize multiple network protocols to enable mobile covert channel usage, as well as we optimize the forwarding of data within the overlay network [1]. In our work, mobile covert channel overlays enable the usage of multiple access devices (e.g. smart phones), protocols and access points, as well as backward-compatible micro protocols.

We present a new approach by applying context-free and regular grammar to verify the conformance of micro protocols to the utilized network protocol (e.g. a covert channel's micro protocol should not break the standard-conform behavior of ICMPv6 if it is embedded within the protocol) [2]. We ensure such standard-conform micro protocols by verifying the inclusion of the micro protocol's language within the language of the utilized protocol.

Furthermore, we demonstrate calculations as well as an implementation for a first *active warden* able to decrease the bandwidth of protocol switching covert channels [3]. Our active warden introduces delays using a Linux netfilter extension to counter the covert channel performance. An important goal of the project is to prevent mentionable effects on the performance of normal (i.e. non-covert) network traffic.

References

[1] Steffen Wendzel and Jörg Keller: *Low-attention forwarding for mobile network covert channels*, in Proc. 12th Conference on Communications and Multimedia Security (CMS 2011), Ghent, Belgium, LNCS vol. 7025, pp. 122-133, Springer, 2011.

[2] Steffen Wendzel and Jörg Keller: *Systematic Engineering of Control Protocols for Covert Channels*, in Proc. 13th Conference on Communications and Multimedia Security (CMS 2012), Kent, 2012 (accepted).

[3] Steffen Wendzel and Jörg Keller: *Design and Implementation of an Active Warden Addressing Protocol Switching Covert Channels*, in Proc. 7th International Conference on Internet Monitoring and Protection (ICIMP 2012), Stuttgart, 2012 (accepted).