Technische Universität München, Department of Informatics

Chair for Network Architectures and Services

Prof. Dr.-Ing. Georg Carle

Thesis B.Sc.

Thesis M.Sc.

Privacy Box – Web filtering

tl;dr: Build a better OnionPi

Motivation

Our aim is to enable the average internet user (with regard to common services like the WWW, e-Mails, VoIP, file sharing...) to protect her privacy without having to rely on third party services which require payment as well as some amount of trust. We use a grass root approach where every user uses a *Privacy Box* which copes with all anonymization and traffic securing while the actual client device (computer, smart phone) does not need more setup than a VPN-connection.

Problem

The web is cluttered with third party services for advertising as well as user tracking. Other websites are indirectly affiliated with providers of unwanted (adult/illegal/malicious) content. Although loading those contents without intention, providers are nevertheless able to track one's access and create cookies.
Browser addons do exist but when using multiple devices they have to be installed every time, each browser has different addons (some have none) and embedded devices are severly constrained with regard to those enhancements.

Your Task

We already have a concept which allows tunneling all client traffic over a middle box – the Privacy Box – as well as basic manipulation of incoming and outgoing traffic. Based on that existing infrastructure your task is to realize a module which allows the

- analysis which domains are accessed
- configuration of blacklists for domains solely providing tracking or advertising
- blacklisting of such domains
- manipulation of cookies (reduction of expiration dates)

At first glance it is obvious, that TLS prevents deep inspection of the accessed content. Here, you may investigate, which methods of filtering are nevertheless possible.

Contact

Dr. Holger Kinkelin	kinkelin@net.in.tum.de
Marcel von Maltitz, M. Sc.	vonmaltitz@net.in.tum.de