Technische Universität München
Chair for Network Architectures and Services
Prof. Dr.-Ing. Georg Carle

BA/MA

Secure and Private P2P Telephony Services based on a web-of-trust

Introduction

At the latest since the publication of international intelligence activities by whistle-blower Edward Snowden the world knows that even the average Joe is in the focus and monitored online.

Problem

A particular focus of online monitoring is Voice over IP (VoIP). Besides recording audio and video also vast amounts of meta-data is collected. Meta-data gives evidence who called whom, how long, at which point in time and maybe even from which location when IP-addresses or cell tower locations are considered as well.

Task Description

Central authorities have lost their trustworthiness in the sequence of the above-mentioned events. In previous work, we have developed mechanisms for a user-centric web-of-trust that users build via interactions of their devices and their homes. In addition, we have developed a DNS-like mechanism to find devices using the naming of the web-of-trust. On this basis, we want you to set-up a secure voice communication channel. This could be by coupling our web-of-trust certificates with TLS / DTLS and sending voice traffic on top of it. Furthermore, the secure communication channel needs to be able to send maintenance and management packets to be able to add privacy-enhancing technologies like re-routing to the solution. Re-routing (like in Tor) is e.g. used to hide the actual location of the sender from observer and receiver. It is also necessary to be able to differentiate between dummy voice traffic and real traffic, another measure to increase privacy. The goal of this thesis is to provide the secure communication and a simple re-routing mechanism. It provides the basic architecture for adding privacy-enhancing mechanisms that are work of subsequent theses.

Requirements

You should have basic skills in Java, some basic knowledge about P2P-systems as well as VoIP. Furthermore we expect you to cooperate with other students and members of the chair working on problems related to this thesis.

Further Information: Dr. Holger Kinkelin, Dr. Heiko Niedermayer und Marcel von Maltitz
(lastname@net.in.tum.de)
Chair for Network Architectures and Services