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

BA/MA

Mix based Anonymity in Telephony Services

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

```
GDLBvOiQJQwbPHlVpFtkpAnItqqUrvvTDZi
gUmNxOvOyCNPcSYnyXlwaXfNfuVpFtkpAnI
CjzCibEFPapvHello_JoeAwYnyfXlFsmguq
oNovMjKvKMcNwCRzWSOEzqBCzvSuNBkdiRP
GDLBvOkbye_SarahiXmdjAnItqqUrvvTDZi
zbePNovMjKvKMcNwCRzWSOEzqBCzvSuNBck
AAPybsCZxWyrKYbDwe will meet at 8KJ
```

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

The overall goal is to explore security and privacy aware telephony services and to create a working prototype. This thesis shall contribute a concept of hiding VoIP traffic between nodes in a network. A first attempt could be a TOR-like approach of *mix based anonymity*. However, different approaches are possible: For instance, a distributed anonymization network could be created following the Peer-to-Peer principle. Each node in this network dedicates some of its bandwidth to the anonymization service. A traffic generator creates artificial, encrypted VoIP traffic, which is then sent to randomly chosen other peers. From the outside, this artificial VoIP traffic may not be distinguishable from real VoIP traffic. Hence, the selection of used protocols and even voice codecs is of paramount importance. Furthermore, the call and conversational patterns like call length and alternate speaking and listening caused by the traffic generator should look "natural". Real VoIP traffic can now be mixed into the artificial traffic. For the outside observer it is not feasible to distinguish real from fake calls and hence it is not possible to collect meta-data. The goal of this thesis is to investigate the issue of artificial traffic generation and to build and evaluate such a tool. The organization of the Peer-to-Peer network or the setup of trusted connections is not within the scope of this work but investigated in partner 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.