Unwanted Traffic and Information Disclosure in VoIP Networks

Ge Zhang

The success of the Internet has brought significant changes to the telecommunication industry. One of the remarkable outcomes of this evolution is Voice over IP (VoIP), which enables realtime voice communications over packet switched networks for a lower cost than traditional public switched telephone networks (PSTN). Nevertheless, security and privacy vulnerabilities pose a significant challenge to hindering VoIP from being widely deployed. The main object of this thesis is to define and elaborate unexplored security & privacy risks on standardized VoIP protocols and their implementations as well as to develop suitable countermeasures. Three research questions are addressed to achieve this objective:

Question 1: What are potential unexplored threats in a SIP VoIP network with regard to availability, confidentiality and privacy by means of unwanted traffic and information disclosure?

Question 2: How far are existing security and privacy mechanisms sufficient to counteract these threats and what are their shortcomings?

Question 3: How can new countermeasures be designed for minimizing or preventing the consequences caused by these threats efficiently in practice?

Part I of the thesis concentrates on the threats caused by ``unwanted traffic", which includes Denial of Service (DoS) attacks and voice spam. They generate unwanted traffic to consume the resources and annoy users. Part II of this thesis explores unauthorized information disclosure in VoIP traffic. Confidential user data such as calling records, identity information, PIN code and data revealing a user's social networks might be disclosed or partially disclosed from VoIP traffic. We studied both threats and countermeasures by conducting experiments or using theoretical assessment. Part II also presents a survey research related to threats and countermeasures for anonymous VoIP communication.