Contact:
Fraunhofer-Institute
Secure Information Technology
Rheinstraße 75
64295 Darmstadt

Dr. Andreas U. Schmidt
Andreas.U.Schmidt@sit.fraunhofer.de
Tel. 06151 – 869 60 227

Nicolai Kuntze
Nicolai.Kuntze@sit.fraunhofer.de
Tel. 06151 – 869 60 054

TECHNISCHE UNIVERSITÄT DARMSTADT

Prof. Dr. Claudia Eckert
Fachbereich Informatik
FG Sicherheit in der Informationstechnik
Hochschulstr. 10
64289 Darmstadt
Telefon +49 (0) 61 51/16-6591
Telefax +49 (0) 61 51/16-3514

Fraunhofer Institut
Sichere Informationstechnologie SIT
Institutsleitung
Prof. Dr. Claudia Eckert

Rheinstraße 75
64295 Darmstadt

E-Mail: eckert@sit.fraunhofer.de
http://www.sit.fraunhofer.de

Diploma Thesis

SUBJECT: SPAM over Internet Telephony and how to deal with it

Background and Goal: Spam is a well-know problem and it is estimated that at least 60% of the e-mail traffic consists of Spam. With the upcoming Voice over Internet (VoIP) standards and their usage, a new variant of Spam may emerge. The so called Spam over Internet Telephony (SPIT) consists in mostly automated messages (e.g. advertisement) to users of VoIP services. From the end-users' point of view, it saturates the voice box with useless messages when the user is not available and increases call load if he is by his phone. From the VoIP providers' point of view, it overloads the servers.
Today, SPIT is not a hot topic for the network operators, since it is very limited. Yet, in view of the drastic increase in VoIP usage, the threat from SPIT may soon become imminent. Some research has been done in the area of SPIT prevention, mostly focused on methods to detect and suppress SPIT, and to ban nodes from which SPIT emanates.
Aim of this diploma thesis is to critically evaluate these SPIT countermeasures and to present if possible ways to circumvent them. Furthermore it is to be evaluated if Trusted Computing based approaches can be helpful in this area by providing e.g. a reliable user, or device, authentication and integrity measurements for the devices used. In particular a software shall be implemented which

- Generates (maybe even synthesises) SPIT and introduces it into common VoIP networks by pretending to be a node or a device
- Camouflages as various device or communication node types (device signatures, and in particular protocol implementation variants)
- Emulates different kinds of communication behaviour (e.g. ringing, call frequencies and duration, etc.)
- If possible, dynamically adapts to SPIT countermeasures

Prerequisites: Good knowledge of SIP and RTP. Knowledge in cryptography. Fluent in Java and knowledge of contemporary Web-application technology. May have heard of trusted computing. English writing skills.

Start: Immediately