Contact:
Fraunhofer-Institute SIT, 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

ARTEC Computer GmbH, Karben

Jerry J. Artishdad
J.Artishdad@artec-it.de
Tel. 06039 – 9154-7511

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/Master Thesis

SUBJECT: Non-Repudiation for Voice over IP Archiving

Background and Goal: With VoIP maturing, it becomes natural to ask for application-level security in the context of IP telephony. Our aim here is to achieve non-repudiation in the context of IP telephony i.e., for speech over packet-oriented, digital channels, and in particular for VoIP conversations. This means the capability to produce tenable evidence that a conversation with the alleged contents has taken place between two or more parties. Ancillary information, e.g., that the conversation partners have designated, personal identities, and the time at which the conversation has taken place, may be of utmost importance in this regard, either to establish a supporting plausibility, e.g., `caller was not absent during the alleged call', or as relevant semantic information, e.g., `telephonic order came in before stock price rose'. For electronic documents this kind of non-repudiation is commonly achieved by applying electronic signatures based on asymmetric cryptography.

Based on the existing diploma thesis “Security and Non-Repudiation for Voice-over-IP conversations” by C. Hett[1] and VoIP Signature concepts presented there the aim of the present, follow-up thesis, which is offered in cooperation with ARTEC Computer GmbH, is

- to develop a concept for a secure archive for VoIP communication.
- Considering aspects of long term archiving as used e.g. in Archisoft[2]
- to implement a demonstrator based on Open Source projects like Asterisk or OpenSER and considering the special abilities and functionalities of these software systems especially with respect to media conversion.
- the development of appropriate data formats for data storage so that the recordings can be handled equal to documents afterwards by already existing DMS.

The thesis work can be performed at the site of ARTEC and is fully supported technically and by their staff.

[1] http://www.sec.informatik.tu-darmstadt.de/pages/dipl/docs/finished/hett_diplom.pdf and http://arxiv.org/abs/cs.CR/0701145
[2] http://www.sit.fraunhofer.de/projekteundthemen/archisoft.jsp

Prerequisites: Knowledge of SIP and RTP. Knowledge in cryptography and security methods like digital signatures. Knowledge in the Open Source Projects Asterisk and/or OpenSER from a conceptual perspective as well as practical experience. Good programming skills in C++/Java and English writing skills are also required.

Start: Immediately