



Gesellschaft



SPIDER: Spam over Internet Telephony Detection Service

Partners:

- Fraunhofer (FOKUS) (Germany)
- University of the Aegean (Greece)
 - AUEB (Greece)
- Voztelecom (Spain)
- Telio (Norway)
- Iptego (Germany)

Scientific Director:

Dimitris Gritzalis
 Dept. of Informatics
 Athens Univ. of Economics & Business
 e-mail: dgrit@aubg.gr
 URL: www.cis.aueb.gr

Technical Director:

Ioannis Marias (AUEB)

Researchers and Consultants:

Michael Avgoustianakis (U. of Athens)
 Panos Constantopoulos (AUEB)
 Stelios Dritsas (AUEB)
 Sokratis Katsikas (U. of Peireus)
 Ioannis Mallios (AUEB)
 Lilian Mitrou (UoA)
 Tassos Ntagioulas (UoA)
 Yiannis Soupionis (AUEB)
 Marianthi Theoharidou (AUEB)
 George Tountas (U. of Peireus)

Project identity:

IST-032720-SPIDER

Source of funding:

European Commission
 IST Programme (Co-OP)

Duration:

October 2006 - September 2008

Budget (funding):

1.700.000 €

Project motivation, scope and objectives

In contrast to traditional PSTN technologies, IP-Telephony is based on the concept of separation between the signalling and media infrastructure. Thus, small and medium enterprises can provide public VoIP services without providing network services, with only a low level of investments. Actually, a VoIP service could be launched using an open-source and commercial software, providing support for the signalling, billing and accounting and database, web portal and a networked computer that could be hosted at a public hosting service. With such a low end infrastructure, a provider can support low-cost VoIP communication.

Due to the similarity of the IP-Telephony infrastructure to other Internet services such as web and Email, IP-Telephony components might suffer from the same threats. However, the knowledge and expertise needed for securing such an infrastructure against misuse is still missing.

Similar to mail and fax services it is possible to generate spam calls causing annoyance at the user level. Spam calls would not only be inconvenient to the subscribers but also tarnish the reputation of the provider. Actually with a reputation of being insecure and open to misuse, the VoIP technology would suffer dramatic economic consequences.

SPIDER aims at securing VoIP infrastructures, in terms of spam protection. It concentrates on increasing the work experience in VoIP infrastructure from a user's point of view, by limiting the possibility for unsolicited messages to reach the user.

Its objectives include the design and implementation of a framework for secure VoIP calls, in order to avoid misuse of VoIP for spam delivery, specification and development of tools for spam detection and suppression, support of different means for detection based on user and provider specific needs, and integration and testing of developed tools and solutions in a provider's VoIP infrastructure.

*“Enabling communication over IP,
 while respecting citizens' privacy and convenience”*