Activity Report (Full Project Duration)
SPIDER
01.10.06-30.09.08

SPIDER Management

Project and technical Coordinator: Sven Ehlert, Fraunhofer Fokus, Tel.: +49 30 34 63 7378
Administrative Coordinator: Stephan Kollmer, Fraunhofer ZV, Tel.: +49 2241 14-2082

Table of Content

WP1: Project Management....2
WP2: Spam security Architecture Requirements and Specification....4
WP3: System Implementation and Prototyping....6
WP4: Integration Evaluation and Trials....8
WP5: Project Dissemination....9
WP6: Legal and Ethical Issues....12

WP1: Project Management

The scope of WP1 covers overall project management activities, including regular reporting and arrangement for review meetings.

The partner's location is spread all over Europe. Hence, for project workflow we have set up a supportive infrastructure:

- A collaborative Workflow server. BSCW (http://bscw.fokus.fraunhofer.de) allows distributed document editing and sharing, Task definitions, Team cooperation and Agenda handling.
- For the implementation phase a shared Code Revision Control System (via CVS) was setup, allowing all partners to collaborate concurrently on the program code developed in SPIDER
- Two project mailing lists. This list allows fast and easy consortium communication. One mailing list is for general project discussion, while the other is for SME-only related discussion.
- A web server (www.projectspider.org). Here, our public progress is visible to the public.

For project communication and procedure guidelines, a Project Handbook (D1.1) and Project Management Guidelines (D1.2) have been published. Especially D1.2 contains a list of related management documents as well as a description of the management structure and templates used for reporting.

Project management included the regulation for Nextsoft's whish to exit the consortium and to assess the possibilities to continue with the project. This included the search for a potential substitute, the negotiation of the terms and conditions with the substitute and the consortium partners and the quick integration of the new partner IPTEGO into the consortium

The following meetings and Audio Conferences took place during the project

- Berlin 9.10.06
  - This was the kick-off meeting of the SPIDER project. The goal was for the partners to meet personally, explain general project procedures, like management issues, and to define the actual task to be performed for every partner
- Audio Conference 31.10.06
  - Discussion of how the spit threat analysis can be handled. The deliverable D2.1 status was also discussed
- Audio Conference 19.12.06
  - Discussion of the spit state of the art techniques. The different sections of the deliverable D2.2 were also discussed
- Barcelona 15-16.03.07

  - The Barcelona meeting was issued to summarize project findings and ideas for WP2, and to define their presentation for D2.1
- Several smaller Audio Conferences in 04.06
  - Due to the exit of Nextsoft from the SPIDER consortium, several small conferences have been setup to discuss, regulate and approve of the entrance of iptego into the consortium as a substitute
- Oslo, 5.-6.7.2007
  - The scope of the Oslo meeting was to finalize the requirements of the SPIDER architecture and to summarize and present the applicability of various available tools on the market in the SPIDER architecture. Also, first implementation feedback was given. Results have been presented in D2.3
- Audio Conference 13.9.06
  - Discussion of the status of the deliverable D3.1.
- Athens, November 12/13
  - Discussion of the proposed anti-spit architecture, identifying the corresponding weaknesses, the status of the development phase, possibilities of disseminating SPIDER, IPRs.
- AC, January, 23
  - Update about the SPIDER architecture, task definitions for D3.2
- Berlin, February 28/29
  - Finalization of the SPIDER architecture, development + test updates, preparation of D3.2, Planning of integration meeting, preparation about VON/CeBit dissemination (n.b. VON was later cancelled)
- Barcelona, May 7-9
  - Developer meeting to finalize individual modules and integrate all modules into one coherent solution, definition of real-life test setups, planning for D4.1, IPR and dissemination updates
- AC, August 29
  - Finalization of IPR and Business plans, tasks for D4.2, D5.2 & D6.2

- Most project related tasks have been coordinated using personal email/phone calls and the SPIDER mailing lists. All project partners' main focus lies on electronic communication, so email is the predominant and obvious communication method for all partners. Thus, email communication was the most effective management method for this project.

WP2: Spam security Architecture Requirements and Specification

This workpackage is to specify and analyse the requirements of VoIP infrastructures in terms of regulatory and operational point of view for Spam protection. Initially, data will be collected and analysed, then, it will be used for identifying spam placement possibilities and the ways to handle them. The work achieved within this workpackage was split into the following tasks,

- Investigation of Spam pattern, usage, motivation and evolution in email communication (⇒ D2.1).
- Definition of Spam in the VoIP world, in the context of appearance and occurrence (⇒ D2.1).
- Description of current VoIP spam occurrences and how this will likely increase in the future (⇒ D2.1).
- We have assessed in detail the vulnerabilities that allow VoIP Spam to occur in the first place. These include vulnerabilities due to VoIP protocol weaknesses, due to optional protocol recommendations, due interoperability with related protocols and security vulnerabilities (⇒ D2.1).
- We have assessed a “common profile” for VoIP spammers, their likely motivation, potential revenue gained from spamming and used spamming infrastructure. This is based on e-mail Spam evaluation with predictions for the VoIP world (⇒ D2.1).
- We have evaluated VoIP Spam requirement that need to be met by potential spammers including a likely set of usable tools (⇒ D2.1).
- Based on the previous assessment we have developed a Spam thread analysis, which predicts the likelihood of VoIP Spam occurring, the potential difficulty to prevent theses cases, and the impact such VoIP Spam will have on the VoIP technology (⇒ D2.1, D2.3).
- We have assessed the current situation of Spam possibilities in e-mail communication. This includes the gathering of spam targets, current applicable e-mail anti-spam solutions and an evaluation of their advantages and disadvantages (⇒ D2.2).
- Listing of available anti-spit proposals (State of the Art). As VoIP Spam prevention is a new topic in the telecommunication market, most VoIP anti-Spam solutions proposals exist only as basic drafts in current research publications. We have gathered all the proposed ideas and assessed their value for the work within the SPIDER project together with the definition of qualitative and quantitative evaluation criteria. This is accumulated in a theoretical evaluation of the solutions with a categorization, advantages and disadvantages (⇒ D2.2).
- Based on the previous VoIP threat analysis, the “spamming profile”, and e-mail target gathering and tools we have outlines possibilities to achieve the same spam effect in the VoIP network, including the identification of potential VoIP Spam targets and, automatization of VoIP Spam delivery, and possibilities for the actual spammer to remain anonymous. With the explanation how SIP VoIP messages are transported within a network, we give a full possible VoIP spamming example (⇒ D2.1).

- To better place our work in the security sector, we have defined the placement of Spam prevention in relevance to other protection mechanisms, e.g. Denial-of-Service prevention (⇒ D2.3).
- We have identified the reasons behind the persistence of email spam and the potential reasons behind the emergence of SPIT. Based on the corresponding results, some requirements have been defined in order to build on top of them the SPIDER architecture (=> D2.3)
- We have defined a multi-layered anti-spit prevention architecture, which detects spit trough the help of different modules. Each module follows a different approach in the area of spam detection, so that a combined deployment will yield a higher detection ad prevention rate. We extensively describe possible modules that could be deployed in such a spit –prevention framework. We demonstrate the applicability of the security framework with different use cases. This way we show how the designed solution can be individually configured for the participating SME's needs (⇒ D2.3).

.

WP3: System Implementation and Prototyping

This workpackage includes the activities for system implementation. System specifications and requirements that are defined in WP2 and WP3 will be the input for the implementation of the solution proposed in SPIDER.

Based on the theoretical analysis performed in WP2, we have defined a VoIP anti-spam framework tat is being implemented in the SPIDER project.

- Based on the possible architectural components, we have agreed on a defined set. This consists of proven working components, which the partners know and trust from their professional experience (⇒ D3.1).
- The basic security framework has been completely specified. This includes a SIP VoIP monitoring and processing solution with defined APIs to delegate the processing sequentially (or in parallel) detection modules. A common way to reach a verdict about each message if it is Spam or not has been defined (⇒ D3.1).
- Implementation has been started by the partners for several prevention modules. This phase will continue onwards into the second term of the project (⇒ D3.1).
- The following detection modules and the way they could be implemented were described in details in D3.1
    - Enhanced identity management module
    - Challenge / Response technique
    - Reputation-based technique
    - Audio-Analysis based Solution
    - Black- / White listing Solution
    - Machine-learning based solution.
- The architecture has evolved during the project, and some modules have been redefined (⇒ D3.2):
    - The machine-learning based solution was exchanged for a passive-monitoring solution. The passive-monitoring solution is based on Palladion from IPTEGO. IPTEGO replaced NextSoft in the second period of the project.
    - An additional proxy check module was added.
    - A decision point was added to control the components of the SPIDER architecture
- The SPIDER authentication module was designed, implemented and made available as a prototype. The module is capable of handling different encryption schemes and is divided in an authentication provider and an authentication verifier (⇒ D3.2).
- The SPIDER proxy check module was designed, implemented and made available as a prototype. It checks all incoming requests to the server (⇒ D3.2).
- The SPIDER white-/blacklist module was designed, implemented and made available as a prototype. It consists of a backend to be deployed at the server and a user interface implemented exemplarily at a Softphone (⇒ D3.2).
- The SPIDER challenge/response (Captcha) module was designed, implemented and made available as a prototype. It uses a separate audio server to generate customizable audio captchas (⇒ D3.2).

- The SPIDER audio analysis module was designed, implemented and made available as a prototype. It was designed for two use cases: Offline analysis of the contents of an answering machine or online analysis during a call. It uses a dedicated media server for handling the additional media processing (⇒ D3.2).
- The SPIDER reputation manager was designed, implemented and made available as a prototype. It runs at the SIP proxy to calculate user repudiation (⇒ D3.2).
- Palladion was made available as the passive-monitoring solution, and made available for SPIDER testing (⇒ D3.2).
- Interfaces between different SPIDER components have been designed and implemented (⇒ D3.2)
- The SPIDER decision point module was designed, implemented and made available as a prototype. This module controls all other SPIDER modules and decides about SPIT ratings (⇒ D3.2).
- An evaluation framework was defined for all SPIDER modules. This framework defines test cases for the modules and defines the expected behavior of the modules under test (⇒ D3.2).

Multiple use cases of the SPIDER architecture have been defined. The architecture is very flexible in the way it can be set up at a provider, and not necessarily all components are needed all the time. We outline different setups for the SPIDER architecture (⇒ D3.2).

WP4: Integration Evaluation and Trials

In WP4 the integration and testing of the implemented system was conducted. This included the evaluation of the technical correctness of the system as well as its usability and advantages as judged by the involved SMEs.

In the first half of the project, only the requirements for the tests have been defined. The final testing has been performed in the second half of the project.

- Setup at individual testbeds for local testing (⇒ D4.1)
  - The partners have defined their requirements for testbeds and their distribution on the partner's locations
  - A local testbed was setup for the authentication module and the reputation module at Fraunhofer FOKUS
  - A local testbed was setup for the Captcha tests at Athens University of Business and Commerce
  - A local testbed was setup for the Palladion test and the Black-White List module at IPTEGO.
  - A local testbed was setup for the Audio Analyzer at Eleven.
  - A local testbed was setup for the Proxy Check module and the decision manager at Telio.
- All modules have been thoroughly tested in local setups (⇒ D4.1)
  - Test cases have been defined.
  - Modules have been verified using these test cases.
- An integration testbed has been setup at Voztelecom, and integration tests have been performed (⇒ D4.1).
  - With the integration testing it was ensured that all modules can cooperate and work in the same setup.
  - A test scenario had been defined and the setup was verified with this scenario.
- Real life tests have been conducted at the provider networks (⇒ D4.1)
  - VozTelecom have setup a SPAN access to their network for testing
    - Modules under test here: Palladion, the Audio Analyzer
  - Telio have created a complete new Alpha network for customers that are interested in new technology

Modules implemented here for direct usage by Telio customers: Proxy Check, Authentication module, Captcha

WP5: Project Dissemination

WP5 provides venues for dissemination of the work as well as identify further exploitation plans. Demonstration activities as well as public presentation of the project results are also to be dealt within the WP.

For WP5, we have dealt with the following topics:

- Finalised of a final IPR agreement
  The partner's have agreed on final IPR agreement. It was introduce in D5.1 will be finalized in D5.2

- Finalising of usage scenarios for SME partners
  Usage plan for every partner has been established It was introduce in D5.1 will be finalized in D5.2

- A final public project report (D4.2) has been issued.

- Following fair events have been conducted to promote SPIDER
  - VON Europe 2008: The main dissemination event for SPIDER was supposed to be VON 2008 in Amsterdam, the major VoIP event in Europe. A booth was ordered and presentation material was developed for the event. However, VON 2008 was cancelled at the last moment by the organizers.
  - CeBIT 2008. SPIDER was presented at CeBIT 2008 in Hannover, at the Fraunhofer booth.

- Following industry talks have been given in regard to SPIDER
  - Alex Hoffman, Fending of VoIP attacks, talk at the International SIP 2008 conference, Paris, Jan 2008
  - R. Rothe, Strategies for a successful Spam Defense, talk at IT Security 2008, Munich, Apr 2008
  - E. Cramer, Spam metrics, Talks at the 14th General Meeting of the Messaging Anti-Abuse Working Group (MAAWG), Fort Laderdale, USA, Apr 2008
  - Alan Duric, "Europe Leads the Way", talk at the VON 2007 event. Boston, USA, Nov 2007
  - Alan Duric, "To What Extent Can Operators Become Service and Content Supermarkets?", talk at the IMS 2.0 event, Amsterdam, Netherlands, Sept 2008
  - Gritzalis D., "SPIT phenomenon: A raising threat", *14th Informatics Applications Conference* and *INFOSYSTEM 2008 International Fair*, Thessaloniki, October 2008.
  - 2. Gritzalis D., Theoharidou M., Soupionis I., "VoIP SPAM (SPIT): Trends and Perspectives", *2nd AIT Annual Workshop on Security* (PRACSE 2007), Athens, November 2007.

- 3. Marias G., "SPAM over Internet Telephony: A new threat", *9th Greek ICT Forum*, Athens, October 2007.
- J. Rodriguez, SIP y VozIP con FreeBSD, talk at the BSDcon 08, Barcelona, Spain, April 2008 (Same talk also at Simo07)
- J. Rodriguez, Asterisk, proxies SIP, servidores de aplicaciones... ¿A qué se. puede jugar?, talk at the Voip2Day, Madrid, Spain, Nov 2008

- Following papers were published,
  - Y. Rebahi et Al, "SIP Service Providers and the Spam Problem" in the Voice over IP Secuity Workshop Proceedings, June 2005, Washington, USA
  - Y. Rebahi et Al, " SIP Spam Detection", In the Proc of IEEE International Conference on Digital Communications, August 29-31, 2006, Cap Esterel , France
  - Y. Rebahi et Al, "A conceptual Architecture for SPIT Mitigation", Book Chapter to appear in the "SIP Handbook: Services, Technologies, and Security", to be published by CRC press in 2008
  - S. Dritsas et Al, "Threat analysis of the Session Initiation Protocol, regarding spam", in Proc. of the 3rd IEEE International Workshop on Information Assurance (in conjunction with the 26th IEEE International Performance Computing and Communications Conference (IPCCC-2007), pp. 426-433, IEEE Press, New Orleans, April 2007.
  - J. Marias et Al, "SIP vulnerabilities and antispit mechanisms assessment", in Proc. of the 16th IEEE International Conference on Computer Communications and Networks (ICCCN '07), August 2007, Hawaii.
  - Mallios J., Dritsas S., Tsoumas B., Gritzalis D., "Attack modeling of SIP-oriented SPIT", in Proc. of the 2nd IEEE-IFIP International Workshop on Critical Information Infrastructures Security (CRITIS '07), Spain, October 2007.
  - Y. Rebahi, S. Ehlert, A. Bergmann, A SPIT Detection Mechanism Based on Audio Analysis, 4th International Mobile Multimedia Communications Conference, Jul 2008, Oulu, Finland
  - Y. Rebahi, S. Ehlert, et Al, "Performance Analysis of the Identity Management in the SIP Protocol", in the Proc of the IEEE AICCSA 2008, March 31 - April 4, 2008, Doha, Qatar
  - S. Ehlert, G. Zhang, and T. Magedanz: "Increasing SIP Firewall Performance by Ruleset Size Limitation", IEEE PIMRC 2008 - VoIP Technologies Workshop, Cannes, France, September 2008
  - Y. Rebahi, et Al, "A Conceptual Architecture for SPIT Mitigation", In the Proc of the Manweek conference 2008, Sep 22- 26, Samos, Greece.
  - Dritsas S., Dritsou V., Tsoumas B., Constantopoulos P., Gritzalis D., "OntoSPIT: SPIT management through Ontologies", *Computer Communications*, Elsevier, 2008 (to appear)
  - Dritsas S., Soupionis J., Theoharidou M., Mallios J., Gritzalis D., "SPIT Identification Criteria Implementations: Effectiveness and Lessons Learned", in *Proc. of the 23rd International Information Security Conference* (SEC-2008), Samarati P., et al. (Eds.), pp. 381-195, Springer, Milan, September 2008.
  - Gritzalis D., Mallios Y., "A SIP-based SPIT management framework", *Computers & Security*, Vol. 27, Nos. 5-6, pp. 136-153, Elsevier, October 2008.

- Mallios J., Dritsas S., Tsoumas B., Gritzalis D., "Attack modelling of SIP-oriented SPIT", in *Proc. of the 2nd IEEE-IFIP International Workshop on Critical Information Infrastructures Security* (CRITIS '07), Lopez J., B. Haemmerli (Eds.), pp. 299-310, LNCS 5141, Springer, Spain, May 2008.
- Soupionis Y., Dritsas S., Gritzalis D., "An adaptive policy-based approach to SPIT management", in *Proc. of the 13th European Symposium on Research in Computer Security* (ESORICS 2008), pp. 446-460, Lopez J., Jajodia S. (Eds.), Springer, Malaga, October 2008
- Marias G., Theoharidou M., Soupionis Y., Ehlert S., Gritzalis D., "SIP vulnerabilities for SPIT, SPIT identification criteria, and anti-SPIT mechanisms evaluation framework", in *IP Handbook: Services, Technologies, and Security of Session Initiation Protocol*, Ilyas M., Ahson S. (Eds.), CRC Press, USA, November 2008 (to appear).
- Rebahi Y., Dritsas S., Golubenko T., Pannier B., Juell J.-F., Gritzalis D., *"A conceptual architecture for SPIT mitigation", in IP Handbook: Services, Technologies, and Security of Session Initiation Protocol*, Ilyas M., Ahson S. (Eds.), CRC Press, USA, November 2008 (to appear).
- The final results of the SPIDER project will be submitted for Journal publication in the next month

- Following other articles have been published in regard to SPIDER
  - R. Rothe, Spam als MP3, Der Tagesspiegel, Issue 2007/10/24
  - R. Rothe, Überleben in der Spam Flut, IT Admin Magazin 2008/10.
  - Arvanitellis M., Gritzali A., *Communications Services and VoIP in Greece: Trends and Perspectives (2005-07)*, AUEB-CIS Review Report Series, Athens, September 2008

- The code of the authentication module implemented by Fokus was given to a research department of Orange (France) in order to be compared to an approach that they are currently developing. This was done after the SPIDER consortium has given his agreement. The comparison results will be disseminated and help in advertising the SPIDER results. On the other side, the feedback of Orange will be very helpful for the SME partners in improving the usage of this module.

WP6: Legal and Ethical Issues

Spam prevention basically means that a user does not receive information another user has sent to him, i.e. a third party spam prevention system inhibit direct communication between two communication partners. To actually know which communication should be blocked by the system, it needs to know the user's preferences what to block, albeit without breaching the user's right of privacy. This issue needs to be addressed in a legal way.

- To meet legal standards, we have assessed available legal definition in the context of unsolicited message delivery and personal data collection. Definition has been assessed for European and National law. (⇒ D2.1).
  - European Law: Directives on Distance Selling, E-commerce, personal data protection, e-privacy and unfair practices.
  - National Law: Germany, Greece, Spain, Czech Republic, Norway
- Evaluation of these legal laws for their applicability to VoIP Spam. Only messages that classify as Spam under these definitions will be considered by SPIDER (⇒ D2.1, ⇒ D6.1).
- Evaluation of these legal laws for their applicability to VoIP personal data and if and how this will have any impact on the development of the SPIDER tools (⇒ D2.1, ⇒D6.1).
- Assessment of the goal to prevent Spam conflicting with the user's right for free speech (⇒ D2.1).
- Based on the legal basis as outlined in D6.1 we show how Spit prevention can be handled legally. The procedure is takes into account the normative principles
  - Legality principle
  - Finality principle
  - Proportionality principle
  - Transparency principle (⇒ D6.2)
- Assessment of the proposed SPIDER architecture and their modules in terms of personal data collection and resulting legal consequences (⇒D6.1, updated in D6,2)
- A discussion about ethical issues in contrast to legal issues within the SPIDER project has been started, with the result that those are overlapping within SPIDER, and no extra ethical issue analysis is needed. (⇒ D6.2)
- If necessary user consent request for data collection have been developed (⇒ D6.2).