The STACS Electronic Submission Service

Jochen Bern, Christoph Meinel, and Harald Sack

FB IV, Lehrstuhl für theoretische Informatik,
Universität Trier, D–54 286 Trier, Germany
{bern,meinel,sack}@Uni-Trier.DE
http://www.informatik.uni-trier.de/TI/

1 Problems in Electronic Conference Submission

One very popular software used to handle electronic conference submissions was written by the SIGACT Electronic Publishing Board. It was first used for the FOCS '95 conference, and later for a range of conferences including COCOON, FOCS, PODC, SODA, SPAA, STOC, and WDAG, staying basically unchanged.

Another conference in computer science that uses electronic submission mechanisms is the Symposium on Theoretical Aspects in Computer Science. STACS is an international conference covering all aspects of Theoretical Computer Science. It has proven to be - together with ICALP - the main European exchange place for ideas in this area. The program committee is internationally of top rank, the number of submissions is high (typically 100 to 140 papers), and the acceptance rate is low. Researchers come from all over the world to attend.

Our experience is that the problems in the design of conference submission services can be grouped into the following categories:

- **User Interface Problems** — First and foremost, selection of (a) **portable file format(s)** for submitted papers would be desirable; Failing that (e.g., PostScript), portability problems should be reported to the submitter **in an intellegible error message.** Next, steps have to be taken to ensure **reliable and unaltered delivery** of submissions. Finally, the whole workflow needs to be **intuitive and "familiar"** to the submitter.
- **Security Related Problems** — Conference announcements nowadays are put onto the WWW and, thus, can be found with search engines, so submission services may be accessed by more people than the attendees. A conference submission service needs to enforce a strict deadline. Consequently, malevolent manipulation is a serious threat and, besides the need for **privacy in submitter-service communications,** there is a need for reasonable protection against **denial of service attacks.** Where this cannot be achieved, we have to ensure that there are means to **trace the source of possibly malevolent manipulation** as far back as possible.
- **Problems in Further Processing** — Organizer, referees, and publisher have requirements on the **metadata** collected along with the submissions, which has to be taken into account in the design of the service. An issue of special importance for conference submissions, as these are usually collated into a single publication, is whether the format of the submissions allows **combination of submitted papers into a single document.**

C. Nikolaou, C. Stephanidis (Eds.): ECDL'98, LNCS 1513, pp. 639–640, 1998.

2 The STACS Submission Service

Most of the user interface is based on email and does not require users to be known beforehand. In order to make a submission, users request an identification (called *ticket*) for the paper to be transmitted, then send a PostScript file with prepended metadata in ASCII, and receive a first analysis in reply.

If this first analysis does not suffice, the user can then request a complete log of the PostScript interpreter (ghostscript) and / or retrieve *pictures* of single pages. The rationale in offering pictures is that their content **is completely environment independent** (barring multicolor issues). ghostscript is by far the most popular, stable, and forgiving PostScript interpreter available. We expect users to be widely familiarized with its warnings and error messages, making the logfiles a usable means for debugging to them.

After having assessed the suitability of the submitted PostScript, the user will finally issue either a SUBMIT command or a DELETE instruction.

Intruders are prevented from guessing a ticket by use of a random number of considerable length. In addition, we would like to have the legitimate traffic encrypted. As a compromise, we made the use of the most common cryptographic toolkit, PGP, optional.

A security precaution against service denial attacks is that we require users to retrieve a ticket *before* they are allowed to send data. The email requesting a ticket won't contain any information besides the reply address, and need not be stored. Thus, in order to clog the disks with fake data, a perpetrator needs to obtain the issued tickets first, which means that the email address is “live” and owned (legally or illegally) by him.

As soon as a paper is SUBMITted, the server software will assign a submission number, watermark the PostScript with the number, and send a notification to the server maintainer and the organizer (as well as the submitter).

3 Relevance to Digital Libraries

It is highly desirable to make documents available electronically some time ahead of the advent of digital libraries to facilitate the conversion of recent, hence popular, works. In the case of nonportable (resp. not-quite-portable) formats, submission of documents to conferences is an important point of verification because of the time constraints and the large number of relatively different and physically remote sites (submission service, organizers, referees). Automated verification of documents upon submission will greatly cut down on the problems incurred later, not to mention encourage use of “benign” tools and formats among authors.

At the same time, the interface between authors and submission service is the easiest place to collect and verify metadata on the documents, too. Introduction of properly constructed questionnaires presented to the authors might well be the method of choice to prevent the electronic documents from turning out to be legacy data in terms of metadata availability.