ERCIM NEWS

European Research Consortium for Informatics and Mathematics
www.ercim.org

Number 49

April 2002

Special Theme:

Information Security

CONTENTS

European Research Area – and Beyond

At the Lisbon summit in 2000 Heads of State and of Governments adopted a new strategic objective for the European Union for the next decade, which is to make Europe the most competitive and dynamic knowledge-based economy in the world.

At the same time it was clear that such an ambitious objective would only be achieved if the Union were to undertake major initiatives. In this context the Commission has proposed measures to make Europe much more active and attractive in the field of research, new technologies and innovation.

When I became Research Commissioner, just over two years ago, I proposed that research should be recognised as a vital area of Union policy. This was accepted and in Lisbon the highest EU representatives endorsed the creation of a European Research Area.

As a result, there is a new awareness that the knowledge-based society requires a much more pro-active, coherent and encompassing vision of the way Europeans manage research. At Union level, research needs a consistent policy with structured, forward-looking objectives.

Philippe Busquin, Commissioner for Research.

The Sixth Framework Programme 2002-2006 was consequently designed above all to be a structuring instrument for realising the European Research Area. As a result it features two major innovations.

The first one is that concentration on a few priorities (such as genomics, information society and sustainable development) has been accepted as a key principle to achieve a critical mass of finance and knowledge.

The second important change concerns new implementing instruments, namely networks of excellence and integrated projects of a much larger order of magnitude than current Community research projects, and the possibility of providing European support for joint research initiatives by several Member States. These innovations will allow the Framework Programme to act as a catalyst within the European Research Area.

In addition, I have recently laid two strong ideas on the table of the Spanish EU Presidency. The first is quantitative: upon my initiative, the Commission has proposed that the Union set itself the objective to increase its global research expenditure to 3% of GDP by 2010, instead of less than 2 % today.

We need to catch up with the United States and Japan. I stress that this is not a matter of increasing public expenditure but of stimulating private sector investments in research: annual R&D investment by European companies currently lags behind that of their US competitors by 43% or almost €71 billion. We cannot claim to become the most dynamic knowledge-based economy while producing far less knowledge than our competitors.

The second objective is qualitative. Creating a knowledge-based Europe clearly hinges on both research and education policies. The dual mission of universities in this respect illustrates clearly to what extent these two fields are linked. Together with my colleague Viviane Reding, the Commissioner for Education and Culture, we are going to put forward an integrated research and education strategy to foster the European Area of Knowledge.

I consider it vital that the European Union achieve these objectives if it is to fulfil the Lisbon goals, and I call on representants of the science and technology community, such as ERCIM, to take up these objectives in all the countries and regions of Europe.

Philippe Busquin

The Norwegian University of Science and Technology is now a Member of ERCIM

NTNU, the Norvegian University of Science and Technology now represents the Norwegian research community in informatics and mathematics including the relevant departments at SINTEF, the University of Oslo, the University of Bergen, the University of Tromsø and the Norwegian Computing Center. Membership was established with support from The Research Council of Norway. Until recently Norway was represented by SINTEF.

The research at NTNU is structured mainly through the basic organisation and five prioritised strategic research areas. The responsibility for ERCIM activities rests with the Faculty of Information Technology, Mathematics and Electrical Engineering (http://www.ime.ntnu.no/eng/). Some of the research activities will be co-ordinated within the framework of the strategic research area of Information and Communication Technology (ICT). (http://www.ntnu.no/satsingsomraader/ikt/english.htm)

NTNU main campus with Trondheim city center in the righ hand background.

NTNU is the major centre for technological education and research in Norway. Traditions in natural sciences and technology are interwoven with broadly based expertise in the classical university disciplines of the humanities, medicine and the social sciences. The Norwegian Institute of Technology (NTH), founded in 1910 is now an integral part of NTNU.

A specific ambition is to promote cross-disciplinary interplay between all forms of human intellectual activities, the arts, the natural and social sciences and technology. This is considered to be of particular importance when exploiting the opportunities of ICT in promoting the information society and innovations for industrial development.

Membership of ERCIM strengthens our position in contributing to European and international development and in providing Norway with an internationally competitive level of technological know-how.

Professor Arne Sølvberg, Dean at Faculty of Information Technology, Mathematics and Electrical Engineering is heading the ERCIM activities at NTNU. He is a member of the Board of Directors. Professor Finn Arve Aagesen, Head of Department of Telecommunications, is the representative on the Executive Committee.

NTNU key information:

- 7 faculties with a total of 79 departments
- 453 professors
- 1,770 other academic staff and doctoral students
- total number of employees: 3300 (37% women)
- at any given time, about 130 academics are on sabbatical
- 20,000 students.

NTNU's research staff is continuously engaged in some 2000 R&D projects. In addition 20-30 major scientific conferences are hosted by NTNU every year. NTNU has bilateral agreements concerning student exchanges with more than 200 foreign universities.

NTNU co-operates closely with SINTEF, a major independent European research institution with about 2,000 employees. SINTEF was established by the university and is located on the university campus. About 25% of the R&D projects of SINTEF are highly relevant to the ERCIM community.

The Faculty of Information Technology, Mathematics and Electrical Engineering has 270 academic staff and doctoral students and is responsible for around 20% of the educational activities at NTNU. The five strategic research areas are:

- Information and Communications Technology (ICT) , with special focus on Web-technology and ICT and learning
- Materials Technology
- Medical Technology and MR
- Energy and Environment
- Marine and Maritime Technology.

SonoWand, an ultrasound-based navigation system for image-guided key-hole surgery developed by MISON, a spin-off company from NTNU and SINTEF. MISON is the first company to resolve a compact integration of high quality 3D ultrasound and neuronavigation. They have achieved international recognition for their accomplishments in ultrasound-guided surgery. In December 2001 they were awarded the prestigious European IST Grand Prize for the best IT product in Europe.

Neuronavigation systems have become very common in neurosurgery in recent years. Conventional systems offer the capability of navigating surgical instruments into the brain based on MR or CT images that are several days old. As the operation proceeds, such images can no longer be trusted, 'the map does not correspond with the terrain'.

SonoWand enables the surgeon to easily update the map during surgery. It takes only a few seconds to scan the brain with high quality 3D ultrasound. The surgeon can then navigate tiny instruments down to the tumor and perform imageguided surgery with high precision (approximately 1mm). Ultrasound images of similar quality as MR-images simplify identification of small remaining tumor structures towards the end of the surgery, and the high precision navigation system simplify localization and removal through a smaller opening in the normal brain.

Focus Area ICT-Web Technology

NTNU's prioritisation of ICT will ensure access to competent professionals for the ICT industry and for all enterprises and other activities in society that make use of ICT. Our plans are developed in co-operation with business and industry.

The academic diversity at NTNU makes it possible to cover most aspects of ICT in research and teaching. The main areas are:

- computer supported co-operation
- information resources
- user interface
- software and system services
- information transport and networks
- electronics and hardware.

NTNU's research within electrical engineering, computer and information science, mathematics, etc., is not limited to the above-mentioned fields within ICT-web technology. For information about the entire range of subjects, see the outline of subjects under the Faculty of Information Technology, Mathematics and Electrical Engineering. http://www.ime.ntnu.no/eng/. Leader of the focus area ICT-web technology is Professor Arne Sølvberg.

Focus Area ICT and learning

The strength of this central field lies in the collaboration between pedagogical and technical experts and academic staff who work with the development of knowledge from many different angles. The central field benefits from the collaboration with business and industry and with system suppliers of telecommunications. Important issues in this field of research are:

- the integration of ICT and learning in teaching at NTNU
- the role of ICT in education in primary, secondary and supplementary education
- interdisciplinary communication
- the development and evaluation of ICT-supported methods of teaching
- experimentation with virtual laboratories and distance learning over the Internet.

The Laboratory for ICT and Learning and the NTNU-forum for ICT and learning are central to the research activities. Leader for ICT and Learning is Professor Bjørn Sørenssen, Department of Art and Media Studies, NTNU.

Links:
NTNU main website:
http://www.ntnu.no/indexe.php

Faculty of Information Technology, Mathematics and Electrical Engineering:
http://www.ime.ntnu.no/eng/

Strategic research area ICT:
http://www.ntnu.no/satsingsomraader/ikt/english.htm

Please contact:
Tore R. Jørgensen, NTNU,
Faculty of Information Technology,
Mathematics and Electrical Engineering
Tel: +47 73598035
E-mail: Tore.R.Jorgensen@ime.ntnu.no

Kick-off Meeting on Image Understanding

by Eric Pauwels

To focus the efforts of several ERCIM partners in high-level vision and image processing, a meeting on Image Understanding was organized in February at CWI.

The meeting drew participants from INRIA, KTH (Stockholm), UTIA (Prague), and TCD, as well as endorsements from CNR, SZTAKI, and FORTH. It served as a kick-off meeting for an official ERCIM Working Group, formal approval being expected later this Spring.

Motivation

Due to a confluence of various technologies, the capturing, storage and manipulation of images or video has become inexpensive and straightforward. As a consequence, vast collections of image-data and video-streams are being amassed in digital libraries rapidly expanding in scope and size. Unfortunately, this evolution might fall victim to its own success as the sheer size and complexity of these digital collections hamper efficient data mining. There is a growing consensus that this new bottleneck can only be alleviated by the development of content-aware processing methodologies that can automatically extract metadata with high semantic value and adapt the processing accordingly. The name of the working group, Image Understanding, has been chosen because it is a broad term that seems to cover all of the above-expounded goals.

Research Themes

The working group intends to organise its activities around three subthemes which by necessity share a lot of common ground. Below we give for each subtheme a non-exhaustive subject list:

- Indexing and retrieval: content-based image and video retrieval, (semi)-automatic generation of semantic metadata, cross-modality data mining (eg, combining images and text)
- Information integration: Fusion of different image modalities, content-aware image enhancement
- Visual decision and control: Visual inspection and expert systems, visual decision and control systems (eg, auto-pilots for cars), intelligent surveillance.

Methodologies

Progress in the above applications will call for methodological advances in research areas such as:

- generic probabilistic models for spatial structure detection and reasoning
- generic mathematical models for spatial processing (eg, morphology, PDEs, wavelets)
- computational intelligence (eg, simulation, Bayesian nets, evolutionary computing).

A scientific workshop will be held as a part of the ERCIM meetings on Thursday 6 June in Vienna. For expression of interest, as well as further information and suggestions,

Link:
http://www.cwi.nl/ERCIM/WG/Image_Understanding/

Please contact:
Eric Pauwels, CWI
Tel: +31 20 592 4225
E-mail: Eric.Pauwels@cwi.nl

Euro-Legal

News about legal information related to Information Technology from European directives, and pan-European legal requirements and regulations.

Network and Information Security
The recent EU Communication on Network and Information Security has as its key requirement the need for interoperability between IT systems and security solutions. Member States are responsible for incorporating effective information security into their e-procurement and e-government activities and in so doing offer a lead to private sector organisations. As technology evolves the use of managed security service providers that offer integrated security solutions is increasingly being considered in an effort to stay ahead of illegal hackers.

Cybercrime
The Communication on cybercrime, under discussion within the EU, recommends that a European forum be established to identify security problems and appropriate pan-European solutions to deal with cybercrime. The law across European jurisdictions at the present time varies considerably and lacks consistency. The demand for security solutions and associated legal advice will increase as awareness of the issues surrounding cybercrime grows.

Data Protection
Article 17 of the Data Protection Directive 95/46/EC requires Data Controllers and Data Processors to ensure that security measures are in place to protect personal data, and that those measures are appropriate to nature of the data and the risks involved with the processing. The 'appropriate measure' in respect of sensitive data, ie data about racial or ethnic origin, religious beliefs, sexual orientation, trade union membership, political opinions, physical or mental health or condition, criminal offences, proceedings or convictions, will require market leading security devices. At the present time there are no international standards for such security solutions.

e-learning
The research firm IDC revealed in their recent study European Corporate Business Skills Training Market Forecast and Analysis 2000-2005 that e-learning represented just 3% of the business skills training market in 2001. According to IDC only as recently as last year were European training organisations offering a mix of instructor-led and e-learning services. The use of e-learning techniques for IT training was slightly higher than for traditional business training, but even so e-learning in IT training only accounted for 6% of the market. IDC estimates a growth rate of 69% in e-learning for IT skills training between 2000-2005; the equivalent growth rate in the business skills sector was estimated at 108%.

by Heather Weaver, CLRC
Tel: +44 1 235 446151
E-mail: H.Weaver@rl.ac.uk

ERCIM Working Group Matrix Computation and Statistics — Second Workshop

by Bernard Philippe

The second workshop of the Working Group on Matrix Computation and Statistics was held in Rennes, France on 14-15 February 2002.

The Working Group 'Matrix Computation and Statistics' aims to find new topics of research emerging from several statistical applications that involve the use of linear algebra methods. The members are particularly interested in very large problems requiring the design of reliable, robust and fast procedures.

Second Workshop

The second workshop of the working group was hosted by INRIA in Rennes. Thirty participants attended fifteen presentations including two invited talks.

Nick Higham gave the first invited lecture on a problem of linear algebra encountered in Finance for the stock correlation study. The second invited speaker, Eric Moreau, presented the state-of-the-art for Independent Component Analysis a popular problem in signal processing. Both talks were video recorded and are available at: http://www.irisa.fr/bibli/videos/.

Thirteen other speakers presented various problems encountered in computational statistics, statistical signal processing and statistical communications. A number of presentations focused on ill conditioned linear systems arising in large least square problems and considered associated techniques as SVD or rank-revealing factorisations. Three talks were related to regression models and finally one talk was devoted to adaptive detection in mobile communication. The workshop programme, the abstracts and the slides of each presentation are available at the group's website.

The third workshop will be held in Neuchatel, 9-10 November, 2002.

Links:
Website of the group:
http://www.irisa.fr/aladin/wg-statlin/
http://www.unine.ch/iiun/matrix/index.htm
Videos of the invited talks:
http://www.irisa.fr/bibli/videos/

Please contact:
Bernard Philippe, INRIA
Tel: +33 2 99 84 73 38
E-mail: Bernard.Philippe@irisa.fr

ERCIM Sponsored Events

ERCIM sponsors up to fifteen conferences, workshops and summer schools per year. The funding for all types of events is in the order of 2000 Euro.

Forthcoming Events Sponsored by ERCIM:

- Eurocrypt2002 - Annual Conference on Cryptology Research
  Amsterdam, 28 April - 2 May, 2002
- MFCSIT2002 - Second Irish Conference on the Mathematical Foundations of Computer Science and Information Technology, National University of Ireland,
  Galway, Ireland, July 18-19, 2002
- ISSTA - International Symposium on Software Testing and Analysis,
  Rome, 22-24 July 2002
- CONCUR 2002, Brno, Czech Republic, 20-23 August 2002
- IEEE Joint International Requirements Engineering Conference (RE'02),
  Essen, Germany, 13-20 September 2002
- HCI02 - Human-computer Interaction for Mobile Devices,
  Pisa, Italy, 18-20 September 2002
- SOFSEM 2002 - 29th Annual Conference on Current Trends in Theory and Practice of Informatics, Milovy, Czech Republic, 24-29 November 2002

For detailed information about ERCIM event sponsorship, see:
http://www.ercim.org/activity/sponsored.html

Cor Baayen Award 2002

The 5000 Euro Cor Baayen Award for the most promising researcher in computer science and applied mathematics was created in 1995 to honour the first ERCIM President. The award is open to any young researcher having completed their PhD thesis in one of the 'ERCIM countries', currently: Austria, Czech Republic, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Norway, Slovakia, Sweden, Switzerland, the Netherlands and the United Kingdom. The selected fellow will be invited to the ERCIM meetings in autumn.

Rules for Nomination

Nominations for each country are made by the corresponding ERCIM Executive Committee member (also referred to as the 'national contact'). Those who wish a particular candidate to be nominated should therefore contact the ERCIM Executive Committee member for their country. Nominees must have carried out their work in one of the 'ERCIM countries' and they must have been awarded their PhD no more than two years prior to the date of nomination. Each ERCIM institute is allowed to nominate up to two persons from its country. A person can only be nominated once for the Cor Baayen Award. The selection of the Cor Baayen award is the responsibility of the ERCIM Executive Committee.

How to Nominate

For proposing a nomination to your national contact, fill out the Cor Baayen Award Nomination Form available at the ERCIM website.

Deadline

30 April 2002: nominations are to be received by the national contacts. Further information can be obtained from your national contact or from the ERCIM Cor Baayen Award coordinator Lubos Brim.

Links:
The ERCIM Cor Baayen Award:
http://www.ercim.org/activity/cor-baayen.html
National contacts:
http://www.ercim.org/contacts/execom/

Please contact:
Lubos Brim, CRCIM
Co-ordinator for the Cor Baayen Award
E-mail: lubos.brim@ercim.org

Information Security — Introduction

by Michael Waidner

Information security is one of the cornerstones of the Information Society. Integrity of financial transactions, accountability for electronic signatures, confidentiality within a virtual enterprise, privacy of personal information, dependability of critical infrastructure, all depend on the availability of strong, trustworthy security mechanisms. Ensuring the availability of these mechanisms requires solving several substantial R&D problems.

Security Engineering

Building secure systems has to evolve from an art to a security engineering discipline, with well-defined methods for constructing secure systems out of secure subsystems and basic components, and for assessing and formally validating security. Security-preserving notions of composability need to be developed, combining techniques from software engineering, secure hardware design, formal methods and cryptography. In particular European researchers have made a lot of progress in this direction, but nevertheless, security engineering is still closer to black magic than to science: the number of new vulnerabilities is still growing with a dreadful rate.

Protecting Privacy

Protecting privacy in the information society requires good security, but more than security is needed: tools that empower ordinary, non-technical users to control the information they reveal about themselves; business models and processes that balance the personal information they consume and customer value they generate; tools that enable enterprises to define and enforce their privacy practices, and to manage the identity and profile information given to them in a trustworthy and responsible way. In particular the development of enterprise privacy technologies has just started.

Intrusion Tolerance

One of the most important R&D topics is the development of intrusion tolerant systems: such systems work securely and safely even if some subsystems have been successfully attacked and maliciously corrupted – which is inevitably the case for most large systems. Such systems might even react on detected intrusions by reconfiguring themselves into a less corrupted state. Over the last few years a lot of work has been done on developing intrusion tolerant systems, in particular in the context of secure group communication and service replication. More work will be needed, in particular towards intrusion tolerance for systems based on large dynamic and ad-hoc groups. New trustworthy, intrusion tolerant means of authentication, authorization and management for such systems need to be developed.

Intrusion Detection

A very related topic is that of intrusion detection: How to detect intrusions, or more generally, high-risk situations? Many sensors have been developed that watch for specific situations, and tools to correlate alarms generated by different sensors in order to get a better picture. But still the main problems remain open: Intrusion detection systems generate by far too many false alarms, and rarely suggest effective reactions on true alarms. More R&D is needed that improves the quality and meaningfulness of alarms, eg, by considering semantically richer layers and specific applications.

This special issue points to some of the existing European R&D in information security. Although far from being a complete collection, it gives a good impression of where the European research community is putting its efforts today, and where one can expect, or at least hope for more results in the future.

Please contact:
Michael Waidner, IBM Zurich Research Lab
Tel: +41 1 724 8220
E-mail: wmi@zurich.ibm.com
http://www.zurich.ibm.com/~wmi

Methods and Tools against Hacker Attacks

by Andreas Wespi

The research work of the Global Security Analysis Lab (GSAL) Zurich is dedicated to ensuring that the benefits and convenience of networked computing continue to outweigh the risks of operating in an open networked environment.

Increasingly refined intrusion-detection techniques allow users to operate with confidence, in spite of the vast number of attacks that threaten computer systems. The Zurich lab supports IBM's security consulting practices and managed security services by developing methodologies and tools for the detection, prevention and analysis of recurring hacker attacks.

A key component for the GSAL's work on intrusion detection is its Vulnerability Database (VulDa), a comprehensive database of computer system weaknesses. Developed by the GSAL and now maintained by IBM's Managed Security Services (MSS) organisation, it contains all known attacks, hacks and countermeasures. It therefore provides a powerful tool for continued intrusion-detection research and, at the same time, supports IBM's security offerings by allowing carefully controlled access to the data by IBM consultants as well as IT architects and developers. VulDa is unique with respect to its size and the quality of the data it contains. It is a product of the continuous monitoring of information that is publicly available on the Internet (hacker Web sites, newsgroups, mailing lists, ftp sites) and data obtained from confidential IBM sources. The filtering and classification methods developed by GSAL provide unique options for accessing the data. Employing three different search engines has optimised the efficiency of information retrieval from the more than 40 gigabytes of compressed data contained in VulDa. In addition to a classical full-text search engine, advanced search techniques involving document clustering and vulnerability profiles vastly improve the accuracy of searches. The GSAL research activities concentrate on distributed intrusion-tolerant intrusion detection systems and are structured along three main axes: (i) development of new ID (Intrusion Detection) sensors, (ii) development of an ID management console, and (iii) research on the application of the dependability paradigm for intrusion detection. The third item constitutes the core of a three-year European project, which started in January 2000 and involves six partners. The Zurich laboratory is co-leader of this project.

Some results of the two first axes constitute the core of the Tivoli Risk Manager product and of a novel ID sensor called 'Web IDS', targeted at detecting attacks against Web servers. Tivoli Risk Manager enables organisations to centrally manage attacks, threats and exposures by correlating security information from various intrusion detectors. The solution enables administrators to eliminate clutter such as false positives, while quickly identifying the real security threats. This helps administrators respond with adaptive security measures. Web IDS is a real-time intrusion-detection system. It addresses penetration of the system, denial-of-service attacks, legal but undesirable activity, existing server vulnerabilities, and policy violations. This is required technology for e-business, because network intrusion-detection systems have a limited ability to detect Web attacks. The Web intrusion-detection system is designed specifically for content-based attacks on URLs using http or https.

Furthermore, three other new ID sensors have been developed and are currently being used. The first one is called a 'sniffer detector', which, as its name implies, is designed to detect so-called sniffers (passive intruders) in a network by simulating network traffic using intentionally false information as bait. Any reuse of this information indicates that a system has been compromised. This can also help locate an intruder within the network.

The second prototype is a so-called behaviour-based approach for intrusion detection. It monitors the behaviour of a system and sends an alert when a deviation from normal behaviour occurs. This behaviour-based approach is used for processes running on UNIX machines. It has broken new ground by applying the 'Teiresias' algorithm, originally used for DNA sequencing, to intrusion detection.

The third prototype, called RID ('routing intrusion detection'), has been developed primarily by a group of the Zurich Lab's Communications Systems department based on its core competency in routing algorithms. The GSAL is contributing to this joint project by providing expertise on the ID front. The principle of RID is to monitor a network for significant deviations from its normal behaviour. Intrusion detection is crucial for providing active security in a network. As a by-product, it also provides a means of automatically detecting potential system misconfigurations or errors that may affect overall network operation. An example of routing intrusion is a reachability attack: an intruder floods false reachability information to hijack calls or to generate a denial-of-service attack. An RID application prototype which detects reachability attacks in OSPF and PNNI has been implemented and is operational.

Please contact:
Andreas Wespi, IBM Zurich Research Lab, Switzerland
Tel: +41 1 724 8264
E-mail: anw@zurich.ibm.com

Regulating Access to Web-published Data

by Pierangela Samarati

The overall goal of the FASTER project (Flexible Access to Statistics Tables and Electronic Resources) is the development of a flexible and open system for controlled dissemination of statistical information. The system includes two major security components: a Statistical Disclosure component, for the sanitization of sensitive tables, and an Access Control component, allowing enforcement of protection requirements on published data.

Today's society places great demand on the dissemination and sharing of information. With the development and widespread use of the Internet and the World Wide Web, organizations in the private and public sectors are increasingly required to make their data available to the outside world. A growing amount of data is being collected by statistical agencies and census bureaus for analysis and subsequent distribution to the general public or to requesting organizations (eg, research institutions, government offices). Data producers can release their data directly, as in the case of national statistical institutions, or through the mediation of archive institutions (data publishers) that collect data from various sources for subsequent distribution.

This data distribution process is clearly selective: data cannot just be released to anybody. For instance, certain sensitive data can only be released to authorised individuals and/or for authorised purposes (eg, health data). Some data is subject to time restrictions and can only be released to the general public after a certain period; some data can be released only for non-commercial purposes; other data can only be released on payment. These few examples already give an idea of the variety of protection requirements that may have to be enforced. There is thus the need for a powerful and flexible access control system able to enforce the different requirements that the data producers (or publishers) may want to impose on the data access.

In the context of the FASTER project, we have developed an Access Control System for specifying and enforcing protection requirements on published data, such as statistical tables that have already undergone a statistical disclosure control process, or survey results, etc.

The access control component is based on a simple, expressive language for the specification of protection requirements. The approach has the following features:

- Abstractions/classifications support: this supports access rules based on the typical abstractions used by data producers and publishers, which can define categorizations of users, purposes of use, types of operations, and data objects.
- Metadata-dependent access rules: the authorization language allows the expression of access rules based on conditions on metadata describing (meta)properties of the stored data and the users, which can be represented through system-maintained profiles. For instance, an access control rule could grant EU citizens access to all census data more than 20 years old, where both the citizenship of the requesters and the age of data are represented as metadata.
- Dynamic condition support: access to certain data may depend on conditions that can be only evaluated at run-time, possibly via interaction with the user. Examples of such conditions, which must be associated with procedural calls executing the necessary actions, are agreement acceptance (that can be as simple as clicking an 'ok' button on a pop-up window), payment fulfillment, registration, or form filling.
- Expressiveness: the language is based on flexible rules specifying the accesses to be granted via boolean expressions evaluating properties of the requestor (metadata), of the data being accessed, as well as of the context (dynamic conditions). It also allows the expression of two kinds of access rules: authorizations and restrictions. Authorizations correspond to traditional permissions specifying sufficient conditions for an access, whereas restrictions make it possible to express conditions necessary for an access. The combined support of the two kinds of rules provides a natural fit for the types of protection requirements examined in real world scenarios known to the partners.
- Declarative: the language also has a simple declarative form, making it easy to use for nonspecialists in the field.

The Access Control System has been implemented and integrated in the FASTER architecture, which has been developed in a collaboration between the Data Archive at Essex University (UK), the Information Technology Dept. of the University of Milan (Italy), the Norwegian Social Science Data Services (Norway), the Dansk Data Arkiv(Denmark), the CentraalBureau voor de Statistiek (Netherlands), the Central Statistics Office (Ireland), the Statistik Sentralbyra (Norway), and the Centre National de la Recherche Scientifique (France). The access control language and component developed at the University of Milan are being adopted by the project partners to express and enforce protection requirements on the data they make available.

The approach used to develop an access control for web-publishing is now being extended to the support of credentials and certified statements (instead of requiring them to be stored at the server as metadata) and to policy composition. Policy composition refers to the controlled combination of access constraints independently specified by different authorities (eg, data respondent, publisher, producer, and privacy advocates and regulators).

Link:
Faster project: http://www.faster-data.org/
Security Group at the Information Technology Department, University of Milan: http://seclab.dti.unimi.it

Please contact:
Pierangela Samarati,
University of Milan, Italy
E-mail: samarati@dti.unimi.it

An.on — Privacy Protection on the Internet

by Hannes Federrath

An.on is a joint project from Dresden University of Technology and the Privacy Commissioner of Schleswig-Holstein/Germany. Its aim is to enable every user to protect his privacy on the Internet.

Using Internet services nowadays means leaving digital traces. More and more companies try to use these traces to create individual profiles of Internet users. Moreover especially people searching for help or advice in the Internet do not want others to get knowledge of their problems or diseases. Just imagine drug-related advisory services or medical information services. Even in the field of e-commerce anonymity plays a big role because no one is happy receiving spam email as a result of his Internet activities.

The An.on project wants to help everyone to protect his e-privacy. The open-source software developed within the project tries to reach this goal. The client software JAP provides anonymous and unobservable communication in the Internet. Upon this basis any privacy-related Internet service could be built. JAP runs on the JAVA platform and is easy to install and use to enable greenhorns among Intenet users to protect their privacy. Two scenarios using JAP are thinkable:

- JAP helps to protect the personal privacy of a single user. JAP can be installed on the user,s computer to protect his Internet actvities.
- JAP helps to protect the privacy of an organization. JAP can also be installed on a dedicated machine, for example on a proxy or firewall. There JAP serves as a privacy gateway for the entire company, and there is no need to install software on the user's workstation. This might be very useful for companies in order to hide their transactions and/or research activities on the Internet against observation by competitors or against other spying activities. (Note that a single user within the organization is traceable by the organization.)

JAP acts as a local proxy between the browser and the insecure Internet. All requests for Web pages go directly to JAP, and are multiply encrypted there. Instead of directly fetching the requested pages, the request is forwarded through a chain of multiple intermediate servers (named Mixes by the inventor of the theoretical background, David Chaum) offered or initiated by the An.on project. The encrypted requests travel through this chain of Mixes to the final destination on the Internet. The web server's responses are returned along the same route. Figure 1 illustrates the architecture of the system. The multiple layers of encryption protect all messages. A Mix samples messages in a batch, changes their coding (removes one layer of encryption) and forwards them all at the same time, but in a different order. All messages have the same length.

The final system developed within An.on will withstand so-called traffic analysis: Even an adversary observing all communication links cannot decide which incoming and outgoing packet belongs to each other. A surfer remains anonymous within the group of all users of the service. The system protects a user's Internet behaviour against tracing as long as at least one Mix in the chain works correctly. The Mixes are run by different organizations who were willing to participate in the An.on project. The chaining also prevents these Mixes from observing. Thus the system provides anonymity even against the anonymity service itself. The client program (JAP) runs on the Java platform. JAP works on all major platforms, for instance Windows, Macintosh, Linux, Solaris, etc. The Mix-servers are written in C++ and work on many different platforms including Windows NT, Linux, Solaris, Irix and other Unix-like operating systems. JAP and Mixes are Open-Source software. Everybody may inspect it and convince himself that the software provides the expected functionality and contains no hidden trapdoors. Figure 2 shows the user interface.

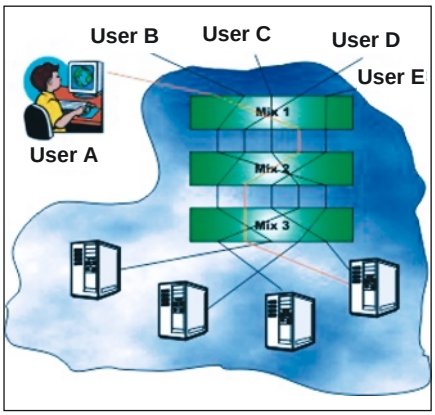


Figure 1: Architecture of the system.

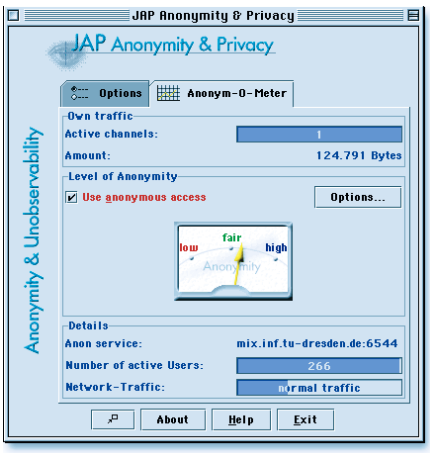


Figure 2: JAP user interface.

Future research in the An.on project concentrates on integrating a payment function in JAP and research on services (eg pseudonymous email) that might be built upon the infrastructure An.on already provides. We are always looking for partners - ISPs, IT security companies, networking companies, privacy commissioners - who are willing to operate a Mix and would like to support the idea of providing a world wide anonymity service. We are open to partners who want to discuss commercialization of our service.

An.on is a joint project from Dresden University of Technology and the Privacy Commissioner of Schleswig-Holstein, Germany. From 2001 to 2003 the project is sponsored by the German Federal Ministry of Economics and Technology.

Link:
An.on project: http://www.anon-online.org/

Please contact:
Hannes Federrath,
Dresden University of Technology, Germany
Tel: +49 351 463 38247
E-mail: jap@inf.tu-dresden.de

Privacy Protection and Trust Models

by Olle Olsson

The SAITS project, a cooperation between SICS, Stockholm University and others, will investigate technical aspects of privacy protection. Trust models is one of the techniques be evaluated.

We are investigating the problem of how computational components can acquire and use knowledge about the reliability of other components. This problem domain is conceptualised in terms of agents that interact with each other, where agents (consumers) may need services, and where other agents (producers) can offer such services. Consumers need to select which producer to enter into a contract with, and they should make this choice with the aim of optimising their accumulated utility, in short-term or long-term perspective. In open computational environments, a consumer is only able to observe the external behaviour of producers, ie, selection of a producer can only be done on the basis of hard facts about past performance of the producers.

How well does this model match properties of real-world problems? One example is electronic shopping on the Web. We consumers have to select which retailer to use, and often we only encounter these retailers on the web. Which one should we choose? Experiences, good or bad, may indicate that some retailers could be preferred while others should be avoided. But it is also important to take into account the potential gains we may make; cheap but dubious vs. expensive but reliable. Furthermore, we can make our decisions based on our own experiences, as well as on what we know about other consumers' experiences of the producers. This scenario is an example of a wider class of applications. Important characteristics of this class are that components can profit from using services provided by 'alien' components, that such alien components have externally observable behaviour, that they may deliver services of a priori unknown quality, and that the quality of services can be established after delivery.

Computational Models of Trust

Practical methods for building systems that use trust as a component in decision making are still in an immature state. The aim of this research is to develop a rational approach to trust-based systems, and to take initial steps towards an engineering methodology for such systems.

A rational approach to trust concerns identification of the theoretical basis of trust. Key elements are incorporated from related disciplines, eg, decision theory and utility theory. As trust is a concept with meaning in a societal context, the theory of social choice offers important scientific underpinnings. Theoretical frameworks as those mentioned provide alternative models of fundamental concepts, as well as proofs of the limits of what can be achieved.

A core problem is the ontological status of the concept of trust. Agents that communicate trust knowledge must conceptualise trust in the compatible ways. To some extent trust can be avoided as an explicit concept, by making agents disseminate information about their experiences in terms of their concrete interactions with other agents. The drawback of this approach is that an agent may thereby disclose private information, information that could compromise the privacy of the agent. By abstracting experiences into statements about trust, an agent can prevent personal sensitive information from being publicly accessible. An intermediate solution is to identify 'regions of trust', where the amount of communicated detailed information depends on the proximity of the trust regions to which the sender and the receiver belong.

A practical engineering methodology must take into account a number of practical issues, eg, how to choose between alternative algorithmic methods for making trust-based decisions. As there are infinitely many such algorithms, it is important to understand in what way a specific class of algorithms contributes to utility of the user. There may be real-world properties that have critical impact on how well certain algorithms succeed in optimising the utility of the user, and, from an engineering point of view, it is critical to understand how such environmental factors may influence the usefulness of specific trust-based methods.

We have developed a generic model of trust, on the level of generic problem-solving methods. A workbench has been developed, based on this model, where systems built on configurable and parametric trust models can be simulated. Preliminary results have been obtained in terms of sensitivity analysis, eg, how strong or weak is the correlation between utility and some environmental factor.

The trust model will be evaluated within a project focussing on privacy in the information society (SAITS). From a social point of view, individual citizens may protect themselves by being co-operative members of their society, and informing their peers about their experiences from earlier interactions with others. This 'gossiping' model is fundamentally about establishing a societal knowledge base of trust experiences, and about the use of this in individual decision making. Important questions are; how far can privacy protection be strengthened through such means, how can 'exchange rates' between different value/preference domains be established, and what are the threats to such societal mechanisms (eg, how to prevent that knowledge bases can be compromised or manipulated).

Please contact:
Olle Olsson, SICS
Tel: +46 8 633 1500
E-mail: olleo@sics.se

idemix for Internet Anonymity

by Endre Bangerter, Jan Camenisch, Els Van Herreweghen and Michael Waidner

The protection of data and privacy in the Internet is an issue of increasing concern and importance. Such protection requires not only that general standards and laws be agreed upon but also that technical measures be taken. An example of the latter is the 'idemix' project at IBM's Zurich Research Laboratory in Rüschlikon.

Modern forms of electronic communication and commerce are such that practically any transaction leaves a data trail in the global Internet, ie, information about who conducted which transaction with whom and when. Novel in this respect is not the fact that these data trails exist but rather the ease with which large amounts of data from many diverse sources can be gathered, combined, and exploited in a wide variety of ways.

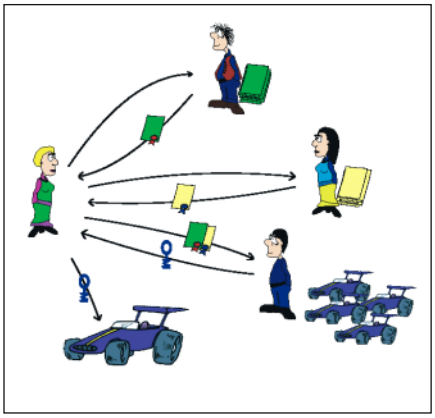
A scenario to illustrate what this can mean for each one of us is quickly given: Anyone who books a hotel room will probably be registered in an electronic system with his or her name, home address, and length of stay. This in itself may have numerous advantages, also for the hotel guest, for example in terms of frequent-flyer mileage. On the other hand, a malicious hotel employee could supply the guest's home address to a complice for a low-risk burglary in the absence of the owner. A regular customer of an on-line bookshop might appreciate receiving reading suggestions based on his or her specific preferences, but will be less than pleased if personal data is passed on to a third party, and the reading preferences are exploited for other purposes.

Using the Internet in a variety of ways increasingly puts personal data at risk. But just as modern technology is a threat to one's privacy, it also provides many tools for its protection: Making consistent use of cryptographic encoding when saving and transmitting data protects personal data from uninvolved third parties. A conscientious check of a business partner's identity, for example using digital signatures and public-key infrastructures (PKIs), can help to ensure that personal data are only given to partners deemed trustworthy. Finally, various technical tools exist to specify the privacy preferences of an individual, for example, which data one is willing to reveal for what purpose and to whom. Moreover, many organizations that process data publish details of their privacy policy, such as which data are gathered, and to whom and for what purpose they may eventually be forwarded.

All these technologies help to prevent an accidental transfer of personal data or a transfer under unclear conditions. But they cannot prevent data being passed on by, for example, a malicious hotel employee or, probably a much more frequent occurrence, being accessed by a curious employee or accidentally revealed because of technical problems.

This is why researchers at IBM's Zurich Research Laboratory in Rüschlikon, Switzerland, go one step further and investigate concepts that embrace 'data parsimony.' The basic concept is very simple: personal data is best protected if not revealed at all, ie, if the amount of data revealed is kept to a minimum. The idea is not new, many laws on the protection of personal data contain data frugality as an implicit guideline. The question then is how 'minimum' is defined.

Anybody who rents a car has to produce a valid driver's license, thereby – whether voluntarily or involuntarily – revealing a wealth of personal data. Actually, the car rental only needs the name and address of the person renting a car in the event of an emergency. As long as there is no accident, it would suffice to know that the person renting a car is in possession of a valid driver's license. In this case, the data minimum could be quite easily achieved: the name and address in the driver's license could simply be replaced by a randomly chosen artificial name, a pseudonym, provided that in an emergency the name hidden by a pseudonym could be retrieved.



In the left scenario, the organizations are the motorvehicle administration, an insurance company, and a sports cars rental agency. Alice on the left wants to rent a car. To do so, she needs to show the car rental agency her driver's licence and an insurance police. Conventionally, Alice would just send such documents to the rental agency who would then check them for valitidy. However, thereby Alice has to reveal the rental agency all kinds of unecessary information such as her name, her address, the details of her insurance policy. Idemix allows Alice to convince the rental agency that she owns a driver's license and an insurace policy without acctually sending them and thus the car rental agency does get to know only the information required but nothing more.

The 'idemix' system developed in Rüschlikon uses precisely such pseudonyms for e-commerce transactions: Today, anybody who subscribes to an on-line service has to register with the service using a user name and a password which he or she has to produce each time he or she wants to access the service. Under 'idemix' a user would first select a pseudonym, then register using this pseudonym and receive the corresponding credentials with an electronic signature. If later the user wants to access the service, he or she only must first provide proof to the service that the corresponding, digitally signed credentials are in his or her possession.

Of course, a user could merely present his or her pseudonym and the credentials; however, in many cases this would invalidate the desired data-protection

advantages in that the on-line service could monitor when and how a user uses the service, which in turn could result in an involuntary de-anonymization. In addition, the on-line service would often even know who owns the pseudonym, for example, for billing purposes.

By employing modern cryptographic techniques, the so-called Zero-Knowledge proofs, researchers at IBM have succeeded in resolving this issue: the pseudonym and credentials are given to the on-line service only in encrypted form. Although the on-line service cannot decrypt the information, it can still employ a clever interaction tactic with the user to verify the authenticity of the encrypted pseudonym and that the users must indeed own correct, digitally signed credentials. In an equally secure manner the user can supply credentials received from another organization to the on-line service. The car rental agency in our example could in this way receive proof of possession of a valid driver's license from the authorities, and of a valid credit card from a bank.

A user can in principle present his or her credentials any number of times in this way. Because a new encryption is used every time, the repeated use is hidden from the on-line service, ie, the user is not re-identified and thus, so to speak, can act completely anonymously. However, for many applications this total anonymity is undesirable: for example, if a rented car is not returned, the identity of the person who rented the car has to be retrievable. Therefore, the idemix system also has provision for a designated authority who can uncover such an identity. In the case of an 'anonymized' driving license, it could for example be the office that issued the license; in a business context it could be a third party trusted by both business partners.

The IBM researchers have also found a solution for another potential problem inherent in such data-protection measures: total anonymity could entice a 'generous' user to share his or her pseudonym and credentials for an expensive on-line service with friends and acquaintances. To render this as unattractive as possible, idemix is set up such that all pseudonyms and credentials of a user are interleaved in a clever and secret manner. If a user allows a friend to use one of his or her credentials, idemix is configured such that this is equivalent to granting permission to use all of his or her credentials. Sharing a password for a magazine subscription would then be virtually equivalent to sharing the secret PIN code of one's ATM card and the secret code for the safety deposit box at the bank. By using smartcards to implement parts of idemix, this sharing of pseudonyms and credentials can be further precluded.

Currently the idemix developers are building a prototype system to guarantee anonymity in the Internet. Decisive factors are not only the functionality but also the speed of the systems. It is estimated that transactions using idemix take about five times as long as transactions executed in the traditional manner. In practical use, however, idemix will not lead to a noticeable slowing down of the transaction speed because transactions typically take milliseconds to complete the actual process.

Link:
idemix project:
http://www.zurich.ibm.com/security/idemix/

Please contact:
Endre Bangerter, Jan Camenisch,
Els van Herreweghen and Michael Waidner,
IBM Zurich Research Lab,Switzerland
E-mail: {eba,jca,evh,wmi}@zurich.ibm.com

Towards Digital Credentials

by Stefan Brands

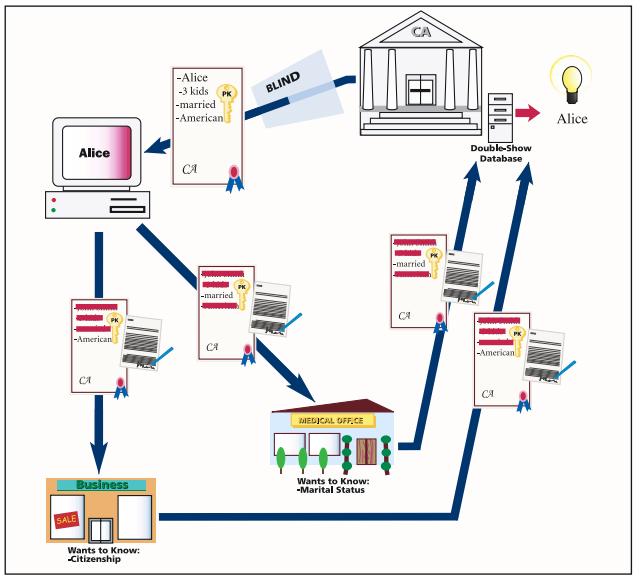
Digital Credentials are the digital equivalent of paper documents and other tangible objects traditionally used for establishing a person's privileges, characteristics, identity, and so on. Since they are just cryptographically protected binary strings, they can be electronically transferred and can be verified with 100 percent accuracy by computers. Digital Credentials preserve the key privacy properties of paper-based documents and plastic tokens, but offer much greater security. They are entirely feasible, as R&D work during the 1990s has shown. Several academic prototypes have been developed recently, and a new Canadian company, Credentica, is now commercializing Digital Credentials.

Often at least one of the parties in a transaction needs to know whether the other party is authorized to perform a certain action. Typically, authorization is granted on the basis of a person's privileges, personal characteristics, reputation, identity, membership to a group, willingness to provide value in exchange, and so on. In all these cases, the verifying party must rely on the inspection of one or more tangible objects issued by trusted third parties. Examples of such 'credentials' are coins and bank notes, stamps, medical prescriptions, cinema tickets, voting ballots, membership cards, access tokens, diplomas, passports, and drivers' licenses.

Physical credentials are increasingly prone to counterfeiting, however, and cannot be transferred by mobile devices, personal computers, and chipcards. Well-known cryptographic techniques,

such as digital identity certificates and message authentication codes, are not a solution:

- they encourage large-scale identity fraud and other devastating abuses of security holes that are inevitably caused by fundamentally relying on the central storage and management of sensitive information
- they ignore the privacy rights of individuals: all their actions can be linked and traced automatically and instantaneously, by a multitude of parties
- they do nothing to discourage participants from using each other's credentials.



Alice fraudulently uses the same one-show Digital Credential at both a medical office and a business. Although each separate transaction cannot be traced by anyone to her identity, the aggregate information is sufficient to enable the central authority to find out her identity.

To overcome these fundamental drawbacks, a transition to cryptographically protected digital forms of credentials is inevitable. (See S. Brands: "Rethinking Public Key Infrastructures and Digital Certificates; Building in Privacy," with a foreword by Ronald L. Rivest. August 2000, MIT Press, ISBN 0-262-02491-8, http://www.credentica.com/technology/book.html; and "A Technical Introduction To Digital Credentials," International Journal on Information Security, ed. Moti Yung, to appear in the August 2002 issue, http://www.credentica.com/ technology/overview.pdf.) It is entirely feasible to design Digital Credentials that address the complete spectrum of security, liability, and privacy risks for all parties involved. Digital Credentials preserve the key privacy properties of paper-based documents and plastic tokens, but offer much greater security and functionality:

- they are just sequences of zeros and ones, and so they can be transferred electronically and can be verified with 100 percent accuracy by computers
- the holder of a Digital Credential can selectively disclose a property of the data that the issuer encoded into it, without revealing anything else. For example, the holder of a 'privacy-enhanced' national ID card can prove that her Digital Credential specifies an identity that is NOT equal to one of several identities on a list of criminal suspects, without revealing her identity
- lending of a Digital Credential can be discouraged by encoding confidential data into it, such as a credit card number of the applicant. Even though the applicant can hide the confidential data when using the Digital Credential himself, it is not possible to use the digital credential without actually knowing the confidential data
- a limited-show Digital Credential can contain a built-in identifier that can be uncovered by a central party only if the Digital Credential is shown more than a predetermined number of times. See the Figure for an example. This property can be used to design secure electronic coins, stamps, gift certificates, and other value tokens
- they can be issued to, or embedded in, low-cost chipcards or other tamper-resistant devices. This provides an additional layer of protection against loss, theft, extortion, lending, copying, and discarding of digital credentials, and can prevent other kinds of unauthorized behaviour.

Digital Credentials are suitable for any communication or transaction system that needs to protect the transfer and storage of information. Examples are access control systems (for VPNs, subscription-based services, Web sites, databases, buildings, and so on); privacy-enhanced national ID cards; public transport tickets; electronic voting; e-health systems; financial securities trading; digital copyright protection; road-toll pricing; and electronic money.

The practicality of Digital Credentials has been well-established. Notably, last year Zeroknowledge Systems in Montreal developed a wireless prototype for RIM's Blackberry as well as a software development toolkit suitable for a wide variety of applications. Also, from 1993 until 1999, CAFE and OPERA, two major European consortiums co-funded by the European ESPRIT Programme, implemented and extensively tested a chipcard-based electronic cash system based on the Digital Credentials technology. (See Rafael Hirschfeld: "OPERA - Open Payments European Research Association", ERCIM News no.30, July 1997, http://www.ercim.org/publication/Ercim_News/enw30/hirschfeld.html.) Furthermore, several computer science graduates in Europe and America have independently developed academic prototypes.

In January 2002, a new company called Credentica was founded to commercialize Digital Credentials. Incorporated in Quebec, Credentica's mission is to deliver multi-party secure solutions for applications that involve the electronic transfer of sensitive information. Credentica leverages the Digital Credentials technology and its specialized R&D expertise to develop tailored software and services for the providers of Internet, wireless, and chipcard applications.

Link:
Credentia: http://www.credentica.com

Please contact:
Stefan Brands, McGill University,
School of Computer Science, Canada
Tel: +1 515 985 4111
E-mail: brands@credentica.com

The Cryptography Group at Aarhus University

by Ronald Cramer

The Cryptography Group at Aarhus University specializes in research of solutions of so called cryptographic protocols.

While Cryptography historically is merely about transporting data securely from A to B, the widespread use of computers in today's society poses new challenges to data security solutions based on cryptography. This goes far beyond virus protection and the like. In fact we need secure implementations of quite complicated tasks that were earlier handled by exchange of paper documents. Examples of this are electronic commerce and payments, electronic elections, etc. In this way, cryptography has become an enabling technology that underpins, for instance, the security of countless homebanking systems across the world. The Cryptography Group at Aarhus University specializes in research of solutions of this kind, so called cryptographic protocols. This can be based on public key cryptography such as RSA, but may also be based on security that is unbreakable, for instance using secure channels protected by quantum cryptography.

When modern cryptography started, in the 70s and early 80s, there was a large gap between theory and practice: whereas solutions did exist that could be analyzed and security proved rigorously, these constructions were way too inefficient for commercial use; on the other hand, no good analysis methods were known for the systems that practitioners were happy with. One of our main goals in the Aarhus crypto group is to contribute to bridging this gap and provide efficient constructions that are also provable. Several of our results, for instance in design of digital signatures and public key encryption schemes are in this direction. Often our research is conducted in close collaboration with other international universities and research labs.

We mention here briefly a couple of concrete lines of research that we have been involved in recently. The first of these is centred around secure electronic implementation of elections. Any election procedure needs to ensure that only people authorized to vote can actually do so, that the results correctly reflects the votes cast, that the privacy of voters is protected, and finally that the result can be verified after the election is over. Particularly the last two concerns may appear to be contradictory: if we can verify that all votes are counted and no one voted twice, it may seem to be necessary that each vote is linked to an individual voter, and so privacy would be violated. Fortunately, this is not the case: votes can be cast in encrypted form, after which all votes are combined to form an encryption of the result, which can the be decrypted and made public. But since this can take place without decrypting any single vote, privacy can still be protected. Several of us have contributed to this area recently, for instance in designing protocols that scale well to large elections, or in providing formal security proofs for election protocols. Through our cooperation with Cryptomathic, an Aarhus based company in security, we are involved in an EU supported project 'EVote' that aims at making such systems commercially available.

In a more general direction, we have also been active in design of general multiparty computation: an election may be seen as a game where a number of players (the voters) have inputs (how they want to vote) and we wish to compute some function on the inputs (the result of the election) securely, ie, the result must be correct and we must protect privacy of the inputs. It is in fact possible to compute any desired function in this way, and one of our main goals has been to provide as efficient as possible solutions of this general type.

A second trend goes towards providing so-called unconditional security: despite progress in the analysis of practical systems, all such schemes in use today are ultimately based on the assumption that certain problems, for instance factoring large integers, are difficult to solve for an attacker.

Unfortunately, we do not know with certainty that any concrete problem really is sufficiently hard. One way to solve these problems is to use quantum communication: we send information encoded in the state of very small physical systems, typically single elementary particles are used. The behaviour of so small systems is governed by quantum physics, and this has some unexpected consequences: information sent in this way cannot be eavesdropped without damaging the information sent in such a way that this can be detected by the receiver. By exploiting this fact properly, we can build channels with security that no amount of computing power can break. These facts have been known since the early 1980s, and the first experimental implementation is from 1990. In collaboration with the Physics Department in Aarhus, we have built a fully operational quantum cryptography prototype and analyzed its security against realistic attacks.

The research group in Cryptography at Aarhus University consists of the following members: head of group Ivan Damgard, senior researchers Ronald Cramer and Louis Salvail , and PhD students Jesper Buus Nielsen, Mads Jurik, Maciej Koprowski, Jens Groth, Kasper Dupont, Kirill Morozow and Jesus Fernandez.

Links:
Group Home Page:
http://www.brics.dk/Activities/Cryptology/

Center for Quantum Information Processing:
http://www.cki.au.dk

Electronic Voting:
http://www.cryptomathic.com/news/tech_frame_evote.html

Please contact:
Ronald Cramer, Aarhus University, Denmark
Tel: +45 89 42 3476
E-mail: cramer@daimi.aau.dk

New Prime Factorisation Record obtained using the General Number Field Sieve

by Friedrich Bahr, Jens Franke and Thorsten Kleinjung

A team of researchers at the University of Bonn established a new record in the art of factoring general integers into primes on 18 January 2002. This has implications for public-key cryptography.

Since the safety of the RSA cryptosystem depends on the difficulty of factoring general integers into primes, the selection of key size for this cryptosystem depends on the state of the art in this area of algorithmic number theory and on likely improvements in the future. Using a new implementation of the general number field sieve (GNFS), we have factored a 158-digit divisor of $2^{953}-1$, establishing a new record for the factorisation of general numbers without small divisors into primes.

The previous record was a 155-digit RSA challenge number factored by a team of mathematicians led by CWI in 1999.

Integer factorisations by GNFS start with a massively parallel polynomial selection step. This is followed by the sieving step, which is also massively parallel and takes most of the CPU time. Both steps are usually carried out using the idle time of ordinary office PCs or workstations. Our new contribution to this step is a new algorithm for lattice sieving, which results in a considerable improvement in speed compared to CWI's implementation.

The most time-consuming part of post-processing the siever output can be thought of as a linear algebra problem over the field F_2 with two elements on a sparse matrix of a few hundred million rows and columns. In a first filtering step, the size of this matrix is reduced to a few million rows and columns. This condensed matrix is then solved using a block Lanczos algorithm for sparse matrices over F_2. For the previous record, the filtering step was done on a large workstation and the Lanczos algorithm was run on a Cray 90 supercomputer. We wrote parallel implementations for both the filtering and the Lanczos step, running them on a LINUX cluster built by the scientific computing department at the institute for applied mathematics in Bonn.

Selected polynomials:

16915642778160*X^5
-756958519686871038*X^4
-1330267448641563970443 2*X^3
893959314395443111107991 93*X^2
8152148842253223998986577 1400*X^1
-6642901540608297872113384 33347600*X^0
and
X-747609196507292558201513 70977

the number:

3950587458326514452641976780061448199602077646030493645413937605157935562652945068360972784246821953509354430587049025199565533571020979922648497794944295 5603

the prime factors:

3388495837466721394368393204672181522815830368604993048084925840555281177
and
1165882340667125990314837655838327081813101225814639260043952099413134433416292453613 9

Conclusion

Due to improvements in the algorithms and their implementation as well as improvements in computer hardware since the CWI broke the 512-bit threshold in 1999, factoring a 512-bit RSA key within a year now costs less than 3000 Euro. Extrapolation of the development of the GNFS in the 1990s makes it likely that 768-bit keys become vulnerable at comparable cost within the decade starting in 2010. For large or medium-sized governments, they may become vulnerable within this decade.

We are indebted to the scientific computing department at the Institute for Applied Mathematics and to the Mathematical Institute at Bonn University for providing much of the computer hardware used for this record.

Links:
http://www.crypto-world.com/announcements/c158.txt
http://www.loria.fr/~zimmerma/records/gnfs158
http://wissrech.iam.uni-bonn.de/research/projects/parnass2

Please contact:
Friedrich Bahr, Jens Franke,
Thorsten Kleinjung,
University of Bonn, Germany
Tel: +49 228 73 29 52
E-mail: franke@math.uni-bonn.de

The Heuristic Evolution of Security and Insecurity

by John Clark and Jeremy Jacob

Researchers of the University of York in England aim to show that heuristic search techniques are powerful tools for modern day cryptology.

Heuristic search techniques such as simulated annealing and genetic algorithms are a major success story of computer science. Their use in cryptology, however, has remained very low key. Most work has been concerned with breaking simple classical ciphers and there has been little application to modern-day cryptological problems. Modern day crypto-algorithms do not lend themselves to cryptanalysis via heuristic search in the way that classical ciphers often do. This may well have led to heuristic search being discounted as a serious tool for cryptologists. We aim to show that its cryptological power is greatly underestimated and outline below some successes so far. The work ranges from the design of fundamental components, through cryptanalysis of identification schemes, to the automated synthesis of provably correct security protocols.

The Design of Cryptographic Building Blocks

Boolean functions (mappings of vectors of Boolean inputs to vectors of Boolean outputs) are at the heart of modern digital cryptography. Block ciphers such as the Data Encryption Standard and Advanced Encryption Standard, for example, can be regarded as (rather complex) Boolean functions (mapping plaintext input to ciphertext output in a manner determined by a secret key). Modern algorithms use simpler Boolean functions as components. These are carefully constructed to resist modern cryptanalytic attacks. Various resilience properties have been proposed as desirable but the field is subtle and engineering functions with excellent properties is surprisingly difficult. Mathematical construction remains the primary derivation technique but for the small single-output case our search approaches, based around simulated annealing, have been able to produce functions with more extreme values of properties than hitherto known. Counter-examples to several conjectures in the literature concerning achievable bounds have been demonstrated (often within a few seconds or less). When functions satisfying many criteria are sought our approaches have equalled, and in many cases bettered, the best results theoretical construction has provided to date. A feature of optimisation-based approaches is that they extend naturally to cater for additional desirable criteria (the cost functions used are appropriately amended). What counts as desirable, however, depends on who you are. Though the focus of our work is the attainment of functions with excellent profiles of positive properties, we have evidence to show that trapdoor properties may easily be incorporated too. Understanding how, why and when the techniques work effectively remains a major challenge.

Exploiting the Computational Dynamics of Search Techniques

Work over the past decade has shown that timing and power consumption characteristics of a cryptosystem can be exploited to reveal the secret keys used. The injection of hardware faults (even transient ones) into a cryptosystem can be similarly exploited. But it is not realised that search techniques such as simulated annealing also have computational dynamics that can be exploited in a cryptological context (using such characteristics we have successfully attacked instances of NP-complete problems underpinning certain identification protocols). The important point here is that annealing is a form of guided search. The way in which the solution moves from a random start point to its eventual destination may provide substantial information about the underlying solution to the problem instance under attack. The order in which solution elements attain their final values (ie the order in which those elements get stuck at that final values during a search) may be related to the actual sought solution. This may be regarded as a form of timing channel. On a different tack, we have obtained excellent results by warping the problem instance under attack in many different ways (in analogy with fault injection) and have used the sets of final solutions obtained by the searches to locate the solution to the original problem.

Profiling is a crucial component of such attacks and cryptosystems lend themselves to such approaches. Every secret key for example may define a representative instance. We can generate many representative instances, apply heuristic search based techniques aimed at finding the underlying secrets, and investigate how the actual secrets sought are related to the final solutions of various search runs and to the trajectories taken to such final solutions. This knowledge can then be applied to instances where the secret key is not known. This has already been demonstrated in the context of some identification schemes (as indicated above) and we now seek to attack block ciphers and public key algorithms.

Evolving Secure Protocols

A protocol is a series of message exchanges, each message designed to achieve some goal, typically making subsequent messages possible or meaningful. The notion of progress towards goals seems inherent to the concept of a protocol. We have sought to exploit this and have created a prototype framework for the automated synthesis of security protocols (eg key distribution protocols) based around the belief logic of Burrows, Abadi and Needham. We

carry out a guided search over the space of feasible protocols. Each protocol achieves something. The closer that something is to what we want, the fitter that protocol is deemed to be. The guided search approach (using simulated annealing or genetic algorithms) allows increasingly fit protocols to be evolved, eventually leading to one (or more) that meets all the intended goals. The formal nature of the belief logic used allows the evolution of protocols whose abstract executions are in fact proofs of their own correctness.

Heuristic search is a powerful tool for professional modern day cryptology. Its power has barely been tapped.

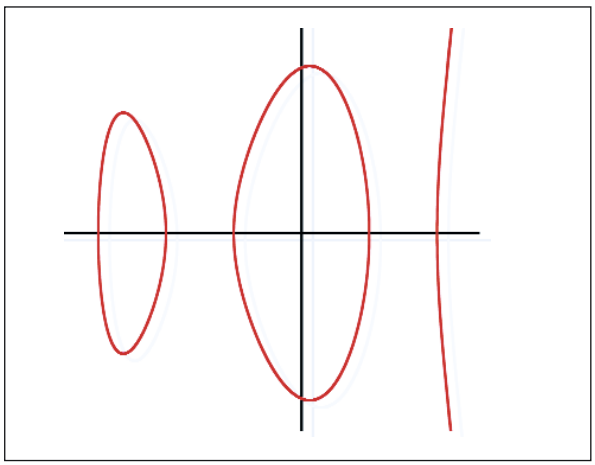
Please contact:
John A Clark and Jeremy L Jacob,
University of York, UK
Tel: +44 1904 433379
E-mail: {jac,jeremy}@cs.york.ac.uk

Cryptography using Hyperelliptic Curves

by Norbert Göb and Georg Kux

The Fraunhofer Institute for Industrial Mathematics in Kaiserslautern is developing a cryptosystem based on hyperelliptic curves. The main goals of this project are the establishment of the algorithmic foundations and the implementation of a prototype.

Nowadays the most popular public key cryptosystem is RSA. Its security relies on the fact that factoring a large integer known to be the product of two primes of similar size is supposed to be a computationally difficult problem. Nevertheless, good progress has been made in factoring due to the so-called number field sieve algorithm. The actual factoring record lies at 158 decimal digits for the composite number (see page 17), which means that 512-bit RSA-keys can no longer guarantee security.



A hyperelliptic curve over the real numbers. For cryptographic purposes one considers only curves over finite fields.

Considering this development it is important to have alternatives available. Many proposals have been made, most of which are not comparable with RSA in terms of running time and security per key-length. Elliptic curves, however, have proved to be a good choice for building public key cryptosystems which can seriously compete with RSA. Their security relies on the problem of computing logarithms in the group of points of an elliptic curve. Since this is supposed to be hard for relatively small parameters, they offer high-grade security even for small keys and are therefore the optimal choice for smart cards and other environments that provide only a limited storage space. Hyperelliptic curves are generalisations of elliptic curves, ie, they are of a higher genus (elliptic curves have a genus equal to one). Not as much is known about them, but they can be used to construct secure and efficient cryptosystems comparable to RSA.

In our project we investigate how the parameters must be chosen to achieve this goal. Certainly this implies consideration of many theoretical results. Contrary to an elliptic curve, the set of points on a hyperelliptic curve alone does not allow a mathematical group structure. In this case one has to generalise somewhat to find a group that provides similar features. This is called the Jacobi group. To offer reasonable security it is of great importance to know the exact number of elements of this group, the so-called class number. This cannot be simply read from the curve equation and there is still no known efficient algorithm to compute it for a general hyperelliptic curve. For special classes of curves, however, there exist methods for determining the class number.

Our current research concentrates on finding construction methods for secure Jacobi groups. These include specifying algorithms to test whether the curve resists all known attacks. Another task is to speed up the arithmetic needed in order to improve the running times of the corresponding cryptosystem.

Link:
http://www.itwm.fhg.de/mab/competences/Crypto/

Please contact:
Norbert Göb, FhG-ITWM
Tel: +49 631 303 1861
E-mail: goeb@itwm.fhg.de

Georg Kux, FhG-ITWM
Tel: +49 631 303 1865
E-mail: kux@itwm.fhg.de

Trusted Logic's Approach to Security for Embedded Systems: Innovation and Pragmatism

by Dominique Bolignano, Daniel Le Métayer and Claire Loiseaux

Trusted Logic is a start-up company stemming from INRIA which was created in January 1999. Its core business is the development and validation of secure embedded systems.

IT security is an area with great opportunities thanks to the ever increasing use of embedded components in everyday life (payment cards and terminals, GSM SIM cards, electronic purses etc). It also involves technical challenges because of the very high expectations of the market regarding security (confidentiality, integrity etc) and the scarce resources of devices such as smart cards and small terminals. One of the reasons for Trusted Logic's success is a pragmatic approach based on the combination of two complementary ingredients:

- the definition and the application of rigorous methodologies and
- the design and use of appropriate innovative tools.

Because security is by its nature a global concern, this combination of methodologies and tools covers all the steps of the design, development and validation of IT products. Here we provide some examples of key components of the security chain and briefly outline Trusted Logic solutions.

System Design: from Security Analysis to Design and Development

Relying on its experience in security evaluation, Trusted Logic has put forward a methodology covering the complete IT product lifecycle: from the risk analysis to the definition of the security architecture and the development of the product. This methodology is based on a precise definition of the model of the IT environment (including roles, assets to be protected, threats, etc.) and the different refinement levels of the product (from the functional specification to the implementation). Most importantly, this approach is in line with the Common Criteria which is the international standard for the evaluation of IT product security. In some sense, it can even be seen as an interpretation of the Common Criteria based on Trusted Logic complementary expertises in security, formal methods and software development.

Trusted Logic has developed a tool supporting its methodology for stepwise refinement. This tool, called TL-FIT, provides a variety of functionalities including modelisation, model consistency checking (both internal and refinement) and Common Criteria document generation. TL-FIT illustrates the pragmatic approach stressed in the introduction because it makes it possible to adapt the description style (informal, semi-formal, formal) and the associated verifications to the level of assurance stemming from the risk analysis. It is also representative of the need for innovation in this area since no other instrumented interpretation of the Common Criteria has been proposed so far and the proper integration of formal and semi-formal methods is still a very active research area.

Validation: Test, Analysis and Verification

Validation often boils down to testing in the traditional software engineering practice. Due to the very high requirements in the area of secure embedded systems, it is necessary to use a wider range of techniques and, most importantly, to justify their use and motivate their complementarity. First, testing itself has to be conducted in a systematic way. Trusted Logic's offer includes both security testing and functional testing. The first category is based on the potential vulnerabilities identified for the product and the second relies on its functional specification. Functional testing is supported by a tool, called TL-CAT, which provides different levels of automation (from the direct description of test suites in a high-level language to the automatic generation of test cases). The other validation techniques used by Trusted Logic are program analysis and program verification. Program analysers have been designed and developed by Trusted Logic to prove various properties of Java Card programs, from standard Java bytecode type correctness to specific security policies. Depending on the technical and economical context, such analysers can run either on the smart card itself, on hardware security modules, or on mundane workstations. The most ambitious verifications, which cannot be performed automatically by a program analyser, can be conducted within an interactive theorem prover. As an illustration, Trusted Logic has used Coq, the prover developed by Inria, to check the correctness of its byte code verifier and other key components of a Java Card virtual machine.

Conclusion: Innovation and Pragmatism

Trusted Logic's original market was the banking sector and smart card industry because this is where a strong need for secure embedded systems first appeared. This market is currently expanding to include terminal manufacturers, GSM, telecommunication operators, application providers etc, and Trusted Logic has become a leading actor in this area. Its reference list includes major players such as Visa, MasterCard, Schlumberger, Gemplus, Ingenico, France Telecom, Sun etc. We believe that the key factors for this success are the following:

1. Innovation: embedded systems have evolved extensively during the last decade and the rate of progress is not expected to slow in the next few years. One of the key technical factors here is the advent of open systems, especially through the rolling out of Java-based solutions. This facility introduces further

challenges in terms of security and so far we have seen only a small number of the new possibilities offered by open systems. To meet these challenges, Trusted Logic devotes a substantial part of its manpower to innovation (as an illustration, most of the techniques sketched in this paper are patented and licensed) and this effort will continue to increase in the future.

2. Pragmatism: the first motto could be "the use of the appropriate technique for the job". The choice of a technique (method or tool) should ultimately be motivated by the risk analysis and by the identification of the key security components which warrant the strongest validation efforts (the top level being verification using a theorem prover). Another crucial issue is the compatibility with standards: as mentioned above, all the methodologies and tools described here are in line with the Common Criteria. This compatibility is of prime importance both from a business and a technical point of view; in particular, it makes it easier to factorise efforts and share a common body of knowledge and methods within the security community. Among the other standards which are at the core of Trusted Logic activities, we should mention the languages of the Java family (in particular Java Card), the GlobalPlatform services for secure card management and the emerging profiles for small terminal interoperability (STIP and MIDP).

In conclusion, we believe that it is necessary for Europe to foster new collaborative efforts between research centres and innovative companies on security for embedded systems. Trusted Logic already collaborates in different ways with several European research centres, including INRIA, and intends to reinforce and multiply these links in the future.

Link:
http://www.trusted-logic.fr/

Please contact:
Daniel Le Métayer,
Trusted Logic S.A., France
Tel: +33 1 30 97 25 14
E-mail: Daniel.Le_Metayer@trusted-logic.fr

Verification of Cryptographic Protocols used in Fixed and Mobile Networks

by Tom Coffey, Reiner Dojen and Tomas Flanagan

The research undertaken by the Data Communications Security Laboratory at the University of Limerick includes: cryptographic algorithms and protocols for open hostile environments, non-repudiation protocols, global-wide identification, authentication and access control schemes, formal verification of security protocols using logical techniques and the developing area of steganography and information hiding.

Network security encompasses cryptographic protocols and algorithms used to ensure secure communication in a hostile environment. Such secure communication is indispensable in areas such as Internet, e-commerce and mobile communications. Fixed and mobile networks are vulnerable to a variety of attacks, such as message replay, parallel session, data interception and/or manipulation, repudiation and impersonation. Before trusting security protocols, it is necessary to have some degree of assurance that they fulfil their intended objectives.

Traditionally, general-purpose cryptographic protocols have been designed and verified using informal and intuitive techniques. However, the absence of formal verification of these protocols can lead to flaws and security errors remaining undetected. For example, the public-key authentication protocol of Needham and Schroeder was considered secure for over a decade. Verification of the Needham-Schroeder protocol using formal logics exposed vulnerability to replay attacks in this protocol. This highlights the fact that even comparably simple protocols are difficult to verify by intuitive techniques.

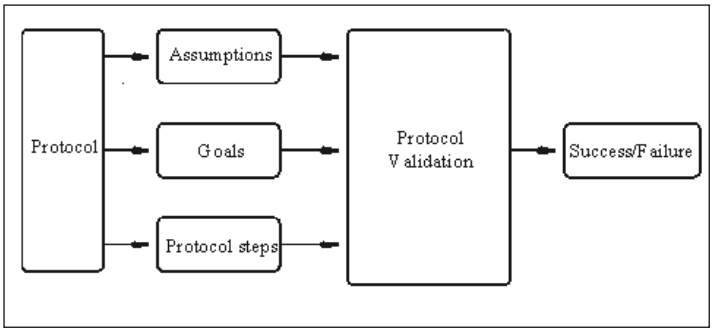
Formal verification aims at providing a rigid and thorough means of evaluating the correctness of a cryptographic protocol so that even subtle defects can be uncovered. Protocol verification methods include state space searching, the use of process algebras and logic-based analysis. Unfortunately, these formal verification methods are highly complex and cannot be easily applied by protocol designers.

The work undertaken by the Data Communications Security Laboratory at the University of Limerick includes the development of a logical technique, which can be used to reason about public-key cryptographic protocols. The technique combines the modal logics of knowledge and belief. Axioms are used to model the low-level properties of cryptographic communication systems such as: (i) data encryption and decryption, (ii) the transmission and reception of network data and (iii) the inability of a principal to decrypt a message without knowing the appropriate private key. These properties can be combined using inference rules to allow analysis of a wide range of public-key cryptographic protocols. The constructs of the logic are general purpose, enabling users deduce their own theorems, thus allowing for increased flexibility.

Protocol validation using this logic can be accomplished by deductive reasoning based on the application of valid rules of inference to sets of valid axioms. Once the logical syntax, rules of inference and axioms have been specified, the deduction process proceeds as follows:

- Formally express protocol steps in the language of the logic
- Formally express the desired protocol goals
- Starting with the initial protocol assumptions, build up logical statements after each protocol step using the logical axioms and inference rules.
- Compare these logical statements with the desired protocol goals, to see if the goals are achieved.

It is important that the protocol goals be correctly formulated. If the desired goals have not been achieved, then this generally points to a missing hypothesis in the protocol assumptions or the presence of some protocol flaw. If a protocol goal is inaccurate or unaccounted for, then the verification cannot succeed. In this way, a formal analysis not only assesses the reliability of a protocol, but also compels a designer to formally and unambiguously state the protocol assumptions and desired goals.



Protocol Verification Process.

Future work is aimed at developing a tool-suite to simplify the formal verification process because current techniques are highly complex and their application is error prone. Major components in this work include:

- automating the application of the logic, which requires the translation of the axioms, theorems and inference rules of the used logic into the language of some proving-engine.
- assistance in specifying protocols in the language of the logic, which involves providing a user-friendly interface to simplify the specification of the goals, assumptions and protocol steps.

Such a formal verification tool will offer communication security protocol designers, for both fixed and mobile networks, a significant advantage in the world ICT marketplace. It will enable them to prove the security and trustworthiness of the cryptographic communication protocol at an early stage of its design. Designers will then be able to prove, and improve, the security of the cryptographic protocols before the implementation phase begins, thereby reducing costs and increasing productivity. In addition this formal verification will significantly add user confidence to the end product.

In the current economic climate, where security poses a most serious obstacle to the continued growth of e-commerce and m-commerce, the requirement that security protocols be formally verified cannot be overstated.

Link:
http://www.ece.ul.ie/Research/DataComms

Please contact:
Tom Coffey, University of Limerick, Ireland
Tel: +353 61 202268
E-mail: Tom.Coffey@ul.ie

Security and Safety through Static Analysis

by Chris Hankin and Thomas Jensen

Static analysis of programs is a proven technology in the implementation of compilers and interpreters. Recent years have begun to see application of static analysis techniques in areas such as software validation and software re-engineering. 'Secsafe' is an IST project that aims at demonstrating that static analysis technology facilitates the validation of security and safety aspects of systems based on the Internet and on smart cards.

With its use of programmable smart cards and payment via the Internet, electronic commerce must guarantee the confidentiality and integrity of the data involved in transactions. The ever-increasing presence of software in these applications means that verifying that this software conforms to such security requirements becomes an all-important task which is far from trivial. The IST project 'Secsafe' has as its aim the development of methods for validating the safety and security of software that apply to both domains. This has led to the project focussing a substantial part of its efforts on the Java programming language and its dialect Java Card, dealing with both source-level and byte-code-level applications. The project is divided into five activities: specification of security properties, semantics, static analysis, algorithms and tools. The partners in the project are Imperial College (coordinator), the Technical University of Denmark, INRIA and the SME Trusted Logic SA.

The primary thrust of the project has been the security of multi-application smart cards programmed using the Java

Card language. Results so far include a list of security properties that Java Card applets should satisfy. Among other things, these properties are concerned with the allocation of memory, the handling of exceptions and the flow of information between applets. Another tangible outcome of the project is the definition of the Carmel intermediate language and its semantics. The Carmel language is distilled from the Java Card bytecode language with the aim of providing a small set of bytecodes that retains all the features of Java Card. This language has been given an operational semantics that specifies in detail the action of each Carmel instruction. In particular, it describes the workings of the firewall that separates the applets installed on a multi-application Java Card.

The verification of security properties is done by a static analysis that will build a correct approximation of the dynamic behaviour of the applets. This approximation will include a description of how data and objects flow between applets, which methods are called by a given applet and which instructions might lead to a security exception being raised. The project aims at developing a family of analyses such that the precision and cost of an analysis can be adjusted to the verification problem at hand. The flow logic framework for specifying static analyses has been chosen as an appropriate technology for ensuring this flexibility. It will be combined with powerful constraint resolution techniques in order to implement the analyses in an efficient manner.

One of the major problems in the field of multi-application smart cards is how to download applets dynamically on a card in a secure fashion. Due to the limited resources on the card, only a certain amount of verification can be done on-card. The Secsafe project contributes to overcoming this difficulty by investigating how analyses can be done as cost-effectively as possible and in a modular fashion. A first and important step towards this goal was achieved when Trusted Logic managed to design a bytecode verifier for Java Card that is efficient enough (in particular memory-wise) to be executed on-card. For this achievement, Trusted Logic won the 2001 European IST Prize. Extending this approach to other kinds of security verifications requires the development of techniques for modelling and analysing fragments of code that will support the inference of secure interfaces for applets. These interfaces will list the properties that a foreign applet must satisfy in order to ensure that its loading will not jeopardise the overall security of the card. The theoretical tools employed in this task include modular abstract interpretation and novel approaches to semantics of open systems.

Link:
Project homepage:
http://www.doc.ic.ac.uk/~siveroni/secsafe/

Please contact:
Thomas Jensen, IRISA/CNRS, France
Tel: +33 2 99 84 74 78
E-mail: Thomas.Jensen@inria.fr

Security: Formal Methods at Work

by Stefano Bistarelli, Fabio Martinelli and Marinella Petrocchi

Security is becoming a crucial issue in economic and social activities that involve electronic transactions. The 'Istituto di Informatica e Telematica' (IIT-CNR) is conducting several activities in the field of computer security. In particular, one group is involved in the definition and application of correct and rigorous formal methods for the analysis of network and system security aspects.

Cryptography has long been regarded as the main practical means to protect the confidentiality of information traveling on the communication networks. It is now also being adopted in many more complex applications, where the correctness of the algorithm does not guarantee 'per se' the correctness of the application. Procedures that apply cryptography are largely being used at the moment for message authentication, personal identification, digital signatures, electronic money transfer and other critical applications. Even if we assume that the cryptography in such procedures is completely reliable, weaknesses may result from the way in which it is used and assembled in the communication protocol. Noteworthy examples of this range from academic cryptographic protocols, such as the Needham-Schroeder public key protocol (1978), which was believed to be correct for several years until shown to be flawed by Lowe in 1996 (using formal techniques), to industrial applications, such as the Java programming language (which was found to have type flaws leading to security holes) and the recently announced security holes in Netscape Navigator and Internet Explorer. Many of these could conceivably have been prevented by a careful formal design and analysis.

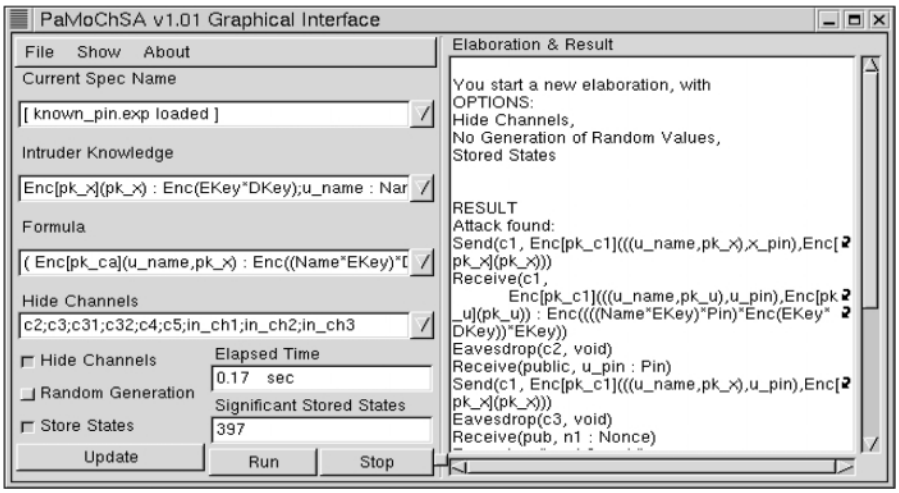
The detection and prevention of bugs are in fact two of the main reasons for using formal methods and related approaches: the specification of a system is an essential tool for analysis, and may help to discover many design errors. If the specification is given in an executable language, system execution can be simulated, making it easier to verify certain properties (early prototyping). Other reasons to use formal specifications typically include the need to express user requirements unambiguously, and to produce a reference guide for the system implementer.

In the formal analysis approach, a security protocol (or architecture) is commonly described as a process in an executable specification language. This process is designed to act in a hostile environment, usually represented as another process of the language (the attacker). In the worst-case analysis scenario, the attacker has complete control over the communication network, ie, it can intercept, fake and eavesdrop all communications. The entire system can be analyzed by applying specific techniques. For instance, security is sometimes analyzed by comparing the state-space resulting from the execution of the protocol with and without the attacker. The differences may represent possible attacks that have to be carefully studied. It is worth noting that the attacker is able to deduce new messages from the messages it has received during a computation. The basic algebraic features of cryptographic functions are represented as rewriting rules for terms of a language that denote cryptographic messages. This means that there may be rules that allow an attacker to discover a message encrypted with a certain key when the attacker also holds the correct decryption key.

Analysis methods of this type can be also implemented in automated software tools. These tools can be used by (reasonably) non-expert people and, hopefully, by the end-user of a security application in order to achieve a better comprehension of the security mechanisms offered by the application itself.

Our current and future activities in the field of formal analysis of computer security can be summarized as follows:

Theoretical: Our goal is to develop new and more efficient analysis techniques for security protocols and open systems. Recent advances concern the simulation of possible attacks using symbolic techniques to represent the state-space of the system under attack more succinctly. Other techniques aim at defining quality measures with respect to the relevance of possible attacks on security protocols, by enabling assessment of the relative merits of the protocols.



PaMoChSA graphical interface.

Applicative: We are now developing and testing a software tool (PaMoChSA, or Partial Model Checking Security Analyzer) implementing our analysis techniques. Features of the current implementation include:

- possibility to check a number of security properties, eg confidentiality, message and entity authentication, integrity
- no specification needed for the attacker
- the underlying theory is almost parametric with respect to the set of term rewriting rules for modeling cryptography
- a compiler translating from the common (and ambiguous) notation for security protocols used in the literature to a more accurate notation based on formal description techniques.

We are now applying our verification tool to real-life case studies. For example, we have performed a conceptual analysis of some procedures of the open source software OpenCA, which is basically a set of procedures for running a Certification Authority, issuing X.509 digital certificates. We have also analyzed some security mechanisms of the Simple Certificate Enrollment Protocol (SCEP).

Several national agencies and institutions support our research, for instance the Italian National Research Council (CNR), the Italian Ministry for the University and Scientific and Technological Research (MURST), the Center of Excellence for Research, Development and Demonstration of Advanced Information and Communication Technology (CSP).

Link:
http://www.iat.cnr.it/attivita/progetti/progetti.html

Please contact:
Fabio Martinelli, IIT-CNR
Tel: +39 050 315 3425
E-mail: fabio.martinelli@iit.cnr.it

CORAS - A Framework for Risk Analysis of Security Critical Systems

by Theo Dimitrakos, Juan Bicarregui and Ketil Stølen

CORAS is a European research and technological development project developing a tool supported framework for model-based security risk assessment.

A proper understanding of the limitations of the existing infrastructures is an important prerequisite for designing new services with a satisfying degree of security. In our opinion, an improved methodology for risk analysis is a necessary first step towards verifying and/or improving the security of such systems.

Ideally, risk management should be applied across all aspects of dependability. However, the increasing complexity of information systems urges the improvement of existing design and analysis methods in order to increase the likelihood that all possible threats are taken into consideration. More particularly there is a need for combining complementary security risk analysis methods with respect to the system architecture. We are not aware of an already developed integrated approach to system design and risk analysis, where the architecture expressed in the information system model is used to guide the combined application of risk analysis techniques. This need is being addressed in the European project CORAS for the area of security risk analysis.

An Overview of CORAS

The overall objective for the CORAS project is to develop a practical framework for model-based security risk assessment by exploiting the synthesis of risk analysis methods with semiformal specification methods supported by an adaptable tool-integration platform. As illustrated by the following figure, the CORAS framework has four main anchor-points.

The CORAS risk assessment methodology integrates aspects of HazOp analysis, Fault Tree Analysis (FTA), Failure Mode and Effect Criticality Analysis (FMECA), Markov Analysis as well as CRAMM. It is model-based in the sense that it gives detailed recommendations for the use of UML-oriented modelling in conjunction with assessment. It employs modelling technology for three main purposes:

- to describe the target of assessment at the right level of abstraction.
- as a medium for communication and interaction between different groups of stakeholders involved in risk assessment.
- to document risk assessment results and the assumptions on which these results depend.

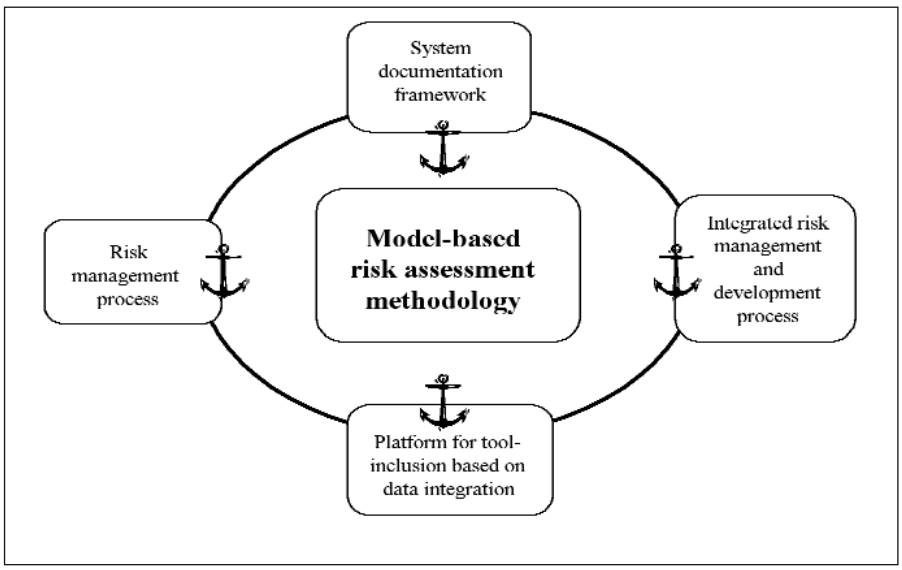


Figure 1: The CORAS framework for model-based risk assessment.

The core risk analysis segment of the CORAS risk management process are three sub-processes ('identify risks', 'analyse risks', 'risk evaluation'), grouped together at the top layer of the figure. The CORAS risk management process consists of instantiations of abstract patterns given the CORAS framework using different risk analysis methods in order to analyse different parts of the system. The choice of risk analysis method upon which the abstract pattern is instantiated depends on the viewpoint in which the part to be analysed appears and the detail incorporated in the context of the analysis depends on the phase in the development lifecycle. The specific instances of the CORAS risk management process that are used throughout the system lifecycle depend on the target (sub)system and the context of the analysis.

As the system description becomes more elaborate, any combination of refinement and decomposition results into a propagation of the risk analysis from the composite object to the components guided by the system architecture.

The CORAS Integration Platform

The CORAS platform is based on data integration implemented in terms of XML technology. The platform is being built around an internal data representation formalised in XML/XMI (characterised by XML schema). Based on XSL, relevant aspects of the internal data representation are being mapped to the internal data representations of other tools (and the other way around). This

allows the integration of system design case-tools with analysis tools or tools for vulnerability and treat management., as shown in the following figure. Standard XML commodity component tools provide much of the basic functionality.

Conclusions

CORAS aims to support the design process by developing an innovative tool-supported risk analysis methodology and process integrating:

- methods for risk analysis
- semiformal description methods – in particular, state-of-the-art methods for viewpoint- and object-oriented modeling (UML, MSC, RM-ODP)
- tool-integration technology supporting openness and interoperability.

The main innovations of the CORAS project stem from its emphasis on integrating risk analysis tightly into a UML and RM-ODP setting, supported by an iterative process, and underpinned by a platform for tool-integration targeting openness and interoperability.

Link:
Project website:
http://www.nr.no/coras

Please contact:
Theo Dimitrakos, CLRC
Tel: +44 1235 44 6387
E-mail: T.Dimitrakos@rl.ac.uk

Ketil Stølen, SINTEF Group, Norway
Tel: +47 22067897
E-mail: Ketil.Stoelen@informatics.sintef.no

SMM – Assessing a Company's IT Security

by Holger Kurrek

Are you investing your money for IT security in a holistic solution or are you guarding your frontage, while leaving the back doors open? The Fraunhofer Institute for Software and Systems Engineering (ISST) has developed a 'Security Maturity Model' (SMM) to assess a company's IT security.

Security is a matter of trust. Today, an enterprise cannot afford to lose its reputation and consequently its clients because of insufficient system security. IT security measures should therefore be transparent, complex and purposeful, but also easy to implement and cost-effective. The question is: how can we accurately define IT security? Since IT systems are strongly influenced by human behaviour, the answer lies far beyond purely technical solutions. The Fraunhofer ISST assesses the 'maturity' of a company's IT security with its specially developed 'Security Maturity Model'. After determining the current safety level, a concept is composed defining all the measures necessary to reach the next level. With this step-by-step model, the expected expenditure can be calculated more thoroughly. Through a goal-directed deployment of all means (within a level), even investments will become economically efficient.

Analysis

The analysis examines technical as well as organisational components and their integration in the corporate culture. The latter two fields have been minimally considered by previous procedures. Therefore, SMM offers a real opportunity for assessment.

Technology

All possible components are tested on their state of technological development and effective usage. The focal points of this assessment are capacity, quality and integration. Costs of purchase and operation as well as future capacity are also considered.

Organization

Technology is, however, only effective if organisational concepts use it effectively. Besides the definition of an IT security policy and its corresponding responsibilities, the focus of interest lies in a holistic IT security concept. Connections with suppliers, customers and partners are of central importance. We therefore examine particularly the contracts and the stated parameters in the Service Level Agreements. Furthermore, we will assess the precise predefinitions of authorisations and responsibilities.

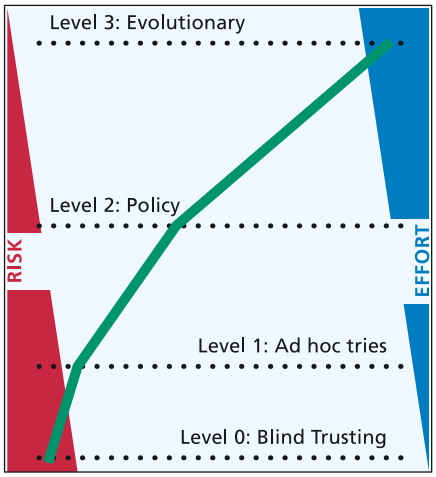
Corporate Culture

Technical and organisational measures must be deeply integrated into the corporate culture if a satisfactory effect is to be produced. Only decisive daily behaviour from both employees and management, also understood in the long term as a quality assurance process, will guarantee success. An atmosphere of attention and care can improve IT security considerably and can be very cost-effective. This is not only an assessment of IT experts and people in charge of IT security, but of all employees working with IT applications.

Apart from psychological aspects, such as the sense of responsibility, we also assess existing know-how and qualifications. A significant factor is purposeful staff development and its appropriate planning.

Assessment

The results of the analysis are then evaluated. Rather than being looked at separately, the various factors are observed in such a way as to take into account how they combine with each other. This allows us to accurately determine the current level of security and ensure the appropriate procedure. Thus, one can reconstruct how this particular level has been attained. Existing measures and actions necessary to reach the next level will also be identified to enable a goal-directed investment in those components



The four levels of the Security Maturity Model.

which are still missing. Often large investments into technical components can be significantly reduced though organisational measures and the normal and necessary development of corporate culture.

The figure shows the four levels of the model. Starting point is level 0 'blind trust', ie, the complete renunciation of IT security. By the use of minimal means, level 1 can be reached. A coordination of measures leads to level 2. The highest level can be attained through the usage of continuous processes (in detail these levels are much more complex and are specified in comprehensive measure catalogues).

Advantages

Using SMM is a fast way to identify the current state of a company's IT security. A cost-effective realisation is made possible through the optimisation of expenditure and concentration on the necessary focal points. With the bundling of all measures, synergies arise. Thus, goals are reached faster and expenditure is simultaneously reduced. The comprehensive model avoids discrepancies within the measures, which could otherwise cause gaps in IT security. The identification of the goals of the following level allows a strategic approach and improves financial control.

Services

Based on SMM, the Fraunhofer ISST offers the following services:

- evaluation of the current situation, eg during Technical Due Diligence
- formulation of measures to increase IT security
- quality assurance attendance of IT security measures.

To realise the measures, the Fraunhofer ISST relies on a procedural model and reference architectures.

Outlook

SMM is constantly being developed, since customers regularly test it in practice (small businesses and also large-scale enterprises and public administrations). In this way, not only is the analysis refined but the measures are also repeatedly rated on the current state of technology and can thus keep pace with its highly dynamic development.

An important focus is the comparability with other companies, not only to classify the competition but also to attain a continuously high level of security between partners. All developments will be added to the procedural model and reference architectures. Collaborations also exist between the institutes of the Fraunhofer-Gesellschaft, especially in the field of encryption and its necessary infrastructures (Public Key Infrastructure, PKI).

Links:
FhG-ISST: http://www.isst.fhg.de/

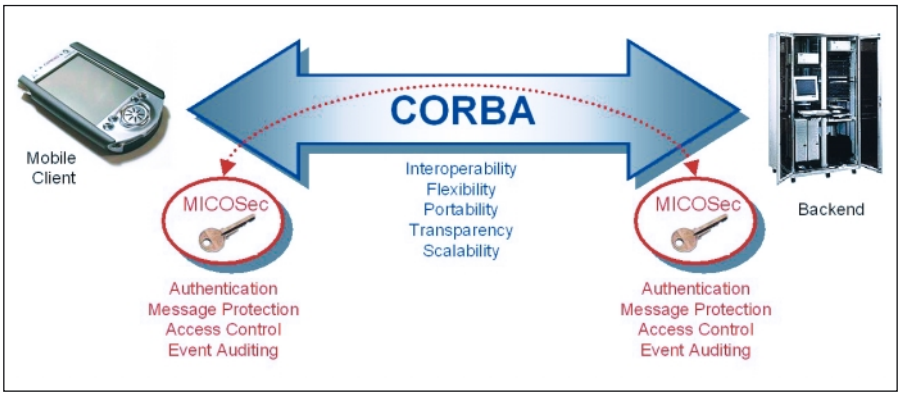
Please contact:
Holger Kurrek, FhG-ISST
Tel: +49 30 243 06 355
E-mail: holger.kurrek@isst.fhg.de

MICOSec: CORBA as a Secure Platform for Mobile Applications

by Rudolf Schreiner and Ulrich Lang

MICOSec is an Open Source implementation of the CORBA Security Services, which was developed by ObjectSecurity Ltd. as part of T-Systems Nova's Secure CORBA project. It was successfully used to develop CORBA-based applications, which comprised mobile clients on Compaq iPAQ Pocket PCs.

MICOSec (www.micosec.org) is an Open Source implementation of the CORBA Security Services (CORBASec), which was designed and implemented by ObjectSecurity Ltd. (www.objectsecurity.com) as part of Deutsche Telekom T-Systems Nova's Secure CORBA project. The original main goal of the project was to evaluate the usability of CORBASec for developing telecommunications applications, eg, for service provisioning or network management. Due to the fact that no CORBASec implementations that met the specific requirements of the project were initially available, it was decided to implement the complete CORBASec 1.7 level 2 specification.



CORBA security features.

MICOSec currently supports IIOP for unprotected communications, SSLIOP based on SSL Version 3, extended attributes for X.509 certificates, extended level 1 interfaces, authentication and message protection, Security Domain Membership Management, domain-based auditing (with flat file, Unix syslog and Postgresql as data storage), and domain-based access control. In addition to the MICO ORB, MICOSec uses OpenSSL as a crypto-library and Postgresql as a database for storing audit events. The latest MICOSec version is based on Portable Interceptors, so the Security Services can easily be ported to other standard conformant CORBA ORBs.

The very high deployment costs for future mobile communications networks make a quick return on investment a key survival factor for many communications carriers. Only attractive applications and services beyond the level of simple voice communication can motivate customers to spend more for mobile communication. To develop these applications quickly and economically, a standard application platform is needed. Since many of these applications will be security sensitive, the platform should also provide security functionality.

CORBA middleware is a sound base for the development of complex and distributed applications, but is normally regarded as too big and too complex to meet the requirements of mobile devices with limited resources. The first attempts to port CORBA ORBs to popular PDAs proved this prejudice to be true, when several groups tried to port the MICO ORB to the Palm Pilot with only limited success. The ORB had to be stripped down to minimal client-side functionality, because the performance of the Palm Pilot, CPU speed, memory and electric power were not sufficient to support a full CORBA ORB.

As part of our project, MICOSec was successfully used for the development of CORBA-based mobile applications on a Compaq iPAQ Pocket PC, a new generation of mobile devices. Porting MICOSec to a Compaq iPAQ Pocket PC running under Linux was straightforward, and it was only necessary to set up an appropriate cross-development environment. Then MICOSec, the underlying crypto-library and some demos could be compiled without problems. Porting existing CORBA applications was also very simple. The main issue was the user interface, since the Pocket PC has no keyboard and only a small display. However, the performance of MICOSec on the Pocket PC is more than satisfying. The main bottleneck is the RSA authentication at the beginning of the SSL handshake, which takes less than one second with a 1024 bit key.

MICOSec is currently used at Deutsche Telekom and ObjectSecurity for various projects (eg, for the development of a secure Parlay platform), for several demo applications to prove the viability of the concept, and for a research project in Ubiquitous Computing. It is anticipated that MICOSec will be used for commercial applications. The main foci of the further development of MICOSec are the secure interoperability with EJB by implementing the Common Secure Interoperability Version 2 protocol, integration into enterprise-wide security infrastructures, and secure CORBA components.

CORBA on the Pocket PC has proven to be a very useful platform for mobile applications, as it leverages all the advantages of CORBA and allows a seamless integration of mobile devices into existing applications. For example, it is possible to easily implement a graphical user interface with a CORBA-based geographical information system. It is also possible to use this platform for security-sensitive applications, since the CORBA security services provide the necessary functionality for the enforcement of various security policies.

MICOSec on mobile platforms will benefit from the further enhancement planned for MICOSec on standard systems, since the code base is the same (eg, in the future it will be possible to deploy secure CORBA components on the Pocket PC). The mobile device will then be a first-class part of a distributed application, rather than just a simple client with limited functionality. We anticipate that this platform will prove valuable for the rapid development of a broad range of applications.

Links:
ObjectSecurity Ltd.:
http://www.objectsecurity.com
MICOSec: http://www.micosec.org

Please contact:
ObjectSecurity Ltd, UK
E-mail: info@objectsecurity.com

Ameneh Alireza,
T-Systems Nova GmbH, Germany
E-mail: ameneh.alireza@t-systems.com

Security for Distributed and Mobile Active Objects with the ProActive Library

by Isabelle Attali, Denis Caromel and Arnaud Contes

In the domain of distributed applications, networks, and mobile agents, this research — started in spring 2001 in the Oasis Team at INRIA Sophia Antipolis — aims to develop mechanisms for specifying a security policy at a high level of abstraction for a given application.

The classical approach in information systems security requires a partitioning from the point of view of the organisation, geography and structure of information, in terms of their level of sensitivity and their domain. With the development of telecommunications however, a system can be distributed all over the world: data and code can be distributed and shared. This tremendous evolution prevents the classical approach being used.

Existing security techniques (PGP, C-SET, SSL, X509, etc) are known as standards working on a particular aspect of security and risks. We propose a complementary approach at the application level, possibly based on the cited standard techniques.

Besides existing system-level and network-level mechanisms, we believe that it is necessary to provide application-specific configurable techniques. Further, information transfer in object systems is enriched and more typed, compared with non-object systems (requests, replies, mobility of agents, remote object creation). These exchanges often require the definition of security attributes (authentication, integrity, confidentiality). Finally, in the setting of a given distributed application, some computers will play a specific role, and as a consequence, require specific rights and protections (eg, two secured servers versus access to a portable computer).

It seems of interest to organise in a hierarchical manner the different computers participating in a given distributed application, and to associate specific rights with these hierarchies. Our work can be seen as the creation of a Virtual Private Network at the application level. Another issue is secured meta-computing: how to use a federation of computing resources in a secure manner. A security policy for an application is specified in a declarative manner. An example of a security policy file is given in Figure 1.

A prototype has been implemented in Java with the ProActive library (over the standard RMI layer). This prototype is made of two parts:

- interpretation and verification of the consistency between different

Domains

INRIA = *.inria.fr;
ETCA = *.etca.fr;

Policy

INRIA <—> ETCA: Q,R # [+A,+I,?C];
ETCA —> INRIA: M # [+A,+I,+C];

Figure 1: Example of a security policy file for an application.

A user defines in this policy two abstract domains (INRIA, ETCA) and expresses that communications – Queries and Replies – have to be authenticated between all computers of INRIA and ETCA (+A).

Moreover, mobile agents (M) are allowed only from ETCA to INRIA, and must be in mode authentication, confidentiality, and integrity (+A, +I, +C).

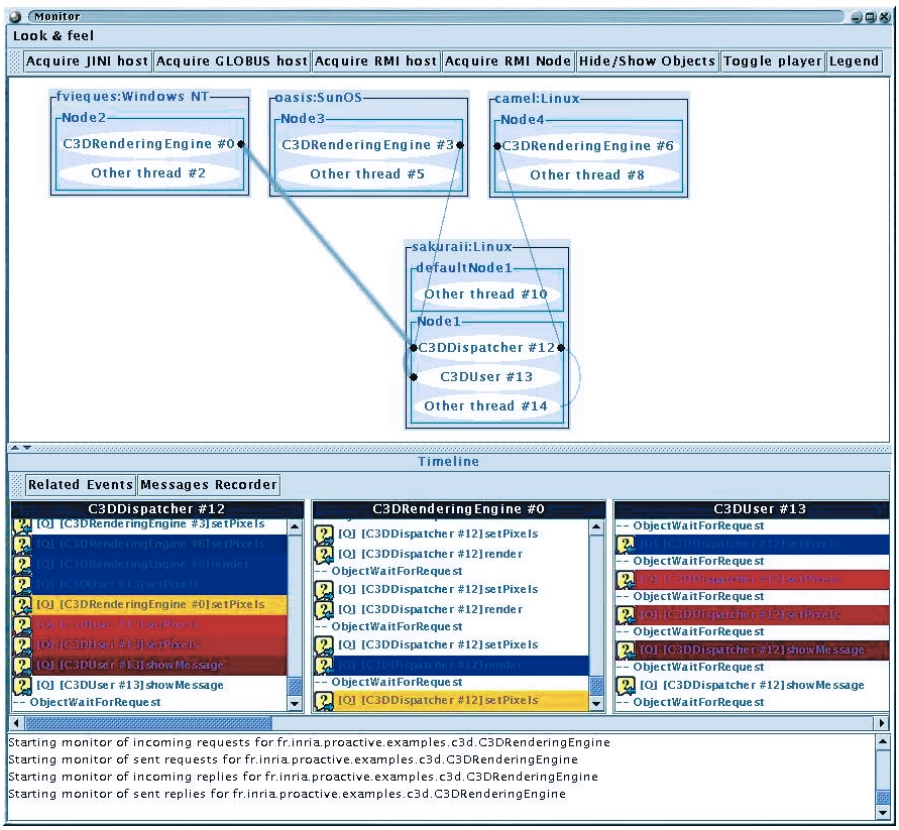


Figure 2: Deploying and monitoring a ProActive application using a graphical interface (IC2D) that makes it possible to 'drag and drop objects over the world'.

security policies, and policy negociation between hosts
- handling of these policies using public, private and symmetric keys; we are using the SPKI public key infrastructure for encoding communications.

Examples have already been specified and executed and early performance measures have shown that this approach is viable. For instance, only 25ms were required for the full treatment of a secured message including encryption, transfer, decryption, and the checking of the sender certificate and digital signature.

Our approach proposes security features at the application level, especially in the setting of distributed objects with mobility.

Compared to related work, the ProActive security can be characterised by four main advantages:
- we use standard (non-modified) tools (eg, standard JVM, standard SPKI infrastructure); this gives a wide portability to our applications
- the declarative language allows easy definition and composition of security policies, potentially in a decentralised manner
- object and activity mobility is now possible in distributed applications and shows up new solutions for information protection
- security can be finely tuned with respect to information sensitivity and threat levels by treating each application separately. This would allow the high cost of cryptographic mechanisms in a local network to be avoided.

Future work will include a better control of security policies in the presence of mobile code and mobile agents. We will also study the composition of security policies (hierarchy, compatibility, static verification, etc). Another issue is to study the centralisation of all (or part) of a security policy. Lastly, we wish to formally model our approach in order to prove that policies are respected, in the presence of migration and variable placements of objects on machines.

Link:
http://www.inria.fr/oasis/ProActive/

Please contact:
Isabelle Attali, INRIA
Tel: +33 4 92 38 79 10
E-mail: ia@sophia.inria.fr

Mobile IP Security in Foreign Networks

by Sami Lehtonen

Mobile IP itself doesn't offer security features such as access restrictions in foreign networks. In the project WLANSecu, started in 2000, a group of scientists at VTT, Kimmo Ahola, Sami Lehtonen, and Sami Pönkänen researched security of mobile users visiting foreign networks.

The aim of the project was to design and implement additional security features to a standard Mobile IP environment. The main prerequisite was to leave the Mobile Node (MN) and Home Agent (HA) unmodified. When the MN is communicating with nodes in the same foreign network the traffic will be routed unnecessarily through the public Internet. This causes a major problem that had to be solved. Another significant objective was to provide a mechanism for the mobile user and the users in the foreign network to dynamically allow and deny connections in between.

Normally, when optimizing routes, the MN requests the HA to send Binding Update to all CNs. In this project the triangular routing between the Home Agent (HA), the Correspondent Node (CN) and the MN (via FA, Foreign Agent) was solved using a Binding Update message sent to the particular CN by the FA. Only the nodes located in the foreign network were altered, thus leaving the MN and the HA unmodified.

An additional application, which we call Mobile Firewall Daemon (MFWD), was designed to provide the dynamic connection control. The FA notifies the MFWD whenever a MN arrives to its network. All traffic to and from the MN would go through MFWD. MFWD would then listen to its web user interface for local and mobile users requesting changes in firewall rules.

These designed mechanisms were implemented on Linux-based systems with the intent to create a 'proof-of-concept' trial network. The function of this trial network has been demonstrated numerous times since its initial setup.

The success in the trial network setup showed that the project achieved reasonable results. However, many improvement ideas have arised, and we are planning to take this concept for another iteration round. A major enchancement would be to implement the MFWD in an Active Network environment, which would make it possible to offer more flexible traffic control and supporting services.

Please contact:
Sami Lehtonen, VTT
Tel: +358 9 456 7240
E-mail: Sami.Lehtonen@vtt.fi

Security Issues underpinning Large Virtual Organisations

by Theo Dimitrakos, Brian Matthews and Juan Bicarregui

GRID computing has emerged as a new approach to a high-performance distributed computing infrastructure within the last five years. The GRID concept has been generalised to cover a virtual organisation, defined as any dynamic collection of individuals and institutions which are required to share resources to achieve certain goals. In this article we provide an overview of ongoing research towards building GRID-aware security and trust management solutions.

GRID technologies define a new powerful computing paradigm by analogy to the electric Power Gird. Based on the Internet, the GRID seeks to extend the scope of distributed computing to encompass large-scale resource sharing including massive data-stores and high-performance networking, and shared use of computational resources, be they supercomputers or large networks of workstations.The GRID concept has been generalised to cover a virtual organisation, defined as any dynamic collection of individuals and institutions which are required to share resources to achieve certain goals.

Currently the applications driving the development of this infrastructure are large-scale scientific collaborations, such as the Information Power GRID, (www.ipg.nasa.gov) and the European DataGRID Project (www.eu-dataGRID.org), which have a clear need for the collaborative use of resources, both data and computational, and established communities which can pool their resources for common goals. Tools are appearing to support the GRID concept, notably those developed in the projects Globus (www.globus.org), Condor (www.cs.wisc.edu/condor) and Legion (www.cs.virginia.edu/~legion). In the near future, the GRID concept will find applications in commerce and industry supporting distributed collaborative design and engineering, or distributed supply chains.

Grid technology will be used to allow enterprises to outsource computing resources and the ad-hoc creation of Virtual Organisations (VOs) within commercially available computing grids will allow for an effective management of computing resources at a global scale.

Security management is major obstacle to overcome in the route of commercialising GRID infrastructures. The traditional GRID infrastructure, such as the GRID Security Infrastructure (GSI) from Globus, using the X.509 certificates as its authentication mechanism, depends on interfaces at the protocol level to provide the security infrastructure. However, this approach has concentrated on authentication and does not cover all aspects of security management. In particular there is little support for authorisation management, the specification and enforcement of security policies, the treatment of cases where the (agents managing the) collaborating resources have no prior knowledge of each other (or their certifying authorities).

In the paper 'Building Trust on the GRID - Trust Issues Underpinning Scalable Virtual Organisations', we identified the need to supplement this infrastructure by raising the level of the trust within a GRID architecture. This builts upon the established literature in trust analysis, which provides a framework for analysing how trust should be transmitted between agents in distributed systems, especially dealing with how to propagate trust between agents with little or no prior knowledge of each other. The basis of this infrastructure is the explicit declaration and publication of trust policies by participating resources on the GRID using an appropriate policy specification exchange language. Agents wishing to utilise resources would be able to present their credentials, policies and requirements to the participating resources and an automated process would verify the credentials, possibly referring to trusted third parties, to establish identity, deduce authorisation based upon supplier and consumer policies and to authorise (or revoke) access under the specified the conditions of use. To support this, one would need to add at least the following:

- resource brokerage services to facilitate resource discovery and allocation in compliance with a contractual realisation of QoS requirements
- a means of publishing, negotiating and exchanging policy statements
- appropriate trust support services, such networks of trust authorities, and an infrastructure allowing for the dynamic formation of certification chains
- a trust management framework able to cope with the complexity and uncertainty underpinning most interactions in open dynamic systems such as the GRID architectures; this will need to draw a distinction between perceived and actual security, relate trust to enterprise objectives and weigh it against transaction risk
- a policy-driven security management system, which is able to support the dynamic formation of collectives of entities which are required to share resources to achieve certain goals.

In a paper entitlet "Policy-Driven Access Control over a Distributed Firewall Architecture" (in Proceedings of the IEEE Policy Workshop 2002, IEEE Press, 2002) we propose to address the latter by bringing together two current lines of research:

- policy-driven access control, where policies are identified as first-class data objects in their own right, which can be negotiated and tailored to particular groups of clients
- a distributed firewalls architecture augmented with the concept of Closed User Groups (CUG), which has the benefits of facilitating P2P collaboration, whilst allowing to maintain the integrity of systems supplied by central administration of the security policies.

So far we have focused on the realisation of policy-driven access control management for CUG-aware distributed firewalls that can easily adapted to facilitate a GRID based implementation. In the following months we plan to test the applicability of this architecture in a GRID test-bed in areas such as e-Science (within CLRC e-Science programme http://www.escience.clrc.ac.uk) or e-Business (within GRASP a forthcoming European project aiming to explore an advanced infrastructure for Application Service Provision based on GRID technology.

Links:
CLRC e-Science programme:
http://www.escience.clrc.ac.uk/
GRASP:
http://www.bitd.clrc.ac.uk/Activity/GRASP/

Please contact:
Theo Dimitrakos, CLRC
Tel: +44 1235 44 6387
E-mail: T.Dimitrakos@rl.ac.uk

Information Systems Security at CLRC

by Trevor Daniels

Maintaining adequate security against the proliferating threats from Internet hackers is difficult enough for an organisation which needs only occasional access to the Internet; achieving it when continuous Internet access is absolutely essential to carrying on the most important parts of the organisation's mission, as it is for research laboratories involved in international collaborations, is a continual challenge to technical staff. We describe in non-technical terms some of the approaches adopted by CLRC over the last three years to meet this challenge.

The main business of CLRC is to promote research, to support the advancement of knowledge and to promote public understanding in science, engineering and technology. This involves close collaboration with a wide variety of academic and research institutes and technological companies world-wide, and a free exchange of information with both these organisations and the general public is a fundamental part of most of CLRC's work.

The facilities offered by the Internet are nowadays essential to meet these requirements for collaboration and dissemination, but they can only be employed effectively by operating a relatively open Internet security policy. Often the operating regime within an international collaboration is determined by that collaboration, and it is not possible to impose security standards which might prevent that collaboration inter-working effectively.

Furthermore, because most parts of the laboratory are involved in such collaborations, a very large number of servers of various kinds must be visible to the Internet, yet the staff involved in maintaining those servers are scientists, not security experts.

Maintaining adequate security under these conditions requires flexibility and a high degree of expertise to configure and maintain the several protection mechanisms deployed in the firewalls: these must keep intruders out yet not impede the work of the laboratory. How has this been achieved? Initially we adopted two main techniques to limit the exposure of CLRC computers to intruders.

First, we divided our computers into those that needed to provide externally visible services (let us call these Class A computers) and those that did not (Class B), and we assigned IP addresses from a specific range to Class A computers. This enabled us to block incoming connections which attempted to contact Class B computers easily and efficiently in the routers connecting our LAN to the Internet. This effectively hid over 90% of our computers from Internet intruders without limiting the ability of those machines to initiate connections themselves.

Second, we determined what precise services each Class A computer needed to provide, and limited connections to those machines to the specific port numbers which were required to deliver those services.

Coupled with the requirement that the system administrators of Class A computers must maintain their systems to specific standards, these relatively simple techniques provided adequate security for most of the period up to the end of 2000, and met the objective of not interfering with the normal work of the Laboratory. However, during early 2001 the continually increasing number of vulnerabilities being actively exploited by intruders, the widening variety and increasing effectiveness of their attacks, and the appearance of automatically propagating worms necessitated further measures.

Because worms are able to propagate very rapidly it is no longer effective to rely on the manual application of patches to systems to prevent infection. The time for a propagating worm to probe the entire Internet is measured in hours or even minutes with optimal search techniques, yet reactive system patching at best takes several hours and this extends to a day or two at weekends. To successfully combat worms it is necessary to anticipate their characteristics and deploy generic preventative measures in advance.

Most worms propagate via either email or websites. It is therefore essential to be able to intercept all email and all web browsing at the site periphery in order to screen out network packets carrying worms. This requires forcing all email to first pass through a single logical receipt service and for all external web browsing to be conducted via a proxy server. During 2001 both of these measures were enforced by appropriate blocks in the main site routers.

Once all the web and email traffic is being routed through specific machines it is possible to install screening services on those machines. These screens take two forms. The first is a standard virus checker, updated automatically at least daily and more frequently manually as necessary. This measure prevents known and established worms and viruses gaining access to the site by these routes. However, this alone is still not effective against new and rapidly propagating worms for which no signature is yet available in the virus scanners. To reduce the exposure to these it is necessary to screen out generically those file types which are likely to carry executable content. This is difficult for those file types which are likely to be transmitted as part of the normal business of the Laboratory, but a number of them, eg those used for screen savers, are not essential to business and may be blocked.

All these measures were introduced at CLRC during 2001. How successful have they been? In spite of these measures there have been a number of compromised machines within CLRC, but none of the compromises has been serious and none have propagated internally. Very little disruption to the work of the Lab has resulted from either the compromises or the preventative measures taken, and to this extent the adopted approach has been successful. We believe the balance between prevention and working restrictions is about right.

Developments

What is needed in 2002? There are some lessons to be learned from our experience, and some further precautions that will be needed to prevent intrusions by the more sophisticated techniques likely to be employed by intruders in 2002.

The first observation is that the essential security methods are technically complex and subject to human error. Most of the intrusions we have seen would have been prevented by the procedures outlined above, but mistakes, perhaps inevitably, were made by the people responsible for their implementation: filters in routers were installed incorrectly, system administrators failed to patch systems promptly or left services running which were not required, or misinterpreted often complex instructions regarding system patching. The lesson is that a single line of defence is inadequate. As many blocks, detection systems and protective measures as possible must be deployed. Externally facing servers must be combined to reduce their number and therefore also the number of staff involved in their maintenance, so concentrating the technical expertise where it matters.

Second, in addition to installing virus detection in all computers, relays and proxies it is now essential to install packet filters in multiple routers to safeguard against both human error and the subsequent internal propagation of infections should a system be compromised. This will require the reorganisation of the internal network to provide several levels of protection. In this respect the use of VLANs offers the simplest solution.

Thirdly, specific action needs to be taken to prevent infections of the more vulnerable home machines, visitor machines and laptops propagating should they be connected to the internal networks. Personal firewalls, specifically protected sub-nets and various security procedures all need to be considered and deployed.

All this in addition to maintaining all the virus checking, router filtering and security procedures already in place.

Conclusions

Computing never stands still, and that maxim applies just as much to hacking techniques and security measures as to any other aspect of computing. Continuous vigilance and continual change are needed to safeguard any system with Internet access. Maintaining adequate technical expertise in networking has never been more important. Achieving the right balance between freedom to exploit all features of the Internet and the restrictions imposed by essential security measures will remain a difficult technical challenge for research laboratories for the foreseeable future.

Please contact:
Trevor Daniels, CLRC
Tel: +44 1235 445755
E-mail: T.Daniels@rl.ac.uk

Secure Collaboration in Global Computing Systems

by Christian Damsgaard Jensen

SECURE is a newly started IST project, partly carried out at Trinity College Dublin, which addresses secure collaboration among computational entities in emerging global computing systems.

The properties of these systems introduce new security challenges that are not adequately addressed by existing security models and mechanisms. The scale and uncertainty of this global computing environment invalidates existing security models. Instead, new security models have to be developed along with new security mechanisms that control access to protected resources.

The past decade has seen the globalisation of the information and communication infrastructure. At the same time, distributed systems have grown from company-wide networks to include global federations of independent and separately managed systems, eg, the Internet. Computing and communication capabilities are increasingly embedded into everyday objects; this means that we will soon be able to interact with billions of 'intelligent' devices whose owners we do not know and which we should not necessarily trust. The scale of such global computing systems means that security policy must encompass billions of potential collaborators. Mobile computational entities are likely to become disconnected from their home network, which requires the ability to make fully autonomous security decisions; they cannot rely on a specific security infrastructure such as certificate authorities and authorisation servers. Although a public key infrastructure may be used to reliably establish the identity of other collaborators, this identity conveys no a priori information about the likely behaviour of the principal. Identity alone therefore cannot be used for access control decisions, ie, all participants are virtually anonymous. This fact excludes the use of most access control mechanisms currently in use on the Internet. The dynamism of global computing systems means that computational entities which offer services will be confronted with requests from entities that they have never met before; mobile entities will need to obtain services within environments that are unfamiliar and possibly hostile. A party faced with such a complex world stands to benefit, but only if it can respond to new entities and assign meaningful privileges to them.

The challenges faced by mobile entities in a global computing system are not unlike those faced by human beings confronted with unexpected or unknown interactions with each other. Human society has developed the mechanism of trust to overcome initial suspicion and gradually evolve privileges. Trust has enabled collaboration amongst humans for thousands of years, so modelling trust offers an obvious approach to addressing the security requirements faced by the global computing infrastructure. Trinity College Dublin leads the SECURE project, which aims to develop a new trust-based security model for global computing systems; other partners in the SECURE project are the universities of Aarhus, Cambridge, Geneva and Strathclyde. The aim of the SECURE project is to develop a formal model in which trust relationships may be established on the basis of interaction between entities, together with a security mechanism expressed in terms of the trust model.

Trust is an elusive concept that defies stringent definition. However, we conjecture that a notion of trust can be realised in sufficient detail to be operational for a specific purpose, namely as the underlying principle for a security mechanism applicable in a global context. Trust has been proposed as a mechanism for reducing risk in unknown situations. The explicit use of trust as a defining principle for security models and policy specification makes trust relationships among entities explicit. Trust thus becomes the commodity that allows an entity facing an interaction in an unfamiliar environment to weigh the risks associated with particular actions. Conventional security mechanisms express policy in terms of the privileges allocated to individuals; role-based access control introduces a level of indirection, in which privileges derive from roles, and policy determines which individuals may enter each role. In either case the mapping from the trust model to the risks inherent in the allocation of privileges is implicit. SECURE proposes to establish a trust-based security model in which computational entities interact on a basis of (mutual) trust.

Interaction between entities may take many different forms. It is worth looking at one form of interaction in more detail. Suppose that a mobile entity needs to obtain a service from another entity within an unfamiliar environment. The entity that offers the service can identify the potential client, but its attributes and probable behaviour are unknown. We assume here that the functions of the service are categorised and their integrity protected by role-based access control. The service allows the potential client to enter role(s) on the basis of their mutual trust. The client can then make use of one or more of the functions of the service. This may place the client under an obligation, for example to make a micro-payment. When the interaction is complete each party records their experience of it, which will include information about the behaviour of the other.

The experience recorded by the service can be used in at least three ways. First, the service performes some function for the mobile entity on the basis of trust alone; the service can learn from the interaction to evolve the mapping between trust and role. Second, the record can be transferred to the mobile client, which can use it as a recommendation when approaching other entities. Finally, the record is available as

evidence to modify the reputation of the mobile entity.

The accumulation of such experience is what allows trust to evolve. Trust is individually formed through an entity's observations of the behaviour of other entities; this allows interaction with unknown entities without prior configuration, a fundamental requirement for security in the global computing environment. In the scenario above we pictured a mobile client interacting with some service, but the essential feature is that the properties of each entity are unfamiliar to the other. The mobile entity will write its own account of the interaction, and may as a satisfied user offer it to the service. That record provides an alternative account of the interaction, and the combination of the two gives a lot of potential information.

Implicitly this scenario presents a rosy picture of a successful interaction, but a lot of things may go wrong. For example, the service may be performed imperfectly, or the client default on the payment in some way. Worse, the two entities may in fact be in collusion, and present fictitious but consistent accounts of the interaction in order to boost their joint reputation in the world at large.

The research presented above is defined in the context of collaboration among mobile users and intelligent devices in a global computing infrastructure. However, it is equally applicable to all areas with great risk and uncertainty and where it is difficult to establish a meaningful identity of other entities, eg, Internet collaboration, peer-to-peer networks, smart environments and e-commerce.

SECURE is a Future and Emerging Technologies project supported by the European Commission under contract IST-2001-32486.

Please contact:
Christian Jensen, TCD
Tel: +353 1 608 24 59
E-mail: Christian.Jensen@cs.tcd.ie

Integrating Biometric Techniques with an Electronic Signature for Remote Authentication

by Luca Bechelli, Stefano Bistarelli, Fabio Martinelli, Marinella Petrocchi and Anna Vaccarelli

Biometric technologies are currently used for physical access controls. Scientists at CNR aim to integrate this technology with certificates, signatures and smartcards to handle remote authentication.

A project is currently under way at IIT-CNR, in collaboration with two industrial partners, which aims at the integration of biometric devices with digital signature technology (in conformity with current Italian standards). The results of the activity are being tested periodically by other CNR Institutes interested in this technology. The main objective of the project is the definition of standards that guarantee:

- confidentiality of non-public information
- authentication of the entities involved in the protocol (smartcard, biometric device and the user)
- integrity of the messages.

A fingerprint template.

All these steps will be necessary to guarantee non-repudiation between authenticated users.

User authentication with biometric techniques does not require 'knowledge' of a secret piece of information, such as the traditional PIN, but requests that the user performs specific 'actions', necessary for a live acquisition of public biometric information.

This is why biometric techniques are used today for physical access controls or for other activities that require the presence of the user. The effective presence of the user during authentication guarantees that the biometric information is not intercepted, stolen or improperly used. Our aim is to perform remote authentication (eg logon to a remote system or unlock of a smart card to sign a document) and to guarantee the presence of the user by using special communication protocols between the biometric device and the smartcard.

The main problems with the use of biometric techniques are:

- the need to ensure that the only way to authenticate the user is the 'action' and not the 'knowledge' of the biometric information
- the association between biometric information and user identity has to be certified.

If these two constraints are not realised, a malicious user could use his own biometric details together with a third party identity (responsibility attack), or attach his identity to third party biometric information (credit attack).

In our work, the biometric information is represented by a fingerprint. During the enrolment phase, a fingerprint template of the user is stored in a secure environment (in our solution inside the smartcard). For integrity and authenticity purposes, the (hashed) fingerprint is then inserted in an 'attribute certificate' signed by an Attribute Authority. In the same smartcard we also store an X.509 certificate of the user, which will be used to digitally sign documents.

In order to validate the fingerprint-identity pair, two important pieces of information are added to the attribute certificate:
- the serial number of the smartcard (in this way the fingerprint can only be used with that smartcard)
- the serial number of the X.509 user digital certificate (in this way, the fingerprint can only be used together with its owner).

This type of solution guarantees:
- that the user can perform classical authentication (with a secret PIN) and use only his X.509 certificate
- the possibility of biometric authentication, and the use of the X.509 certificate for remote authentication and digital signature
- the possibility of only handling the biometric information locally and privately.

In conclusion, biometric techniques work well if the verifier can check two things:
- that the biometric information was supplied at the time of verification (livescan)
- that the biometric information matches the template on file.

If the system cannot do this, then it fails. In fact, biometrics data provide unique identifiers, but are not secret.

We intend to implement the specification described above using the hardware and software products of our industrial partners with template-on-card technologies.

We plan to extend the implementation employing Match-On-Card (where the extraction of the certificate is performed on the card and the match on the system) and System-On-Card technologies (where match, extraction and storage of the template are performed inside the card).

This work has been carried out within a scientific cooperation between IIT-CNR and BiometriKa, an Italian company.

Link:
http://www.iat.cnr.it/attivita/progetti/progetti.html

Please contact:
Stefano Bistarelli, IIT-CNR
Tel: +39 050 315 3438
E-mail: stefano.bistarelli@iit.cnr.it

Secure Resale of Tangible and Digital Goods

by Harald Häuschen

A secure transfer system for reselling physical and digital goods is being developed at the University of Zurich. The project is unique in its approach of dealing with security issues to support resale transactions between users with or without electronic marketplaces.

Today more and more resale transactions involving both physical and digital products are taking place between consumers, as well as between businesses and business customers, through electronic marketplaces or directly between users. The problem for the purchaser in these situations is that he/she does not know:
- whether the product exists
- whether the product may legally be traded
- whether the seller actually has all the necessary legal rights to the item offered for resale
- whether the purchaser him/herself will actually acquire all the legal rights to the item once the resale has gone through
- whether the holder can't sell the same product to several people.

Clarifying all of these points is not an easy exercise and most importantly, to date it has not been possible to automate this process. Trust, however, is important for e-commerce. Marketplaces need security support on all levels to increase trust for all transactions. To support secure resale transactions, we started a project in 2001 called eDOT (electronic document of ownership transfer system). The aim of this project is to build a system which allows a secure resale of tangible and digital goods. With help of this system, rights to physical and digital goods can be electronically documented, the product and its owner are clearly identifiable for all parties, the product and rights can be transferred without problems (ie, just for limited time period) and forgeries, as in the case of physical documents or products, are not possible. Moreover, the electronic document of ownership can be used at the same time for authentication and authorisation. The system is a

single component, which can be used to extend existing marketplaces.

Until now, customer uncertainty and lack of confidence are undoubtedly significant in the context of resale. It is important that potential customers feel sure that a one-off product they buy will actually belong to them once payment has been made and will not be re-sold several times over by the seller. A potential customer also wishes to be sure that the tangible goods or digital product really exists and may in fact be traded. Therefore the system consists of two essential components: firstly, an electronic certificate of ownership which confirms that the product exists and that it is owned by the person currently in possession of this product, and secondly, a component whereby ownership rights may be transferred securely and unequivocally under certain specified conditions.

The 'ownership certificate' allows the description of goods and the allocation of them to an owner. The main task of the transfer component, as a trusted entity, is to ensure the secure transfer of ownership together with the settlement of the corresponding payments. Security is guaranteed at various levels. The system is protected against forgeries after the ownership certificate is created. There is no risk of losing ownership and the system is clear and transparent, ie, all activities can be checked and understood by those involved.

To validate our approach we made a first implementation for an agent-based marketplace. Agents, on behalf of their originator, take over the task of looking for specific items, negotiating with their seller and concluding a deal. However, agents are not just limited to purchasing goods on behalf of users, since they too can act as sellers in that they can offer for resale goods that they themselves have purchased. Our first implementation shows that the use of the ownership transfer system could solve all the security problems without significantly changing a marketplace.

The project represents an important step forward that will enable secure and efficient business transactions involving multi-stage (intermediate level) trading to take place alongside direct sales channels. Implementation is simplified because existing systems only need to be modified and not replaced. At the moment we are defining a new component to support resale via mobile phones.

Please contact:
Harald Häuschen, University of Zurich
Tel: +41 1 635 43 11
E-mail: haeusche@ifi.unizh.ch

Managing Authorisations

by Babak Sadighi Firozabadi and Mads Dam

The problem of authorisation, delegation, and authorisation management in distributed systems has been studied at SICS for the last two years. Our main focus has been the development of a delegation logic which is based on the idea of delegation as the explicityet constrained creation of new privileges.

The Amanda project is the common denominator for a small collection of projects involving Microsoft Research, Cambridge, the Swedish Defence Material Agency, SaabTech Systems, and SICS. Over the past two years, a team of researchers have examined the problems of authorisation, delegation, and authorisation management in distributed systems.

A very topical issue is the establishment of Public-Key Infrastructures (PKI) as a fundamental basis for secure interaction on the web. Whereas the establishment of PKIs at the level of closed systems – individual organisations – is now to a large extent routine, significant problems remain to be solved at the level of open systems, slowing down the wider adoption of PKI in industry. Important factors are concerns related to certificate interoperability, certificate management, authorisation (roles and delegation) and organisational structure.

Important as it is however, in many Internet applications a strong authentication mechanism is not in itself the goal. Authentication is needed to support other functions such as authorisation and auditing. The development of authorisation and auditing mechanisms for distributed systems is currently a very active field of research. Traditional authorisation mechanisms are based on the Access Control List (ACL) model. The ACL model was originally designed for access control decisions in closed systems, and requires that a server know in advance the identities and the permissions of its clients. Such information is recorded in an ACL that is centrally administered. However the ACL model is fraught with problems, in particular as systems scale up and become deployed in increasingly open contexts. One set of problems concerns management, relations to organisational structure and the ability to easily adapt to changes on both individual and group levels. Moreover, in open systems, a server may not know who is the next potential client. Therefore solutions based on the ACL model are not suitable for authorisation mechanisms in Internet applications, and there is a need for a more generic and common framework for authorisation and auditing in open distributed systems.

The research field of 'trust management' provides the seed for such a

model. In trust management the core aspect of authorisation is to answer the following question: Does the set of credentials C prove that the request r complies with the set of local policies P? The local policies are the policies of a server that controls access to some resources, and a client provides – directly or indirectly – some credentials to support its request. These credentials will typically take the form of attribute certificates, digitally signed by trusted parties or empowered authorities.

A good delegation logic is a key component in such a framework, since delegation is the central mechanism by which administrative tasks and procedures are broken down into manageable parts. It is also in our opinion crucially important that a clear separation be made between administrative and executive powers. It is very easy to conceive of situations where a power to manage some administrative attributes of a given resource should be granted, but direct access to that resource should be denied. An example is outsourced management.

The main focus of the work at SICS has been the development of a delegation logic which is based on the idea of delegation as the explicit yet constrained creation of new privileges. We have examined the basic principles of such a model, considered the problem of revocation in this context, and produced a number of prototype implementations including adaptations to the ongoing work on SPKI/SDSI at IETF.

Links:
SICS Intelligent Systems Lab:
http://www.sics.se/isl/pbr
Amanda project:
http://www.sics.se/fdt/amanda

Please contact:
Babak Sadighi Firozabadi, SICS
Tel: +46 8 633 1582
E-mail: babak@sics.se

The Role of Smart Cards in Practical Information Security

by Javier López, Antonio Maña, Pedro Merino and José M. Troya

The GISUM research group at the University of Málaga is looking at the use of smart cards to increase security in different scenarios. The work is supported by the EU and the Spanish Ministry of Science. Some interesting results are represented by two recent projects. These are the eTicket project, which has defined and implemented a secure electronic ticketing procedure including related protocols and support services, and the Alcance project, which has developed a secure electronic forms framework for secure communication between citizens and the public administration.

The transition from traditional commerce to electronic and mobile commerce is fostered by aspects like convenience, speed and ease of use. However, security issues remain unsolved. Smart cards open new possibilities for the development of security schemes and protocols that can provide security in applications such as electronic payments or software protection where traditional cryptographic tools are not useful. The GISUM group is involved in several research projects that make use of smart cards. Current applications include a secure electronic forms framework for government-citizen relations, electronic ticketing systems for GMS phones and Internet, a PDA-based digital signature environment, public transport, access control systems, software protection and banking applications. This report focuses on two recent projects: the eTicket electronic ticketing project (1FD97 1269 C02 02 (TAP)), a coordinated project with the Carlos III University of Madrid; and the Alcance project, consisting of the development of a secure electronic forms framework for secure Internet-based communication between citizens and the public administration (1FD97 0850 (TIC)).

Electronic Ticketing

Ticketing services represent an attractive application that is both useful and convenient for the user. However, security features and greater flexibility are needed in order to foster their extensive use and popularity. Most of these services use a single value (usually a numeric code) to represent the ticket. In consequence, tickets can easily be copied or forged, it is impossible to represent different types of tickets, no delegation is supported and finally, the verifier needs to receive a database of tickets emitted before allowing clients to access the service. Our project therefore focuses on the following two points: the development of a representation for the tickets and the development of protocols and mechanisms for the use of the tickets.

After a careful analysis of the electronic ticketing requirements, the following goals were defined: versatility, compactness, security, payment, fast offline ticket verification, minimal number of messages emitted by users and ticket delegation. Our system is based on cryptographic smart cards which contain a key pair generated inside the card and which ensure that the private key never leaves the card. Each card will also contain a certificate of the public key

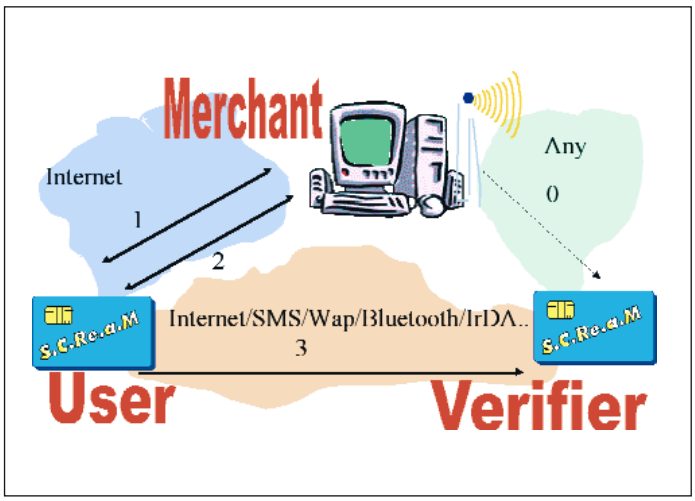


Figure 1: eTicket system architecture.

(signed by the card issuer), the public key of the card manufacturer and some support software.

Ticket merchants are assumed to have access to the public keys of all card issuers whom they wish to accept for the sale of the tickets (usually a small number). When the user requests a ticket from the merchant, an 'open' ticket (ie, one that is not associated with any user) is sent to him. Once the open ticket is received, the smart card verifies that it is correct, extracts the service identifier and authorisation components and stores them in its memory. The authorisation component includes, among other values, the number of closed tickets that the smart card is allowed to produce from that open ticket. To spend an open ticket the user must first close it, which is achieved by including some identification information for the spending of the ticket. This process must be done in the card of the user who bought the ticket from the merchant. Where the user and buyer of the ticket are different entities, we say that the ticket is delegated. Ticket delegation is possible because the software contained in the smart card is trustworthy. For the same reason, there is no possibility for the card to produce more closed tickets than are authorised.

The trustworthiness and the authenticity of the card software is guaranteed because the card issuer signs the public keys of the cards it sells.

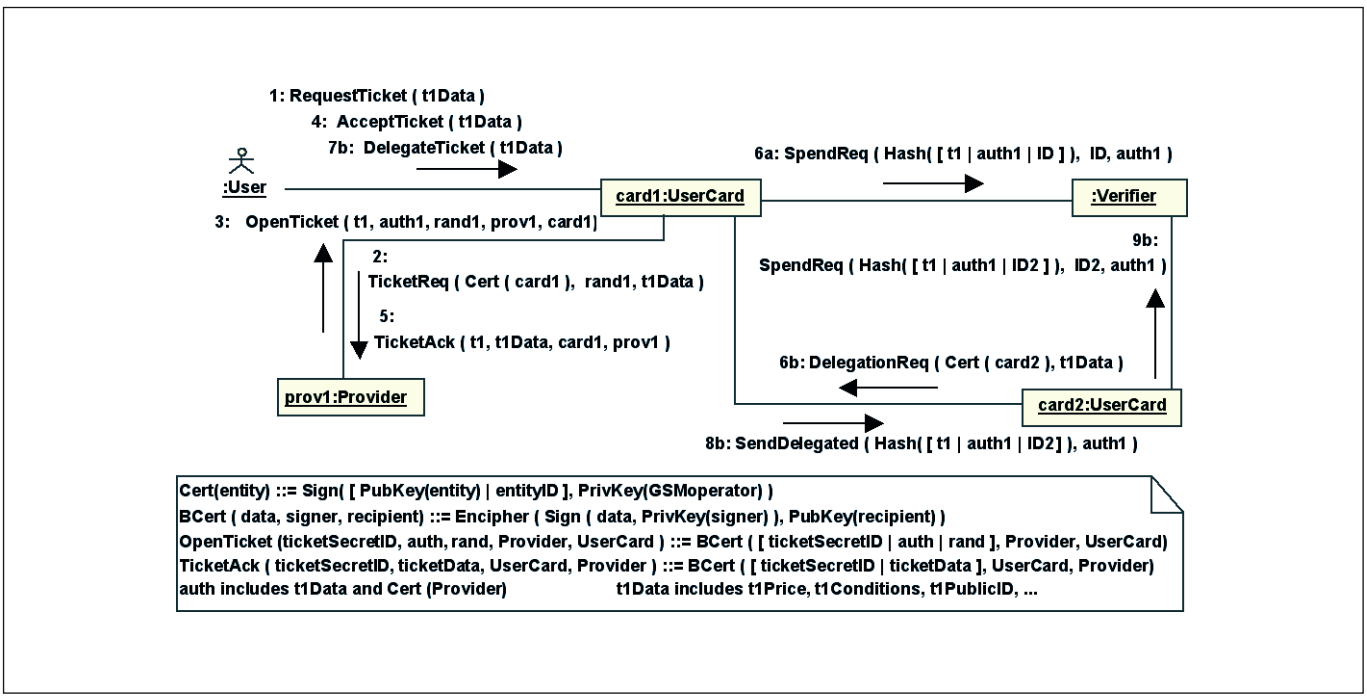
To spend the ticket the user presents the closed ticket to the verifier, providing evidence that he has received the secret service identifier. This is both a fast proof - the only operation involved is a hash - and a secure one, because it is not feasible for a dishonest user to produce the result of the hash operation without knowledge of the secret service identifier.

Secure Software Framework

For public organisations, a telematic version of administrative procedures would bring meaningful benefits concerning accessibility and availability of documents and services, regardless of time, location and quantity. While some implementations exist, a number of technological deficiencies hinder a higher degree of communication between administrations and citizens/companies through the Internet.

It is convenient to define models to include security properties into applications as well as components that have been already developed, and this must be fulfilled making small changes to the code.

The area of application of this project was determined by the computerisation of the Junta de Andalusia Sanction Procedures, which are associated with



Scenarios for ticket spending and delegation.

the Ground Transport Arrangement Law. More specifically, Alcance is being developed inside the Strategia Project, associated with the Works and Transport Council of Junta de Andalusia. The project involves several independent systems, with the Sanction System being one of the most important. Inside the Sanction System, the main task related to our research project is the design of a module which, by using Web browsers, will allow over fifty thousand private organisations and companies to track and transact the sanction files assigned to them in one or more sanction procedures. The module developed allows private organisations and companies, whose access is controlled by Web digital certificates, to monitor their files independently of location and time. Certificates on smart cards support the authenticity necessary for the communication between companies and the Council, and allow the exchange of signed official documents.

We have designed and developed a Form Description Language, called LDF, which is based on XML, and more precisely on XFDL. The use of LDF and related tools introduces many advantages in comparison with traditional use of HTML. Regarding forms status, it is easy to add new components not included in HTML. These new components can be useful for avoiding invalid inputs in the electronic forms, thus achieving a more dynamic management. Additionally, automatic data validation can be done without programming specific code for that operation, as the form specification includes the check itself. Regarding forms management, LDF includes the possibility of forms visualisation by using a traditional browser (for on-line operations) or an independent application (for any off-line ones). Signed forms management is easier, as signers can store in their own hard disk a copy of a partially filled document, which can be opened later for completion using a browser. Moreover, one or more users can sign forms that can be encrypted using unconstrained implementations of algorithms.

Regarding communication, a specialised format ensures the context of the signature is not lost, so that the authenticity of the data is never compromised. Besides this, the document is audited (persons involved, date of the agreement, etc) on its own. In contrast to HTML, LDF provides a data structure and separates application, presentation and logic levels.

Link:
GISUM research group:
http://www.lcc.uma.es/~gisum/

Please contact:
Javier López, Antonio Maña, Pedro Merino, José M. Troya, University of Málaga, Spain
E-mail: {jlm,amg,pedro,troya}@lcc.uma.es

Realizing Trust through Smart Cards

by István Mezgár and Zoltán Kincses

Trust from users is a fundamental element in network-based services. Building blocks of trust are different security mechanisms. A smart card (SC) is a device that can integrate different security mechanisms in a handy form, but interoperability problems can decrease its wide usability. Software reconfiguration can be a way to overcome this problem. A project has been started at SZTAKI to develop an ontology-based reference architecture that supports SC reconfiguration.

Trust and confidence are essential for the users of networked systems, as for all members of the Information Society. The lack of trustworthy security services is the main reason of not using the electronic and mobile technologies in private, business or in public services.

The basic term of trust means reliability in some person or thing, or to allow to do something without fear of the outcome. Trust is of different categories, eg, Impersonal/Structural trust, Dispositional trust, Personal /Interpersonal trust.

In order to motivate individuals to use a certain information system, users have to be convinced that it is safe to use the system, their data will not be modified, lost, used in other way as defined previously, etc. In case the individual has been convinced, one will trust the system and will use it.

Access control (identification), authentication, privacy, and confidentiality are services forming the sense of trust for a human being. To achieve these services three basic building blocks of security mechanisms are applied: encryption (for providing confidentiality, authentication and integrity protection), digital signatures (for authentication, integrity protection and non-repudiation), checksums/hash algorithms (for integrity protection and authentication).

Smart cards can become essential trust elements in a security infrastructure as they are able to integrate different security mechanisms besides the current application. They are efficient devices to execute security functions, such as digital signatures. The workable interoperability of technical and organizational frameworks and supporting infrastructures is a big problem, as the lack of them can decrease SC usability. Overcoming this problem can help the software reconfiguration.

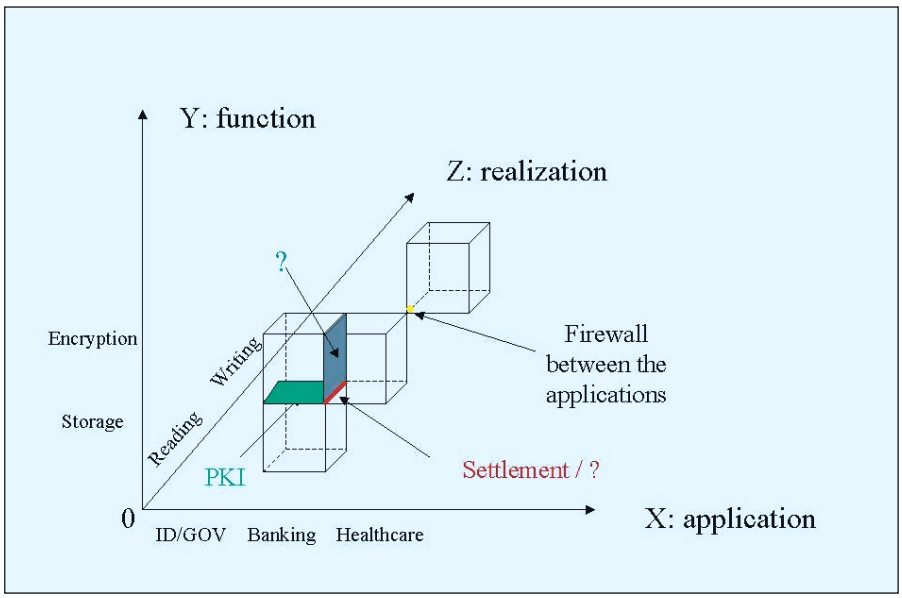
In the close future smart cards will have a role more important than today. Multifunctional cards can integrate different applications; identity card, bank-card,

health card, etc. They can be a key component for mobile phones used as mobile personal terminals, a personal trusted device (PTD).

The very broad field covered by the different applications needs different solutions for the expected functions of SCs. The way of identification (able-bodied, or handicapped), the different encrypting algorithms (strong/weak encryption) need different HW and SW solutions/configurations of the SC. The set of applications of a smart card can alter during its life cycle, so the SW configuration has to be modified. In these cases applications have to be added or removed, namely, the software of the smart card has to be reconfigured probably several times. Another demand is to have standardized interfaces to handle the different application software (interoperability), and standardized HW building blocks.

A balanced system means that the needed functions of the current application are realized with the optimal HW and SW. Optimal means to select the proper technical parameters with a combination of an economic financial solution. This demand needs a complex, flexible configuration that can be altered/modified according to the user's actual needs (eg geographic spot, new services). Defining this configuration is a real complex task, consequently, there is a need for a kind of structured description of the present (and possible future) requirements of the different applications, and of the HW and SW possibilities. This representation structure can be a reference architecture that is based theoretically.

The development of the reference architecture is going on in the frame of the project 'The Theoretical Elaboration and Prototype Implementation of a General Reference Architecture for Smart Cards (GRASC)', supported by the Hungarian Scientific Research Found (OTKA). The basic goal of the project is to produce a first qualitative version of a theoretical-based multi-view, multi-layer, multi-element description of SC functions, SW and HW systems and applications. This representation will be integrated, unified, consistent, and – very important – dynamic, as it will also describe the connections among the elements.



A three-dimensional graphical representation of a function – application – realisation architecture with reference models (represented by cubes).

The starting point of research was to develop a smart card ontology (SCO). Smart card ontology, this special structured representation is the guarantee for the full description of entities (applications and system elements), their levels and the logical connections between the levels and the entities. The main characteristics of smart card ontology are; the formalization level is structured informal/formal, the purpose of application is the interoperability among systems and it is domain ontology. As the description of SC ontology would well exceed the given extent of the paper, only a few elements of the SCO are introduced: meta-ontology (defines the basic terms of ontology), activities, functions, architectures and building blocks, applications, etc. There are further subgroups, numerous terms and definitions completing the ontology.

Based on the ontology, the number and content of the dimensions of the reference architecture (RA) can be defined. As a second step, discrete reference models (RM) can be allocated based on the RA. Based on the content of the RA sets of the reference models will be defined. It can be done based on the elements of the ontology taking the logical, functional and the derivative connections into consideration. Each RM is in a close, strict functional/logical contact with the neighbouring reference models. This results that the boundary communication between the RMs and the logic (I/O dataflow) of this communication can be defined exactly. Based on this knowledge exact protocols can be determined.The figure shows a three-dimensional graphical representation of a function-application-realisation architecture with reference models (represented by cubes).

The expected results of the GRASC are a structured description of smart card systems from different aspects, easy configuration/reconfiguration possibilities of SCs for different (multi) applications, and content/form of communication can be clearly described in case of different functions/applications.

Please contact:
István Mezgár, SZTAKI
Tel: +36 1 279 6141
E-mail: mezgar@sztaki.hu

Zoltán Kincses, SEARCH Laboratory,
Budapest University of Technology
and Economics
E-mail: kincses@mit.bme.hu

Phytoplankton Dynamics — the Struggle for Light

by Ben Sommeijer

A fairly realistic mathematical model describing the dynamics of phytoplankton was developed at CWI jointly with the research group on Aquatic Microbiology at the University of Amsterdam. One result negates a recent idea to reduce two environmental problems in one action.

The idea seemed attractive. Collect our scrap iron, and feed it to the tiny organisms in the oceans called phytoplankton. They love it and their population will grow on it. They love carbon dioxide too, extracting it from the atmosphere (the present intake is several gigatons per year). This carbon is transported downward by sinking phytoplankton species, and will eventually end up 'in the deep bosom of the ocean buried' – a mechanism called 'Biological Pump' (Figure 1) . Thus two birds would be killed with one stone: disposal of industrial waste and reduction of the greenhouse effect. Alas, the idea lasted as long as it remained qualitative. One of the studies with the mathematical model concerned, which is fairly realistic because it incorporates the most essential mechanisms, explains the recent field observation that iron fertilization fails to enhance carbon export to the deep ocean.

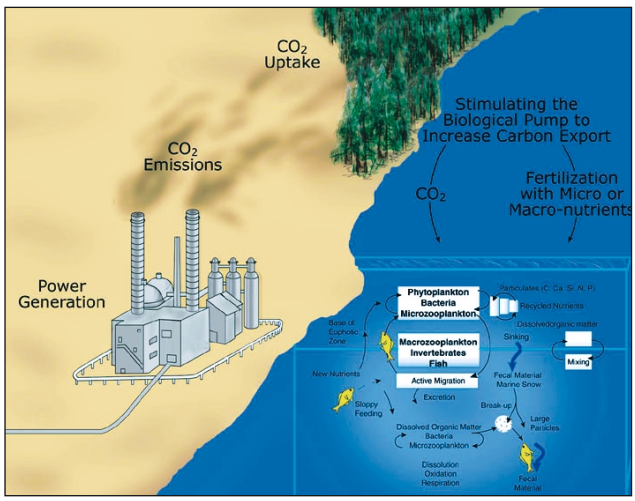


Figure 1: CO_2 is emitted into the atmosphere by several sources. Uptake of CO_2 by the ocean is enhanced through stimulation by fertilizers of the Biological Pump. Source: DOE Center for Research on Ocean Carbon Sequestration.

Phytoplankton is a generic name for a great variety of micro-organisms (algae) that live in lakes and oceans. Modelling its dynamics is of great interest, since phytoplankton provides the basis of the food chain. Phytoplankton requires light for photosynthesis. In a water column, light intensity decreases with depth, due to absorption. As a result, the phytoplankton production rate, which is determined by the local light intensity, decreases with depth. Furthermore, mortality rates and transport by turbulent diffusion in a water column (mixing) play a role. Also, phytoplankton species often have a specific weight different from that of water, giving rise to vertical transport in the form of sinking or buoyancy. All these processes are incorporated in an integro-partial differential equation of advection-diffusion-reaction type describing the population dynamics of phytoplankton. On the basis of this model we developed both analytical and numerical tools for several studies. One result is that the long term survival of a particular phytoplankton species ('bloom development') crucially depends on the mixing rate, the water column depth and the vertical velocity. Another result is that the maximal sinking velocity of phytoplankton that can be sustained is inversely proportional to the water turbidity. Hence the downward flux of phytoplankton biomass is very different for clear and for turbid water, explaining why iron fertilization does not enhance downward carbon transport (see Fig. 1). Since there are thousands of different phytoplankton species, slowly drifting in lakes and oceans (Figure 2), a natural extension of the model is to systems in which various species are competing. Buoyant species seem to have an advantage over sinking species since they can easily reside in the well-lit upper zone close to the water surface, and hence capture a lot of light. Moreover, they have the additional advantage to shade other species at deeper levels. Nevertheless, as it turns out, the balance between survival and death for the various species is very delicate and depends on values of other parameters as well, such as background turbidity, incident light intensity, and specific light attenuation coefficients of the different species.

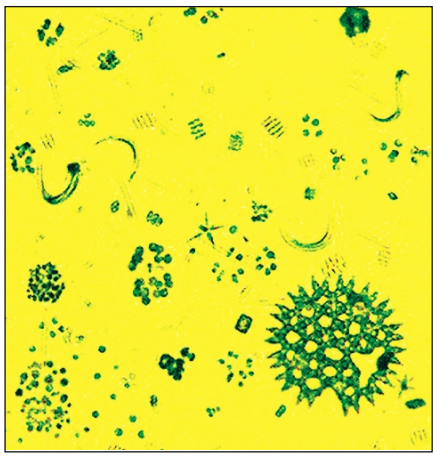


Figure 2. The several thousands of phytoplankton species have very different shapes. Source: Dr Petra Visser, IBED - Aquatic Microbiology, University of Amsterdam.

Link:
http://www.cwi.nl/projects/plankton

Please contact:
Ben Sommeijer, CWI
Tel: +31 20 592 4192
E-mail: B.P.Sommeijer@cwi.nl

Virtual and Interactive Environments for Workplaces of the Future

by John Wilson

VIEW is an ongoing R&D project, involving three ERCIM members and addressing best practice in integrating Virtual Environments within industrial product development, testing and training for workplaces of the future.

Work of the future, in industry and in commerce, will have an increasing array of technical systems available, of ever increasing sophistication and improving functionality. These new technical systems, however, will be of no value and may prove even disruptive or harmful if they are not implemented with proper understanding of their capabilities and of the human and organisational issues surrounding their use.

'Virtual and Interactive Environments for Workplaces of the Future' (VIEW) is a EU-funded research and development project that addresses these requirements in the particular context of Virtual reality technologies and virtual environments. The Project started in January 2001 and will be completed at the end of 2003.

The overall aim of VIEW is to develop best practice for industrial implementation and use of virtual environments, and integrate Virtual Environments in product development, testing and training for workplaces of the future. The main project objective is to face the numerous questions that arise from the lack of appropriate guidelines and standards on best practice implementation and use of Virtual Environment (VE) technologies. Moreover, VIEW focuses on initiating and supporting the integration of VEs in product development, testing and training processes, as well as on the broad adoption of VEs in European industries. In this context, the VIEW Project aims to develop essential technologies, methodologies and tools that will enable the industry to develop and use VEs in an appropriate way. In order to achieve this goal, the project will:

- study and analyse the impact of VEs on their users
- identify potential barriers for industries in making use of VEs
- provide guidelines and strategies to overcome those barriers
- use its findings in practice for designing appropriate VE workplaces
- provide tools and guidelines for industrial users so as to make appropriate use of VEs.

The project will review existing and emerging VE systems and applications and will establish a user forum to facilitate the conduct of surveys of VE users, in order to identify user requirements. A usability test battery will be developed to capture physiological and cognitive aspects of the impact that VEs may have on end-users. The project will also develop new, multi-modal, mobile and multi-media interfaces by combining different input/output (I/O) modalities, as well as new intuitive navigation and manipulation concepts. Those interfaces will be implemented and tested in various pilot applications, which will allow reliable evaluation of the usability test battery, as well as critical assessment of interaction concepts, devices and design guidelines. The evaluation process will cover several topics, such as the ergonomics of VE technology; issues of usability, health and safety; socio-economic impact for users and society; appropriateness of the VE technology to meet user company needs; gains in terms of work effectiveness and quality.

The knowledge and experience acquired during the project will be analysed and reported in a code of good practice, which will allow the application of practical and validated guidance to the selection, design, implementation and use of VE systems in different types of workplaces and for different needs. This code of good practice will be integrated into an interactive design support tool, which will provide the knowledge developed by the project (guidelines, code of good practice, best use guidance, examples, etc.) to decision makers, VE designers, developers and users in an appropriate way and format.

Virtual environments for workplaces of the future.

The VIEW of the Future Consortium includes three ERCIM members, namely the Fraunhofer Institute for Industrial Engineering (IAO) (with the role of Technical Coordinator), VTT and ICS-FORTH. Other consortium partners are: University of Nottingham, United Kingdom (Administrative coordinator); University of Stuttgart Institute for Human Factors and Technology Management (IAT), Germany; Suomen WINTEC Oy, Finland; John Deere, Germany; Alenia Spazio, Italy; Volvo, Sweden; PSA Peugeot Citroen, France; Center of Applied Technologies in Mental Health (COAT-Basel), Switzerland; Institute of Communication and Computer Systems of the National Technical University of Athens (ICCS-NTUA), Greece.

Link:
http://www.view.iao.fhg.de/

Please contact:
John Wilson, University of Nottingham, UK
Tel: +44 0 115 9514004
E-mail: John.Wilson@nottingham.ac.uk

Blind Image Analysis helps Research in Cosmology

by Emanuele Salerno, Luigi Bedini, Ercan Kuruoglu and Anna Tonazzini

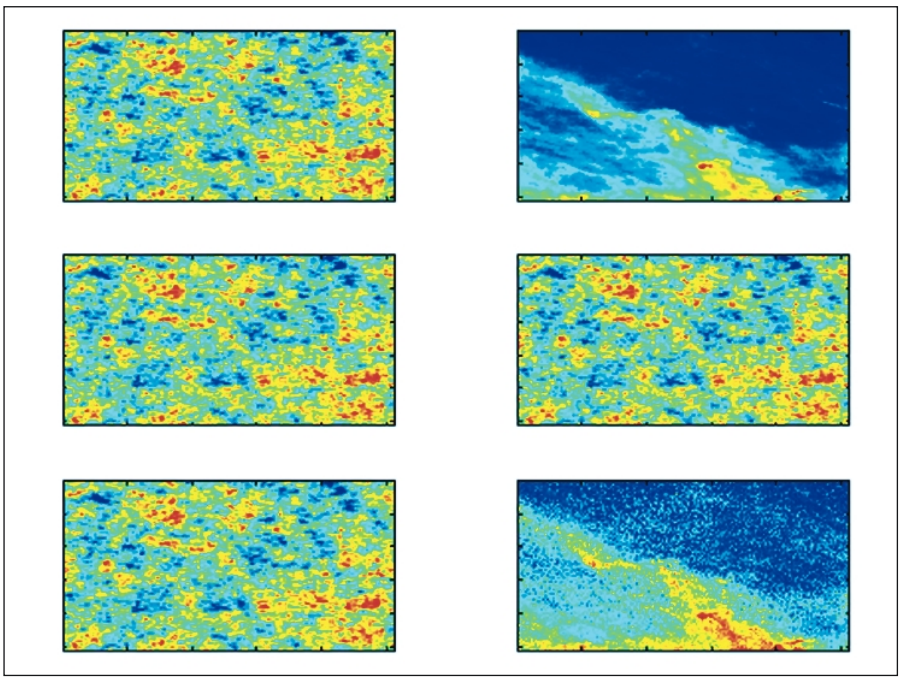
Blind image processing techniques are being studied at IEI-CNR, with the aim of extracting useful information from satellite radiometric maps of the celestial sphere. This activity is undertaken on behalf of the European Space Agency Planck Surveyor Satellite programme.

The Planck mission, to be launched in February 2007, will produce a very large amount of data, in the form of maps of the entire celestial sphere in the millimeter and submillimeter-wave bands. Its main goal is to map the cosmic microwave background (CMB) anisotropy with unprecedented angular resolution and sensitivity. It is known that CMB is a relic radiation coming from an epoch very close to the big-bang. Studying its anisotropy will provide important information on the origins and evolution of the universe.

The antenna temperatures measured by the satellite-borne radiometers are generated both by CMB radiation and by other astrophysical processes, whose effects are superimposed on the maps. Whereas the interest of cosmologists is focused on CMB, all the processes mapped are of interest in astrophysics and should thus be separated out.

The problem can be briefly formulated as follows: the data set is given by a number of sky maps, each on a different frequency channel; each map is a linear mixture of the maps related to the individual physical processes (source processes); the mixing coefficients depend on frequency through the source emission spectra and the frequency responses of the radiometers over the different measurement channels. Our objective is to separate the individual sources from knowledge of the mixed maps on all the channels.

There are two main reasons why this is difficult. First, the mixing coefficients are normally not known; second, the sensor noise is expected to be particularly strong because of the very small quantities (tens of microkelvin) that are to be measured and nonstationary, due to the uneven sky coverage of the Planck telescope scanning strategy.



An example of separation of two source processes from their mixtures over two measurement channels. Top row: simulated CMB anisotropy (left) and galactic dust radiation maps, assumed as original source processes. Middle row: noisy mixture maps. Bottom row: estimated sources.

One approach to this problem assumes that the mixing coefficients are perfectly known. However, this does not guarantee a good result, especially when the matrix assumed is significantly different from the actual matrix and the noise is particularly strong. The ideal solution should come from a totally 'blind' approach, ie, from trying to estimate both the source maps and the mixing coefficients from knowledge of the measured data alone. Clearly, this is not possible, since the problem is underdetermined, but the data model (ie, the mixing coefficients) is not the only place where we can exploit prior knowledge. Indeed, the different radiation processes in the sky are very likely to be statistically independent. Moreover, with the exception of the CMB, the different radiations can be modeled as nongaussian processes. The Independent Component Analysis (ICA) principle states that, if a number of independent random processes are linearly combined, a linear operator can be applied to the mixed data in order to obtain independent outputs. If all the source processes, except at most one, are nongaussian, the outputs of the linear operator are copies of the original source processes. On the basis of this principle, or an equivalent one, different blind separation approaches can be adopted. These approaches are characterized by explicit or implicit assumptions on the component distributions and in the inclusion of noise in the data model. At our Institute, a neural algorithm for blind separation has been experimented on data sets simulating the Planck instrument output, giving good results for uniform low-level noise. Successively, a fast non-neural algorithm (Noisy fastICA) has been applied to separate the sources from the same data sets with a higher, but still uniform, noise level. The latter procedure

is now under experimentation by astrophysical research teams in the Planck collaboration.

We are now focussing on the modelling of nonuniform noise and the estimation of the source statistical distributions. We are experimenting with the recently proposed Independent Factor Analysis (IFA) approach for this purpose. Before estimating the data model, this technique learns a statistical source model, thus enabling a more accurate estimation of both the data model and the original source maps. An interesting feature of this approach is that prior information can be inserted easily into both the data model and the source distributions. This means that the IFA approach can be made only partially blind, since it is able to exploit both the simple independence and any additional information available, thus providing a better solution.

Please contact:
Emanuele Salerno, IEI-CNR
Tel: +39 050 3153137
E-mail: salerno@iei.pi.cnr.it

Relativistic MHD Computation of Gamma-ray Bursts

by Barry Koren

Gamma ray bursts constitute the most energetic events in the Universe so far. Their nature is still a mystery. Recent observations enable comparison with model computations. CWI develops numerical methods to solve the relativistic equations of magnetohydrodynamics (MHD) underlying such models.

A gamma-ray burst hit the Italian-Dutch Beppo-SAX satellite for about 80 seconds on February 28, 1997 (Figure 1). Its monitor accurately measured the position of the burst, and within eight hours the spacecraft's x-ray telescope found a rapidly fading source of x-rays on the spot. Never before a burst had been pinpointed so accurately and so quickly. Subsequent observation with the powerful Hubble Space Telescope in the optical domain revealed a bright spot surrounded by a somewhat elongated background object (Figure 2). The latter is believed to be a galaxy. If so, it must be near the edge of the observable universe, and the gamma-ray burst represented the most powerful explosion observed thus far. Such bursts emit within the span of minutes or even seconds more energy than the Sun will in its entire life. Since their (accidental) discovery in the late 1960s, their origin and incredible energy remain a mystery. One scenario is a collapsing binary neutron star system, where gravitational energy is converted into kinetic energy of an expanding cloud of protons moving at relativistic speeds. Gamma rays are then generated by electrons accelerated by the intense electromagnetic fields occurring in shock waves. These waves result from collisions inside the proton cloud as well as with the surrounding gas. This scenario with shock waves implies that gamma-ray bursts are followed by long afterglows of x-rays and visible light. The burst of February 1997 provides strong evidence for such a tail.

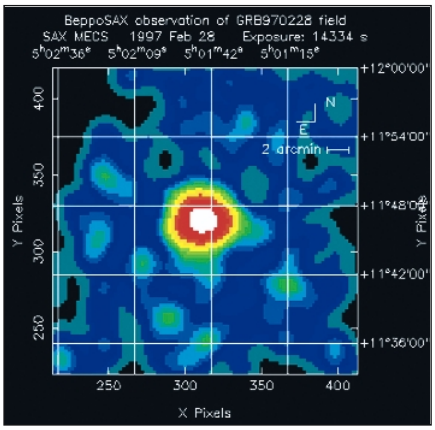


Figure 1: Gamma-ray burst GRB970228. Beppo-SAX team, Agenzia Spaziale Italiana, ESA.

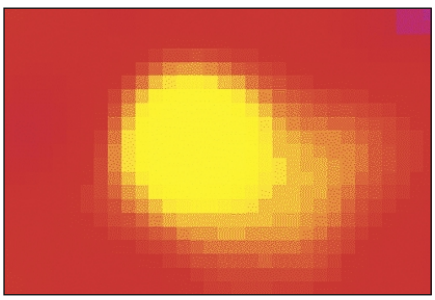


Figure 2: GRB970228 housed in a galaxy? Team of J. van Paradijs, Hubble Space Telescope, NASA.

Since experiments are impossible, insight into the nature of gamma-ray bursts can only be attained by solving the full relativistic equations of magnetohydrodynamics (MHD). At CWI the Computational Fluid Dynamics group addresses this problem, with partners at the University of Utrecht (Astro-Plasmaphysics) and the Institute for Plasma Physics in Rijnhuizen (Numerical Plasma Dynamics). As a first step, a computational method is developed for the relativistic equations of gas dynamics, which form a system of hyperbolic partial differential equations. A tailor-made discretization will take into account the different propagation velocities of rarefaction waves, shock waves, and contact discontinuities. An approximate Riemann-solver will be derived, as well as a staggered-grid approach. These two methods will be tested against a highly relativistic spherical explosion, for which an exact solution exists, thus serving as a severe numerical benchmark. After having passed this test, and a few others, electromagnetic effects will be incorporated and the second step of solving the relativistic MHD equations will be made. This system of equations is still hyperbolic, but its wave patterns are more complex. For its numerical solution approximate Riemann solvers and a staggered-grid approach will be developed as well. CWI's research contribution is crucial for the further development of large-scale computer codes in astrophysics.

Please contact:
Barry Koren, CWI
Tel: +31 20 592 4114
E-mail: Barry.Koren@cwi.nl
http://www.cwi.nl/~barry/

The CORVAL2 Contribution to achieve Confidence in Middleware

by Ina Schieferdecker, Axel Rennoch and Dorota Witaszek

The European Commission has initiated the development of a conformance test suite for the validation of Common Object Request Broker Architecture (CORBA) infrastructure products. Investigations of enhanced techniques for CORBA validation is the core of the CORVAL2 project.

Any software user knows about instable software programs. Today we are software users in many life situations: eg, if we are customers of a (real or e-commerce) shop or travel agency, users of any communication system, players of electronic games, and even passengers of a (private or public) transport vehicle. The utilization of this software provides benefits and comfort to its users, as long as they trust the system and/or services. It is not necessary to go into psychological details to understand the increasing stress if software behaves different to its declared expectations, or more formally: if the software does not conform to its specification.

What gives a user the trust in software? First of all, there will be her experience of availability and reliability. But, what if she is lacking these experiences? The situation may be even more difficult: what do users perceive and think, if they are exposed with a particular application, eg in the Internet? In almost all cases there is a complex system behind, which is layered and often distributed with a set of different services involved. And it seems obvious that end-user may avoid an application, if it is embedded in a faulty system. That leads to the view that middleware, which is the ability of computer programs to make use of any service implemented on heterogeneous hardware or operation system, is a technology which is crucial for software applications and needs to be verified carefully.

In the telecommunication sector it is well accepted that the efforts for testing may cover up to 50% of the complete development process, since the service reliability is an extreme critical point. During the last decades an elaborated Conformance Testing Methodology Framework (CTMF) [ISO/ITU-T and ETSI 1997] has been developed and established in this context. But its applicability appears to be much more general.

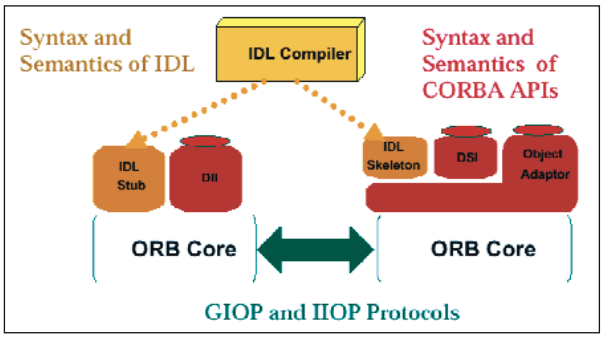
In January 2000 the EU commission started funding the R&D project CORVAL2 to enhance confidence in software quality in the realm of middleware. The target of this initiative is the conformance of the Common Object Request Broker Architecture (CORBA) based infrastructure for interworking in computer networks towards its international requirement specification [CORBA standard V.2.3, OMG 1999]. The idea is to enhance software reliability due to the application of high-qualified technical tests.

Due to the nature of the CORBA middleware, any conformance testing of the CORBA infrastructure will focus on the interaction between a service user or provider and the CORBA infrastructure. Further, the communication within the CORBA entities across soft- and hardware boundaries is subject of testing. The major testing aspects in CORBA are:

- the provision of a specification-conformant user interface (API)
- the verification of the standardized translation of CORBA interface definitions (IDL) into the target language of the Application Programming Interface (API)
- the protocol-conformant data-exchange between CORBA Object request broker (ORB) entities on different platforms or systems.

Obviously, these aspects cover a large field of conformance aspects and testing technologies: operation-based interface testing, compiler testing, and protocol conformance testing.

The major outcome of CORVAL2 is the availability of the conformance test suite for both C++ and Java API language binded CORBA ORB implementations. The total amount of test cases is very large, it varies on the conformance testing aspect to be verified: the numbers for the C++ test suite are for example: 400 syntax tests and 380 dynamic behaviour tests with reference to the IDL compiler output, 1240 API declaration tests and 470 API semantic behaviour tests, and about 150 tests on GIOP, the protocol definition for the inter-ORB communication. The different numbers are due to the different testing purposes. The high number of API declaration tests, for example, is reasonable due to the various features an API provides to an user (member functions, class inheritance etc.).



Corba conformance aspects.

The beta version or the test suite is available for inspection and download via the CORVAL2 project web site. Due to the

IPR ownership, the test suite is publicly available, but the Open Source License does not apply. In CORVAL2, the test suite has been applied for the different CORBA ORB products, which are available among the project partners. Some failures have been identified during this test campaign, eg, incorrect extraction/insertion of CORBA: Any types or wrong GIOP codings.

The big volume of the test suite and the level of details of the tests give reasons to trust the quality of the System under Test (SUT) which have passed the conformance tests. But this technical argumentation might be sufficient for the technical engineers only and not to the end user of CORBA middleware. Therefore a Brand program has been started in October 2001 to give vendors the opportunity to prove the application of the tests to their CORBA ORB product. Branded ORB products will get a certification document and logo for promotional usage. If any deficit has been discovered within the SUT (due to the application of the conformance tests) the granularity of the test suite allows identifying and correcting the failure.

The partners of the project are: The Open Group, Reading, UK; Fraunhofer FOKUS, Berlin; IONA - Object Oriented Concepts, Karlsruhe, Germany; Fujitsu - ICL, Dublin; Eric Leach Marketing Ltd., London; Object Management Group, Inc., Needham, MA, USA.

Links:
www.opengroup.org/corval2
www.fokus.fhg.de/tip/corval2/CorbaTests

Please contact:
Ina Schieferdecker, FhG FOKUS
Tel: +49 30 3463 7236
E-mail: schieferdecker@fokus.fhg.de

COVAX: an Internet Access to Libraries, Archives and Museums

by Luciana Bordoni

COVAX is testing the use of XML to combine document descriptions with digitised surrogates of cultural documents. The aim is to build a global system for search and retrieval, increasing accessibility via the Internet to the digital collections of memory institutions regardless of their location.

The objectives of the EU-funded COVAX project are:

- to build a web service for search and retrieval of contemporary European cultural documents from memory institutions
- to make existing library, archive and museum document descriptions accessible over the Internet
- to assist memory institutions to provide access to their collections, regardless of document type or collection size
- to implement standards and achieve interoperability between retrieval systems operating in the cultural heritage area.

Partners in the project include technology developers and providers (public research organisations and private companies) and content owners (memory institutions). The content owners have collections of varying type and size, catalogued using a variety of library, museum and archiving systems. The project is assessing ways to improve access to these collections by converting samples of existing data into a limited set of common structured formats, each of which can be expressed using XML (eXtensible Markup Language).

According to the philosophy adopted by the project, future catalogs for libraries, museums and archives will be stored in a variety of XML formats instead of proprietary formats, or formats such as MARC which have not gained wide acceptance outside of their development context. Since much material is already described in machine-readable form, the project worked on developing tools to convert such descriptions to XML and to integrate them with native XML data in order to build user-friendly websites and data archives.

COVAX is converting existing files into homogeneously-encoded document descriptions of bibliographic records, archive finding aids, museum records and catalogs, and electronic texts using XML and adapting the different document type descriptions (DTDs) currently used for library cataloguing (MARC), archive finding aids (EAD), museum data (AMICO DTD) and cultural texts (TEIlite). COVAX is designed to form a network of XML repositories structured in a distributed database and will act as a meta-search engine, offering access to all types of cultural data.

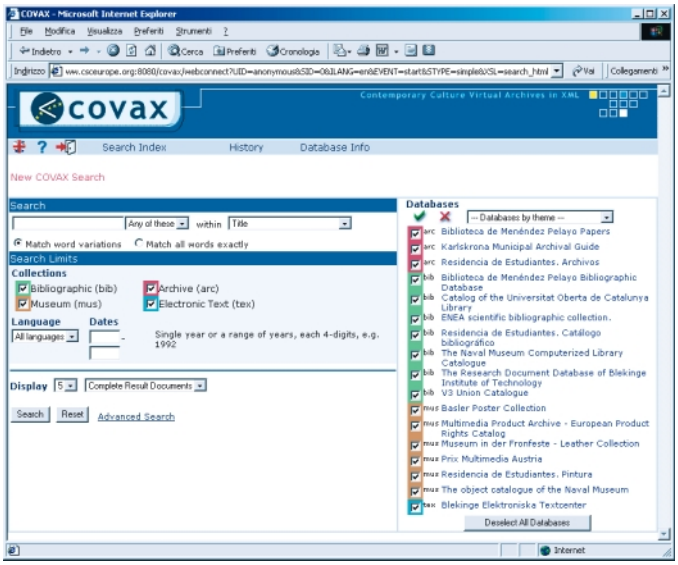
The COVAX system has implemented a multilingual user interface to access different data (catalog records, finding aids….) and documents (manuscripts, electronic texts, images, etc). The project is not creating new standards but will adopt existing standards and concepts (XML, existing DTDs, http…). The Z39.50 protocol provides a conceptual basis for communication between the multilingual user interface and meta-search engine and Dublin Core Metadata Element Set elements as cross-domain access points.

A comprehensive set of documents for the implementation of the prototype was selected. It contains a wide variety of documents, descriptions, formats and databases: standard and non-standard bibliographic records (including five different MARC formats), four different structures for archive and museum

finding aids and information in six different languages (Catalan, Italian, English, German, Spanish, Swedish).

COVAX is intended to satisfy the needs of the general public as well as professional users. User requirements are basically structured around these criteria:

- the user must be able to select any or all of the COVAX databases for his/her search
- the user must be able to select any or all document types for his/her search
- the user interface must permit simple searches, suitable for the general public, or more complex searches, for specialised users.



Search in the COVAX Prototype.

COVAX partners have implemented two different database models: ad hoc XML databases, or existing non-XML repositories. In the latter case, information is retrieved from the original database and transformed into XML format before presenting it to users. To summarise, COVAX is not only incorporating XML as a basic standard but also integrating other standards, and adapting them to XML.

COVAX partners have implemented XML repositories using two software packages, Tamino from Software AG, a COVAX technical partner and TeXtML from IXIAsoft. Sites have been established in London, Rome, Salzburg, Graz and Madrid.

COVAX will test the benefits of XML to encode and process cultural heritage information, explore the feasibility of converting existing cultural heritage descriptions into XML encoded information, adapt cultural information systems to user requirements and contribute to the extension of standards for presentation and dissemination of cultural heritage.

Ultimately, it will enhance access to cultural heritage (one of Europe's most important competitive advantages) for all citizens.

Link:
http://www.covax.org/

Please contact:
Luciana Bordoni, ENEA/UDA, Italy
Tel: +39 06 3048 3503
E-mail: bordoni@casaccia.enea.it

A Cluster of European Projects on Agents and Middleware Technologies

by Massimo Busuoli and Emanuela Rasconi

European Take-Up of Essential Information Society Technologies – Agents and Middleware (EUTIST-AMI) is a cluster of 13 different application-oriented projects that aims at demonstrating the potential of agent-based systems and middleware technologies when applied to real industrial environments.

EUTIST-AMI started in July 2001, and is intended to create a replication effect in order to push the use of these technologies within European industry. EUTIST-AMI, coordinated by ENEA UDA (Italy) in collaboration with LogOn (Germany), CSIC (Spain), SZTAKI (Hungary) and DFKI (Germany), will last for three years and its purpose is to improve the efficiency of the management and the dissemination of the results deriving from the 13 projects within the cluster. It also helps emphasising the European dimension of the projects. A key benefit of the cluster is the ability to coordinate dissemination activities. As the results of the individual projects become available, the coordinators will organize European wide dissemination campaigns. These will focus on success stories of the projects, in order to show other potential users the benefits that these two types of technology can offer.

The effectiveness of the message is also reinforced by the fact that the 13 projects are realized by partners coming from nine different European countries: Italy, France, Hungary, Switzerland, Austria, Germany, United Kingdom, Sweden and Spain.

Each project represents a real example in which agents and middleware technologies are used to solve problems relevant to a different industrial area. For example, in MODA-ML (a project realized by a Franco-Italian consortium) the problem of the data exchange in the supply chain of the textile sector will be addressed by providing a common language based on XML technology (one of the main languages used to realize middleware tools). This will allow the electronic exchange of data or documents (such as orders, technical documents, and administrative information). This should lead to a five to ten fold reduction in costs compared to the processing of paper documents.

In the medical sector, the MOWGLI project (realized by an Italian consortium) will use middleware to process patients' data. This involves the retrieval and exchange of all of the heterogeneous information (such as patients' demographic data, the allocation of diagnostic machines, and diagnostic exams, reports, and images) which is generated in a radiology department by patients from the time they enter the hospital until they leave. The information related to the individual patients will be available in electronic format and in a secure and confidential way through the Web. This will reduce to zero the use of paper for exchanging information between administrative, clinical and diagnostic staff, allowing the possibility of real-time feedback from a radiology examination.

A good example of the use of agent technology in the public administration is the CASSY project (realized by a German consortium) in which agent technologies are used to create a virtual receptionist that will provide the citizens of a German city with administrative information and personal assistance. The receptionist is able to answer requests made by citizens in natural language thus easing the problem of navigation within the web site and reducing the level skills needed to interact with the site.

These are only three examples from the 13 projects; more information about the other projects and the cluster as a whole can be found at the EUTIST-AMI website. EUTIST-AMI is funded by the European Commission within the Information Society Technology initiative of the Fifth Framework Programme.

Link:
EUTIST-AMI:
http://www.eutist-ami.org

Please contact:
Massimo Busuoli, ENEA UDA-Agency
for Sustainable Growth, Italy
Tel: +39 051 6098 178
E-mail: busuoli@bologna.enea.it

László Kovács, SZTAKI
Tel: ++36 1 279 6212
E-mail: laszlo.kovacs@sztaki.hu

Jalios: Master your Content

by Vincent Bouthors

Jalios is a recent spin-off company emerging from the joint INRIA-Bull Economic Interest Group 'DYADE' . The company develops and provides innovative content management software.

Jalios has been created in December 2001. This spin-off from INRIA (Rocquencourt) and Bull develops and provides a content management software which is the result of a cooperation between INRIA and Bull organized through DYADE, a GIE (Economic Interest Group). Jalios is the third company resulting from this fruitful cooperation.

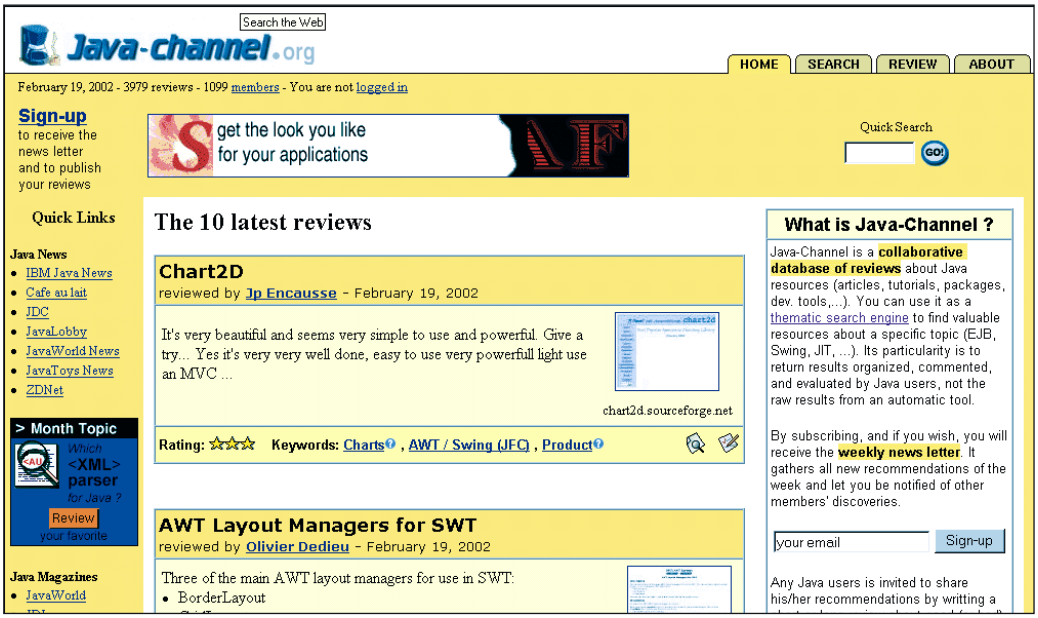
A Project: Pharos

Jalios has its origins in the INRIA project Pharos, which developed a collaborative infrastructure for web knowledge sharing. This project had two goals: the first goal, at the application level, was to build a collaborative recommendation service; the second goal, at the technical level, was to design a replication mechanism supporting disconnected replicates. The application Pharos was primarily targeted at internal use, to take more benefit of the resources available from the web. Today, web sites based on this application are still of great interest and used either by technical contributors such as java-channel.org (http://www.java-channel.org/) or by communities of interest such as educadoc (http://www.educavie.francetelecom.com/), a French thematic index of Web resources for teachers by teachers.

The database replication mechanism was intended to allow any kind of topology and to allow to perform updates in each replicate even if not connected. This is of interest for nomad users willing to update their data (on their replicate) on their laptop while being on the road as well as for confidentiality and security reasons in defense or national security businesses. The work, conducted in a thesis, has lead to the definition of a framework for optimistic replication. The main problem was to handle synchronization between replicates: to detect conflicts, to solve those which can be solved automatically, and notify users of the other conflicts. Detection of the conflicts is achieved by the framework: the developer can program conflict resolution either by choosing default algorithms or by developing some others according to the semantic associated with the data. This main functional innovation has involved the INRIA research group SOR (http://www-sor.inria.fr/).

From Research to the Product

A light object-oriented data-base was developed to support the application and



www.java-channel.org is an example of a website based on the Pharos application.

to prototype the replication protocol. This data-base is very similar to an explicit persistence mechanism: all basic operations (creation, update, deletion) are stored in a journal in XML format. This native in-memory data-base appears to offer obvious benefits for the developers: it makes programming very intuitive and it reduces drastically the need to perform request to retrieve data. On the other side, memory size and loading time of the database when rebooting the server are obvious limitations, but not for most of the applications : multimedia information are stored in the file system not in the data-base, and RAM is cheaper every day. Since the collaborative recommendation application had shown a need to share other kind of information we have decided to design a generic content management application, and to use the light object-oriented data-base as its kernel.

There are a lot of competitors in the domain of content management. Like other content management applications, Jalios handles independently content and presentation ; it takes use of the structure of objects to make easier multiple contribution, validation process, diffusion, and querying.

The replication is the main functional innovation of Jalios. Jalios also provides process innovations : it empowers each categories of users contributing to a content management site, letting them fully use their existing tools. People responsible for web design may continue to use their favorite authoring tool, like Dreamweaver, in order to edit HTML templates. All other users of the solution can achieve their task through their browser: the administrator who gives rights to members, the editorialist in charge of creating new types of publication and validating them, the writers who publish their articles and modify them after reviews, the readers who may interact, ask questions or possibly give their advice.

Our first customers have cheered Jalios for being a plateform that is easy and fast to install, easy to customize, and fully extensible. Some of them have selected it because it was a rapid prototyping plateform and kept using it, because it is an efficient solution for their production needs. Even though we are now launching our commercial operation, we are still interested in developing and looking for new partnerships to explore new usage and develop dedicated applications. One such application is being developed in a project with Renault (MAGIE) to provide a support for innovation, working group, survey, convergence meeting, knowledge transfer.

We would like to emphasis two points. First, it is very important for Research Institutes to provide researchers with support for creating a company to catch business opportunities. In our case, the help from INRIA-transfert was decisive. Second, we believe that process innovations may be as noble as functional innovation and if many research works focus on the second ones, the first ones are probably more important for industrial success in a competitive business such as the content management market.

Links:
http://www.jalios.com/

Please contact:
Vincent Bouthors, Jalios, France
Tel: +33 1 39 63 51 53
E-mail: Vincent.Bouthors@jalios.com

SPONSORED BY ERCIM

SOFSEM 2001 - 28th Conference on Current Trends in Theory and Practice of Informatics

by Gabriela Andrejkova

The SOFSEM (SOFtware SEMinar) is an annual international computer science and computer engineering conference of generalistic and multidisciplinary nature. SOFSEM roots are in the former Czechoslovakia. SOFSEM 2001, the 28th in a row, was held in Piestany, Slovakia, from 24 November to 1 December 2001. SOFSEM 2001 received support from ERCIM and several other institutions from the IT industry. There were 147 participants from 18 countries, about two thirds from Bohemia and Slovakia.

Initially the Proceedings of the seminar were published in Czech and Slovak. Since 1990 the proceedings started to appear in English and since 1995 they have been published in the Springer-Verlag Lecture Notes in Computer Science (LNCS) series.

The Session in 2001 - which was also the second session held in Slovakia since the division of former Czechoslovakia - was organized by the Slovak Society for Computer Science and Faculty of Mathematics, Physics and Informatics of Comenius University (Bratislava) in cooperation with Czech Society of Computer Science, Faculty of Electrical Engineering and Information Technology of Slovak University of Technology, Institute of Informatics and Statistics, Mathematical Institute of Slovak Academy of Sciences and SOFTEC. It was supported by European Association for Theoretical Computer Science and ERCIM (European Research Consortium for Informatics and Mathematics).

The scientific programme of the seminar was divided into three principal areas: Trends in Informatics, Enabling Technologies for Global Computing Practical Systems Engineering and Applications. The Program Committee was chaired by Peter Ruzicka of the Comenius University, Bratislava.

The above areas were covered through 12 invited talks presented by prominent researchers. There were 18 contributed talks, selected by the international Programme Committee from among 46 submitted papers. The conference was accompanied by workshops on Electronic Commerce Systems (coordinated by H. D. Zimmermann) and Soft Computing (coordinated by P.Hajek, ERCIM Working Group). The Proceedings of the conference appeared as volume LNCS 2234 of the Lecture Notes in Computer Science of the Springer-Verlag. The contributed papers presented of the workshop on Soft Computing were published in Neural Network World, No. 6, 2001. The contributed papers of the workshop on Electronic Commerce Systems were published in the local proceedings of Faculty of Mathematics, Physiscs and Informatics of Comenius University.

SOFSEM 2002 will be held at Milovy in the Bohemian Highlands (approximately two hours by car from Brno). We hope that it will be as successful as it was on numerous previous occasions in the same venue.

Links:
SOFSEM 2002:
http://www.sofsem.cz/sofsem02
SOFSEM 2001:
http://www.sofsem.sk/

Please contact:
Gabriela Andrejkova, SRCIM
E-mail: andrejkova@science.upjs.sk

European Interoperability Tour 2002

The World Wide Web Consortium will be holding a series of one-day events around Europe this spring to promote W3C technology recommendations and show how they facilitate interoperability on the World Wide Web.

The mission of the World Wide Web Consortium (W3C) is to 'lead the Web to its full potential' by evolving the Web as a 'robust, scaleable, adaptive infrastructure'. W3C's main deliverables are its recommendations (specifications) that evolve the Web protocols plus timely conversion tools, validation systems and checklists.

W3C is hosted by three organizations in three countries: the Massachusetts Institute of Technology (MIT) in the United States, the French National Institute for Research in Computer Science and Control (INRIA) in France, and Keio University in Japan.

All events will feature talks from:
- Daniel Dardailler, Director of W3C Europe
- Ivan Herman, Head of W3C Offices.

Each event will also feature a speaker from W3C and a local W3C member who will provide a case study of the benefits of W3C technologies. Each event will also include a panel discussion lead by the chair of the local W3C Office on W3C recommendations and how they facilitate interoperability.

Dates and locations of the events:
- 21 May: Paris
- 23 May: Milan
- 28 May: Vienna
- 30 May: Dublin
- 3 June: Brussels

Link:
http://www.w3c.rl.ac.uk/

Please contact:
Marie-Claire Forgue, W3C
European Communications Officer
Tel: +33 4 92 38 75 94
E-mail: mcf@w3.org

Workshop on Current Research Directions in Computer Music

by Leonello Tarabella, Graziano Bertini and Gabriele Boschi

A workshop, held in November 2001 at the Audiovisual Institute, Pompeu Fabra University, Barcelona, provided an overview of the first year of activities of the European Network: MOSART (Music Orchestration Systems in Algorithmic Research and Technology). The event was structured around four main topics: Music Generation, Music Performance, Music Interfaces and Music Sound Modelling.

MOSART is a 3-year project of the European Commission within the Research Training Networks programme. The aim is to 'promote training-through-research, especially of young researchers, both pre- and post-doctoral level, within the frame of high quality trans-national collaborative research projects, including those in emerging fields of research'. MOSART promotes research in the field of Sound and Music Computing, focussing on machine analysis and understanding of musical aspects of sound, such as timbre space and control and virtualisation of instruments. Issues regarding the areas of Interactive Musical Performance and of Human Computer Interactive Conducting Tools are studied, with special attention being given to the use of computers in music analysis, digital music representation and computer assisted musical composition and performance.

The institutions involved in the coordination of the MOSART project are DIKU-University of Copenhagen, DAIMI-DIEM-University of Aarhus, DTU-Danish Technical University, Denmark; NTNU-Norwegian University of Science and Technology, Norway; KTH-Royal Institute of Technology, Sweden; University of Sheffield, United Kingdom; NICI-University of Nijmegen, The Netherlands; Austrian Research Institute for Artificial Intelligence, Vienna, Austria; DEI-University of Padua, DIST-University of Genoa, CNUCE/IEI-CNR, Pisa, Italy; LMA-Centre Nationale de la Recherche Scientifique, Marseille, France; IUA-Pompeu Fabra University, Barcelona, Spain.

The Workshop was structured around four main topics: Music Generation (emphasizing algorithmic composition and composition systems), Music Performance (focussing on quantitative models of performance, cognitive models of perception and production, and expressive performance and emotion); Music Interfaces (with attention to gesture based interaction, mapping strategies and multimodality); Music Sound Modelling (concentrating on instrument modelling, instrument recognition and content processing).

There were three types of events: presentations of overview and short papers (published in the proceedings), posters/demos allowing in-depth discussions between presenters and participants, and panels which provided the opportunity for more informal discussions on the state of the art and future directions of the topics.

Links
Workshop website:
http://www.iua.upf.es/mtg/mosart/
MOSART Network resources:
http://www.diku.dk/research-groups/musinf/mosart/
cART Lab, CNUCE-CNR:
http://www.cnuce.pi.cnr.it/tarabella/cART.html

Please contact:
Leonello Tarabella, CNUCE-CNR
Tel: +39 050 315 3012 (office) 2043 (lab)
E-mail: l.tarabella@cnuce.cnr.it

Graziano Bertini, IEI-CNR
Tel: +39 050 315 3125 (office) 3144 (lab)
E-mail: bertini@iei.pi.cnr.it

CALL FOR PARTICIPATION

The International Conference on Pervasive Computing – PERVASIVE 2002

Zurich, Switzerland, 26-28 August 2002

The objective of this conference will be to present, discuss, and explore the latest technical developments in the emerging field of pervasive computing as well as potential future directions and issues. The conference will focus on technical infrastructure and application issues. It will include presentations, panel discussions, short paper sessions, and demos on topics such as:

- system architectures and platforms for pervasive computing
- middleware and pervasive computing infrastructures
- mobile, wireless, and wearable technologies
- innovative small computing and intelligent devices
- emerging applications and mobile business issues
- scenarios for information appliances
- service discovery protocols
- content distribution and delivery
- user interfaces for invisible and embedded computing
- context awareness
- security and privacy issues.

Further information:
http://www.pervasive2002.org/

CALL FOR PAPERS

7th ERCIM Workshop 'User Interfaces for All"

Chantilly, France, 23-25 October 2002

The vision of User Interfaces for All advocates the proactive realisation of the 'design for all' principle in the field of Human-Computer Interaction (HCI), and involves the development of user interfaces to interactive applications and telematic services, which provide universal access and usability to potentially all users. The emphasis of this year's event is on 'Universal Access' and invites contributions on a broad range of topics, including technological applications and policy developments aiming to advance the notion of Information Society Technologies accessible and acceptable by the widest possible end-user population.

The requirement for Universal Access stems from the growing impact of the fusion of the emerging technologies, and from the different dimensions of diversity that are intrinsic to the Information Society. These dimensions become evident when considering the broad range of user characteristics, the changing nature of human activities, the variety of contexts of use, the increasing availability and diversification of information, knowledge sources and services, the proliferation of technological platforms, etc. In this context, Universal Access refers to the accessibility, usability and, ultimately, acceptability of Information Society Technologies by anyone, anywhere, anytime, thus enabling equitable access and active participation of potentially all citizens in existing and emerging computer-mediated human activities. The user population includes people with different cultural, educational, training and employment background, novice and experienced computer users, the very young and the elderly, and people with different types of disabilities, in various interaction contexts and scenarios of use. As people experience technology through their contact with the user interface of interactive products, applications and services, the field of HCI has a critical and catalytic role to play towards a universally accessible, usable and acceptable Information Society.

Scientific/technological contributions should be on concepts and tools that advance our understanding of, and contribute towards, Universal Access to the new computer-mediated virtual spaces. Areas of interest include, but are not limited to, future and emerging technologies, novel computing paradigms, computer-mediated virtual spaces, architectures and tools, interaction platforms, interaction metaphors, experimental or empirical studies, etc., which bear an impact on the scope of human access to digital content in an Information Society.

Applications-oriented contributions may address practice and experience in the application of Universal Access principles in critical domains such as health, education, employment, etc. In this context, this year's workshop encourages contributions that elaborate upon, adopt, apply or validate a Universal Access code of practice in selected application domains.

Finally, contributions on policy developments should discuss the impact of non-technological factors, such as legislation, standardisation, technology transfer, etc., on developing a culture for Universal Access in the Information Society, for all parties concerned and in particular the industry. Policy contributions may cover success stories of the past or lay out prevailing obstacles to be addressed and removed by effective policy interventions.

Areas of Interest

Areas of interest for which papers are solicited, include, but are not limited to, the following topics:

- Adaptable and adaptive interaction, user modelling
- Intelligent interface technologies
- Multilinguality, internationalisation/localisation of interactive applications
- Novel interaction techniques, multimedia/multimodal interfaces
- Dialogue design methodologies and approaches
- Universal Access design methodologies and tools
- Interface architectures, development tools, interoperability
- Evaluation techniques and tools
- Universal Access scenarios for ambient intelligence
- Universal Access and novel interaction paradigms (wearable and ubiquitous computing, tangible interfaces, Virtual Reality)
- Interaction metaphors
- User Support
- Cooperation
- Personalised content delivery
- Access to e-services
- National and European policies for e-accessibility
- Standards development for Universal Design and Universal Access
- Advances in legislation for Universal Access
- Accessibility of (public) web sites
- User involvement.

Important Dates

- 24 June 2002: Deadline for electronic submission of all papers
- 30 July 2002: Conditional notification of acceptance (confirmation will be given upon registration)
- 16 September 2002: Deadline for electronic submission of camera-ready papers
- 4 October 2002: Deadline for registration.

Keynote Speakers

- Alfred Kobsa, University of California, Irvine, USA
- Steven Pemberton, CWI.

Special events

Two special pre-ERCIM Workshop events will be organised in cooperation with the IS4ALL project (IST-1999-14101) on 23rd October 2002:

- IS4ALL Seminar: Half-day (morning) IS4ALL seminar on 'Universal access: A practitioner's guide in Health Telematics'.
- IS4ALL Thematic Workshop: Half-day (afternoon) workshop entitled 'Methods and tools for designing universal access'. This will include invited position papers by IS4ALL members, and other actors in the fields of Health Telematics and HCI, followed by open discussion.

More details on these events will be published on the IS4ALL project website: http://is4all.ics.forth.gr.

Further information:
http://ui4all.ics.forth.gr/workshop2002/

ERCIM NEWS

ERCIM News is the magazine of ERCIM. Published quarterly, the newsletter reports on joint actions of the ERCIM partners, and aims to reflect the contribution made by ERCIM to the European Community in Information Technology. Through short articles and news items, it provides a forum for the exchange of information between the institutes and also with the wider scientific community. ERCIM News has a circulation of over 7500 copies.

ERCIM News online edition is available at http://www.ercim.org/publication/ERCIM_News/

ERCIM News is published by ERCIM EEIG, BP 93, F-06902 Sophia-Antipolis Cedex
Tel: +33 4 9238 5010, E-mail: office@ercim.org
ISSN 0926-4981

Director: Bernard Larrouturou
Central Editor:
Peter Kunz
peter.kunz@ercim.org
Local Editors:
CLRC: Martin Prime
M.J.Prime@rl.ac.uk
CRCIM: Michal Haindl
haindl@utia.cas.cz
CWI: Henk Nieland
Henk.Nieland@cwi.nl
CNR: Carol Peters
carol@iei.pi.cnr.it
FORTH: Leta Karefilaki
karef@ics.forth.gr
FhG: Michael Krapp
michael.krapp@iuk.fhg.de
INRIA: Bernard Hidoine
bernard.hidoine@inria.fr
NTNU: Truls Gjestland
truls.gjestland@ime.ntnu.no
SARIT: Harry Rudin
hrudin@smile.ch
SICS: Kersti Hedman
kersti@sics.se
SRCIM: Gabriela Andrejkova
andrejk@kosice.upjs.sk
SZTAKI: Erzsébet Csuhaj-Varjú
csuhaj@sztaki.hu
TCD: Ann McNamara
Ann.McNamara@cs.tcd.ie
VTT: Pia-Maria Linden-Linna
pia-maria.linden-linna@vtt.fi

Free subscription

You can subscribe to ERCIM News free of charge by:

- sending e-mail to your local editor
- contacting the ERCIM office (see address above)
- filling out the form at the ERCIM website at http://www.ercim.org/

CALL FOR PARTICIPATION

13th Eurographics Workshop on Rendering

Pisa, Italy, 26-28 June 2002

The Workshop on Rendering is well established as a major international forum for the exchange of ideas and experiences in the area of rendering algorithms and techniques. The Workshop is organised this year by the Visual Computing Group of the Institute for Information Sciences and Technologies, CNR, Pisa, in association with Eurographics and within the framework of the Eurographics Working Group on Rendering Activities.

In addition to a first class program of full papers, the workhop includes invited talks by well known experts in the field of Rendering. The invited speakers this year are: Hans-Peter Seidel (MPI - Saarbruecken, Germany) and Doug Roble (Digital Domain, USA).

Further information:
http://vcg.iei.pi.cnr.it/egrw02.htm

CALL FOR PAPERS

ECDL 2002 – 6th European Conference on Research and Advanced Technology for Digital Libraries

Rome, Italy, 16-18 September 2002

ECDL 2002 is the sixth conference in the series of European Digital Libraries conferences. The focus of ECDL 2002 is on underlying principles, methods, systems and tools to build and make available to final end users effective digital libraries.

Important Dates

- 1 May 2002: Deadline for all proposals
- 15 May 2002: Notification of acceptance for tutorials and workshops
- 15 June 2002: Notification of acceptance for papers, panels, demos and posters
- 1 July 2002: Camera ready papers from the authors.

Scientific Programme

Submissions on all topic areas are welcome and will receive full and equal consideration. Submissions may be full papers, posters, demos, panels, tutorials, or workshops. Although submissions are not restricted in topic or scope, we expect that submissions will fall into one or more of the following broad areas:

- Research: Significant research results on all aspects of digital libraries, focussing on integration of methods, interoperability across different services, data and metadata structures and algorithms, information and text mining, knowledge and multimedia content management, validation also through implementation and use, as well as evaluation.
- Policy: Discussion of significant policy issues related to the design, operation, and economics of digital libraries.
- System: System issues in design, implementation, and building of digital libraries, preferably based on prototypes and strongly backed by practical experience.
- Experience/Evaluation. Analysis of actual implementations of and user interactions with digital libraries in different application areas, possibly including contributions from the humanities, semiotics, and other areas.
- Fundamentals: Studies associating digital libraries with previous areas of thought and discourse. This explicitly includes topics ranging from library/information science to philosophy. However, contributions in this area, as with the other areas, must be accessible to the range of conference attendees, including the more practical outlook of system developers.

ECDL 2002 also provides a forum for discussing applications of digital library concepts and techniques in areas not yet really considered as being part of the Digital Library world, such as education and health care applications, digital earth-sky-law-art and music, humanities, social sciences, environmental monitoring, natural sciences, and historical and scientific archives.

Further information:
http://www.ecdl2002.org

The Research Council of Norway has launched an eight year, 23 million Euro, ICT program, ICT-2010. The primary goals of this program is to generate new knowledge within communications technology, distributed IT systems, and large information and software systems. Among other things the program will emphasize the transfer of expertise and cooperation. The transfer of expertise to users in society in general, industry and applied research will be ensured by training candidates who will move to non-academic positions, and via cooperation between basic research groups and users of research results. Such cooperation also provides valuable feedback and a basis for studying new problems in the basic research environment. Another important aspect of cooperation is that the basic research groups are given the opportunity to profile their research in such a way that it is of relevance to Norwegian user groups. The program wishes research groups to build up strong international contacts. Such contacts are important as antennas for capturing new development trends at an early stage, in an area in which much research takes place abroad. In order to promote such contacts, the program's doctoral students should spend six months to a year abroad.

International Review of UK Research in Computer Science. The International Review of UK Research in Computer Science was conducted by a panel of experts from all over the world on behalf of the Office of Science & Technology, the Engineering & Physical Sciences Research Council, the IEE, the British Computer Society and the Royal Society. A final report published in November 2001 confirms the traditional high quality of UK computer science, but warns that the nation's position as a world leader is by no means assured. Declines in certain fields are already evident, it claims, and more will follow given current levels of support and the nature of today's university research environment. Identifying several broad areas in which UK research strength is particularly at risk – including programming language design, artificial intelligence, human-computer interaction and bio-informatics – the panel highlights algorithms and complexity research as key areas of potentially massive future importance where research needs to be encouraged. Given the opportunities that will be created by the recently announced three-year e-Science initiative, it adds, the absence of funding within the scheme for longer-term computer science research seems 'ill considered' at a time of declining UK research activity in high-performance scientific computing. See http://www.iee.org/Policy/CSreport/

SZTAKI — **Tamás Roska** received the Bolyai Prize, Hungary's highest non-state scientific award named after the world-renowned mathematician János Bolyai (1802-1860), from Ferenc Mádl, President of Hungary, in the Budapest Convention

Hungarian President Ferenc Mádl (left) presents the Bolyai Prize to Tamás Roska.

Centre on 2 March 2002. The Bolyai Prize Foundation was set up in 1998 at a non-governmental initiative. The prize, with a purse of USD 50,000 was first awarded in 2000. Tamás Roska is the head of the Analogic and Neural Computing Research Laboratory, SZTAKI and Professor and Dean of the Faculty of Information Technology at the Pázmány P. Catholic University, Budapest. He is a co-inventor of the CNN Universal Machine (with Leon O. Chua) and the analogic CNN Bionic Eye (with Frank S. Werblin and Leon O. Chua), both are US patents owned by the University of California at Berkeley. Tamás Roska recently coordinated an EU-NSF strategic workshop on Bionics organized by ERCIM.

CNR — **Franco Denoth** has been appointed as Director of the newly constituted Istituto di Informatica e Telematica, located in the CNR Research Area, Pisa. IIT-CNR has been

formed as a result of the merging of the Institutes for Computational Mathematics and Telematic Applications, part of the ongoing restructuring of CNR. The main areas of interest at IIT are: web algorithmics; search engines; safety in shared environments; computational biology; electronic transactions and safety protocol; advanced and safe systems for the production of network structured information. Further information can be found at http://www.iit.cnr.it/

INRIA — **The new innovation and communication center** (PIC) of the INRIA Rocquencourt unit was inaugurated on 15 January 2002. The center has a show floor and conference area, including a large amphitheater named after the famous mathematician Jacques-Louis Lions, in honor of the Institute's past President from 1979 to 1983. An information area is open to the public and another area is dedicated to development and transfer. The latter will host incubating companies in the field of ICST wishing for scientific proximity. The whole building covers an area of nearly 5,000m^2 and was designed by architect Henri Ciriani. The construction was financed by the Government, the Yvelines Departmental Council and the Île-de-France Regional Council.

ERCIM – The European Research Consortium for Informatics and Mathematics is an organisation dedicated to the advancement of European research and development, in information technology and applied mathematics. Its national member institutions aim to foster collaborative work within the European research community and to increase co-operation with European industry.

Austrian Association for Research in IT
c/o Österreichische Computer Gesellschaft
Wollzeile 1-3, A-1010 Wien, Austria
Tel: +43 1 512 02 35 0, Fax: +43 1 512 02 35 9
http://www.aarit.at/

Central Laboratory of the Research Councils
Rutherford Appleton Laboratory
Chilton, Didcot, Oxfordshire OX11 0QX, United Kingdom
Tel: +44 1235 82 1900, Fax: +44 1235 44 5385
http://www.cclrc.ac.uk/

Consiglio Nazionale delle Ricerche, IEI-CNR
Area della Ricerca CNR di Pisa,
Via G. Moruzzi 1, 56124 Pisa, Italy
Tel: +39 050 315 2878, Fax: +39 050 315 2810
http://www.iei.pi.cnr.it/

Czech Research Consortium
for Informatics and Mathematics
FI MU, Botanicka 68a, CZ-602 00 Brno, Czech Republic
Tel: +420 2 688 4669, Fax: +420 2 688 4903
http://www.utia.cas.cz/CRCIM/home.html

Centrum voor Wiskunde en Informatica
Kruislaan 413, NL-1098 SJ Amsterdam,
The Netherlands
Tel: +31 20 592 9333, Fax: +31 20 592 4199
http://www.cwi.nl/

Foundation for Research and Technology – Hellas
Institute of Computer Science
P.O. Box 1385, GR-71110 Heraklion, Crete, Greece
Tel: +30 81 39 16 00, Fax: +30 81 39 16 01
http://www.ics.forth.gr/

Fraunhofer-Gesellschaft,
Information and Communication Technology Alliance
Schloß Birlinghoven, D-53754 Sankt Augustin, Germany
Tel: +49 2241 14 0, Fax: +49 2241 14 2889
http://www.fraunhofer.de/

Institut National de Recherche en Informatique
et en Automatique
B.P. 105, F-78153 Le Chesnay, France
Tel: +33 1 3963 5511, Fax: +33 1 3963 5330
http://www.inria.fr/

Norvegian University of Technology,
Faculty of Information Technology, Mathematics and
Electrical Engineering, N 7491 Trondheim, Norway
Tel: +47 73 59 80 35, Fax: +47 73 59 36 28
http://www.ntnu.no/

Swedish Institute of Computer Science
Box 1263,
SE-164 29 Kista, Sweden
Tel: +46 8 633 1500, Fax: +46 8 751 72 30
http://www.sics.se/

Swiss Association for Research in Information Technology
Dept. Informatik, ETH-Zentrum, CH-8092 Zürich,
Switzerland
Tel: +41 1 632 72 41, Fax: +41 1 632 11 72
http://www.sarit.ch/

Slovak Research Consortium for Informatics and
Mathematics, Comenius University, Dept.of Computer
Science, Mlynska Dolina M, SK-84248 Bratislava,
Slovakia, Tel: +421 7 726635, Fax: +421 7 727041
http://www.srcim.sk/

Magyar Tudományos Akadémia
Számítástechnikai és Automatizálási Kutató Intézete
P.O. Box 63, H-1518 Budapest, Hungary
Tel: +36 1 279 6000, Fax: + 36 1 466 7503
http://www.sztaki.hu/

Trinity College
Department of Computer Science,
Dublin 2, Ireland
Tel: +353 1 608 1765, Fax: 353 1 677 2204
http://www.cs.tcd.ie/ERCIM

Technical Research Centre of Finland
VTT Information Technology, P.O. Box 1200, FIN-
02044 VTT, Finland
Tel:+358 9 456 6041, Fax :+358 9 456 6027
http://www.vtt.fi/

Order Form

If you wish to subscribe to ERCIM News ***free of charge*** *or if you know of a colleague who would like to receive regular copies of ERCIM News, please fill in this form and we will add you/them to the mailing list.*

send, fax or email this form to:

ERCIM NEWS
Domaine de Voluceau
Rocquencourt
BP 105
F-78153 Le Chesnay Cedex
Fax: +33 1 3963 5052
E-mail: office@ercim.org

Name:

Organisation/Company:

Address:

Post Code:

City:

Country

E-mail:

Data from this form will be held on a computer database. By giving your email address, you allow ERCIM to send you email

You can also subscribe to ERCIM News and order back copies by filling out the form at the ERCIM website at http://www.ercim.org/publication/Ercim_News/