INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team SMIS

Secured and Mobile Information Systems

Rocquencourt

THEME SYM

Table of contents

1. Team

Head of project-team
Philippe Pucheral [PR1 - UVSQ (on secondment at INRIA), HdR]

Vice-head of project team
Luc Bouganim [DR2 - INRIA, HdR]

Inria research scientist
Nicolas Anciaux [CR2 - INRIA]

Part-time research scientist (external partner)
Béatrice Finance [MC - UVSQ, HdR]

Visiting professor
Dennis Shasha [New York University, Invited Professor, from July 1st]

Administrative assistant
Elisabeth Baque [AI - INRIA]

Ph. D. students
François Dang Ngoc [UVSQ, INRIA grant]
Mehdi Benzine [UVSQ, MESR]
Bashkar Biswas [Ecole Polytechnique, CORDI INRIA (joint PhD with CODES project-team)]
Harold van Heerde [University of Twente (joint PhD with P. Apers team)]

Project technical staff
Christophe Salperwyck [Engineer Polytech'Nantes]

Graduate student intern
Tristan Allard [Master UVSQ]
Vincent Jantet [ENS Cachan - antenne de Bretagne]
Shaoyi Yin [Renmin University of China]

2. Overall Objectives

2.1. Overall Objectives

Keywords: *Database management systems*, *database security (data confidentiality and privacy)*, *mobile and embedded databases*.

The emergence of ubiquitous and pervasive computing introduces the need for embedding various forms of data in ever lighter and specialized computing devices (personal digital assistants, cellular phones, chips dedicated to home networks, cars, health, etc). In this context, the first objective of the SMIS project is the definition of core database technologies tackling the hardware constraints of specialized computing devices. By making the information more accessible and by multiplying the - transparent - ways of acquiring this information, ubiquitous and pervasive computing induce new threats on data confidentiality. More generally, preserving the confidentiality of personal data spread among a large variety of sources (mobiles, smart objects as well as corporate, commercial and public databases) has become a major challenge for the database community. Thus, the second objective pursued by the SMIS project is the definition of access control models preserving data confidentiality and privacy and the definition of tamper-resistant database architectures enforcing this control. These two objectives are refined below.

Ubiquitous/pervasive data management: Important research efforts have to be undertaken to capture the impact of each devices hardware constraints on database techniques and to set up co-design rules helping calibrating the hardware resources of future devices in order to match specific applications requirements. This research direction is interested in storage models, indexation structures and query execution techniques matching strong hardware constraints in terms of RAM, energy and communication bandwidth consumption. Electronic stable storage technologies (EEPROM, Flash, MEMS, etc) have also a considerable impact on the organization of the data at rest. Problems related to the interaction of ultra-light devices with a larger information system deserve also a particular attention (e.g., querying data disseminated among a large population of ultra-light devices, defining and managing ambient databases, exploiting external computing and storage resources).

Data confidentiality and privacy: The increasing amount of sensitive data gathered in databases, and in particular of personal data, imposes the definition of fine-grain access control models. While access control in client-server relational database is roughly mature, new issues appear today: fine-grain access control over hierarchical and semi-structured data (e.g., XML), integration of privacy concern in the access control policies (e.g., users consent, usage control), access control administration over multiple distributed, heterogeneous and autonomous resources. A complementary issue we are interested in is the security (i.e., tamper-resistance) of the access control itself. Cryptographic techniques can be exploited to this end. While encryption is used successfully for years to secure communications, database encryption introduces difficult theoretical and practical problems: how to execute efficiently queries over encrypted data, how to conciliate declarative (i.e., predicate based) and dynamic access rights with encryption, how to distribute encryption keys between users sharing part of the database? Our objective is to try providing accurate answers to these questions by devising secured models based on tamper-resistant hardware to query, update and share encrypted databases.

The complementarity of these two research issues is twofold. First, ubiquitous/pervasive data management generates specific confidentiality problems that must be tackled accurately. Hence, this first area of research is expected to feed the second one with relevant motivating examples. Second, data management techniques embedded in secured devices (e.g., smart cards, secured tokens) can be the foundation for new security models. For example, remote databases can be made secure by delegating part of the data management to a secured device. Thus, a strong cross-fertilization can be expected between these two research areas.

Beyond the scientific objectives detailed above, which are expected to generate publications in top level database and security conferences and journals, our ambition is to develop high quality prototypes that will serve two purposes: (1) validate our results and real hardware/software platforms and (2) integrate our results on real applications where data confidentiality is a primary concern (Electronic Health Record systems, ambient intelligence privacy).

3. Scientific Foundations

3.1. Ubiquitous data management

Keywords: *embedded databases*, *query processing*, *secured computing platforms*, *storage and indexation models*, *transaction management*.

The vision of the future dataspace, a physical space enhanced with digital information made available through large-scale networks of smart objects is paint in [41]. The management of data in such dataspace differs dramatically from the mainframe database setting. In this context, the data sources are moving, managed by highly constrained computing devices, might get temporarily or permanently disconnected and have at best a partial knowledge about their environment.

This setting strongly impacts the way the data are managed locally. Actually, not only the data but also data management techniques (e.g., query, access control, transaction) have frequently to be embedded in highly constrained hardware devices. For example, sensor networks collecting weather or pollution data [36] are evolving towards real distributed databases in which each sensor acts as an active node (i.e., as a micro-data server queryable remotely) [43]. Protecting the confidentiality of portable folders (e.g., healthcare folders, users' profiles) is another motivation to embed data management techniques into tamper-resistant devices (e.g., smart cards) [9]. More generally, embedded database techniques are required in every context where computations have to be performed in a disconnected mode. To conceive embedded database components is however not obvious. Each target architecture is specifically designed to meet desirable properties (portability, energy consumption, tamper resistance, etc) under imposed hardware constraints (maximum silicon die size, memory technology, etc). In addition, these architectures evolve rapidly to catch new applications. The challenge is then twofold: (i) being able to design dedicated embedded database components and (ii) being able to set up co-design rules helping hardware manufacturers calibrating their future platforms to match the requirements of data driven applications. While a large body of work has been conducted on data management techniques for high-end servers (storage, indexation and query optimization models minimizing the I/O bottleneck, parallel DBMS, main memory DBMS, replication and fault tolerance, etc), few research efforts have been placed so far on embedded database techniques. Light versions of popular DBMS have been designed for powerful handheld devices but DBMS vendors never addressed the more complex problem of embedding database components into chips. Recent works have been conducted on smart card databases and on data management techniques for sensor networks but this research field is still at a preliminary stage.

The dataspace setting also impacts the way queries are expressed (spatio-temporal conditions, continuous queries) and executed (decentralized control, scarce local computing resources, uncertain availability of the data sources). Distributed query management has been extensively studied for thirty years [45], considering a reduced collection of data sources managed by high-end servers. These methods are irrelevant in a context involving potentially millions of data sources managed by lightweight devices. Query management in Peer-to-Peer systems and in Data Grids address the scalability issue and the unpredictable availability of data sources but do not consider lightweight devices. The first works to consider distributed queries (restricted to filters and aggregations) over lightweight devices have been conducted in the sensor network field. Hence, regular queries distributed over a large collection of full-fledged databases managed by lightweight devices remains an open issue.

3.2. Data confidentiality

Keywords: *access control models*, *data confidentiality and privacy*, *encrypted databases*, *secured computing platforms*.

Confidentiality, Integrity and Availability are the three fundamental properties ruling the security of any information system. Data confidentiality has recently become a major concern for individuals as well as for companies and governments. Several kinds of data are threatened: personal data gathered by visited Web sites or by smart objects used in the daily life, corporate databases hosted by untrusted Database Service Providers, central databases subject to piracy. The CSI/FBI reports that database attacks constitute the principal source of cyber-criminology and that more than fifty percents of the attacks are conducted by insiders [42]. In this context, governments are setting up more constraining legislations. The problem is then to translate laws into technological means: authentication mechanisms, data and communication encryption, access control, intrusion detection, data and operation anonymization, privacy preserving data mining, etc. The area of investigation is extremely large. Our own research program focuses on access and usage control management and on the way this control can be made secure (i.e., tamper-resistant).

Access control management has been deeply studied for decades. Different models have been proposed to declare and administer access control policies, like DAC, MAC, RBAC, TMAC, OrBAC [38]. While access control management in relational databases is now well established and normalized, new access control models have to be defined to cope with more complex data (e.g., hierarchical and semi-structured data like XML) and new forms of data distribution (e.g., selective data dissemination). Privacy models are emerging today [32].

Privacy distinguishes from confidentiality is the sense that the data to be protected are personal. Hence, the user's consent must be reflected in the access control policies and not only the access but also the usage of the data must be controlled carefully.

Securing the access control against different forms of tampering is a very important issue. Server-enforced access control is widely accepted [35] but remains inoperative against insider attacks. Several attempts have been made to strengthen server-based security with database encryption [44] [40]. However, the Database Administrator (or an intruder usurping her identity) has enough privilege to tamper the encryption mechanism and get the clear-text data. Client-based security approaches have been recently investigated. Encryption and decryption occur at the client side to prevent any disclosure of clear-text data at the server. Storage Service Providers proposing encrypted backups for personal data are crude representative of this approach. The management of SQL queries over encrypted data complements well this approach [39]. Client-based decryption is also used in the field of selective data dissemination (e.g., Digital Right Management). However, the sharing scenarios among users are generally coarse grain and static (i.e., pre-compiled at encryption time). Tamper-resistant hardware can help devising secured database architectures alleviating this problem. Finally, securing the usage of authorized data is becoming as important as securing the access control as far as privacy preservation is concerned. Thus, database encryption, tamper-resistant hardware and their relationships with access control and usage control constitute a tremendous field of investigation.

4. Application Domains

4.1. Application Domains

Keywords: *ambient intelligence*, *healthcare*, *secure data dissemination*, *web-hosting databases*.

Our work on ubiquitous data management addresses varied application domains. Typically, database components on chip are required each time data-driven applications have to be embedded in ultra-light computing devices. This situation occurs for example in healthcare applications where complex portable folders are embedded into smart tokens (e.g., smart cards, secured USB keys), in telephony applications where personal data (address book, agenda, etc.) are embedded into cellular phones, in sensor networks where sensors log row measurements and perform local computation on them, in home networks where a collection of smart appliances gather information about the occupants to provide them a personalized service, and more generally in most applications related to ambient intelligence.

Safeguarding data confidentiality has become a primary concern for citizens, administrations and companies, broadening the application domains of our work on access control policies definition and enforcement. The threat on data confidentiality is manifold: external and internal attacks on the data at rest and the data on transit, data hosted in untrusted environments (e.g., Database Service Providers, Web-hosting companies) and subject to illegal usage, insidious gathering of personal data in an ambient intelligence surrounding. Hence, new access control models and security mechanisms are required to accurately declare and safely control who is granted access to which data and for which purpose.

While the application domains mentioned above are rather large, two applications are more specifically targeted by the SMIS project. The first one deals with privacy preservation in an ambient intelligence context. Our objective is twofold: (1) to complement smart objects with Hippocratic features, a term introduced in [32] to denote DBMSs able to keep secret the data for which the owner did not give explicit delivery consent and (2) to define a data retention mechanism which decreases the precision of personal data acquired by sensors and gathered in databases over time, avoiding people to be tracked forever. The second target application deals with privacy preservation in EHR (Electronic Health Record) systems. France launched recently an ambitious EHR program where medical folders will be centralized and hosted by private Database Service Providers. Centralization and hosting increase the risk of privacy violation. Hence, fine-grain access control models and robust database security mechanisms are highly required. Portable folder on secured mass storage chips can also help reducing the risk. We are setting up a project tackling precisely this issue (cf. Section 7).

5. Software

5.1. Introduction

In our domain of expertise, developing software prototypes is an important mean to validate research solutions. This prototyping task is however difficult since it requires specialized computing devices (e.g., smart cards), themselves sometimes at an early stage of development (see Section 7.1.1)). While time consuming, these prototypes are the vector for research publications, demonstrations at conferences and exhibitions as well as for cooperations with industry. The recent Gold Award we received at the SIMagine'05 international software contest illustrates well this strategy. This award has rewarded one of our prototype, named MobiDiQ, an advanced Digital Right Management (DRM) engine embedded in a SIM card (cell phone smart card) and enabling fair use (e.g., promotional access to cultural contents for students or artists, parental or teacher control prohibiting access to non-ethical contents). In 2006, we started a new prototype activity around PlugDB, a data management technique embedded in a secure USB key which allows managing databases contaning a mix of public and highly sensitive data. We do not detail PlugDB further since the prototype is only at an earlier stage (principles of the solution are sketched in Section 6.3).

In the following, we concentrate on two main prototyping activities started before 2006 but still active today.

5.2. PicoDBMS

Participants: Nicolas Anciaux [correspondent], Luc Bouganim, Philippe Pucheral.

PicoDBMS is a smart card full-fledged DBMS aiming at managing shared secured portable folders. A first prototype written in JavaCard has been demonstrated at the VLDB'01 conference [34]. It showed the feasibility of the approach but exhibited disastrous performance. Since then, a second prototype has been written in C and optimized partly with the help of Axalto (their smart card OS has been modified to better support data intensive on-board applications). This prototype is now running on an experimental smart card platform and exhibits two order of magnitude better performances than its JavaCard counterpart. A cycle-accurate hardware simulator allowed us to predict the PicoDBMS performance on future smart card platforms. Extensive experimentations have been conducted recently on this prototype thanks to a dedicated PicoDatabase Benchmark [33], [23]. The PicoDBMS prototype has been a major vehicle to validate our results, to develop strong competencies in terms of design rules for embedded database components and to set up a long term industrial cooperation with Axalto. The management of large databases (e.g., several GB) embedded in Smart Secured Mass Storage Cards (roughly speaking, a combination of a secured chip and an insecure USB key-like mass storage) deserves new studies. Link: http://www-smis.inria.fr/Eprototype_PicoDBMS.html.

5.3. Chip-Secured XML Access

Participants: François Dang Ngoc [correspondent], Luc Bouganim, Christophe Salperwyck, Philippe Pucheral.

Chip-Secured XML Access (C-SXA) is an XML-based access rights controller embedded in a smart card. C-SXA evaluates user's privileges on a queried or streaming XML encrypted document and delivers the authorized subset of this document. Compared to existing methods, C-SXA supports fine grain and dynamic access control policies by separating access control issues from encryption. Application domains cover the exchange of confidential data among a community of users (e.g., collaborative work) as well as selective data dissemination. A first C-SXA prototype has been developed on a hardware cycle-accurate simulator to assess the medium-term viability of the approach in terms of performance [7]. Then, a C-SXA engine has been developed in JavaCard on a real smart card platform and has been demonstrated at the SIGMOD'05 conference [37]. An application scenario dealing with selective disseminations of multimedia content has been developed on top of this engine (MobiDiQ). Link: http://www-smis.inria.fr/Eprototype_C-SXA.html.

6. New Results

6.1. Embedded data management

Keywords: *benchmarks*, *co-design*, *query processing*, *storage and indexation models for embedded databases*.

Participants: Nicolas Anciaux, Tristan Allard, Luc Bouganim, Philippe Pucheral, Shaoyi Yin.

Preliminary studies led us to design the first full-fledged DBMS embedded in a smart card, called PicoDBMS. PicoDBMS aims at managing shared secured portable folders. The specific hardware architecture of smart cards entailed a thorough re-thinking of existing database techniques [9]. As detailed in Section 5.2, three years of joint efforts with our industrial partner Axalto (design optimization, new hardware platform, OS adaptation) were necessary to get a convincing prototype. In 2006, we designed a benchmark for secure chip DBMS in order to (1) compare the relative performance of candidate storage and indexation data structures, (2) predict the limits of on-chip applications, and (3) provide co-design hints to help calibrating the resources of a future secure chip to meet the requirements of on-chip data intensive applications [23]. This work concludes the PicoDBMS study.

Our new research investigates the impact of different stable storage technologies (EEPROM, Flash, FeRAM, MEMS) on traditional database techniques. Electronic stable memories exhibit very specific read and write characteristics impacting database storage, indexation, querying and transaction management. We are currently specifying a storage and indexation model dedicated to NAND-Flash. The compactness of FLASH memory makes it well adapted to lightweight devices and smart card manufacturers are announcing SSMSC devices (Smart Secured Mass Storage Cards) equipped with several Gigabytes of (NAND) FLASH. Note that contributions on FLASH database techniques may have a broader impact on core database research as solid-state Flash disks technology could become an alternative to failure-prone mechanical Hard Disk Drives.

6.2. Data confidentiality and privacy

Keywords: *access control models*, *data confidentiality and privacy*, *data retention*.

Participants: Nicolas Anciaux, Luc Bouganim, Harold J. W. van Heerde, Philippe Pucheral.

Smartness and privacy are contradictory requirements for Ambient Intelligence (AmI). On one hand, AmI must collect enough context information reflecting physical surroundings such as individuals location, activity, and habits. This information provides the required smartness to adapt, infer, learn, and anticipate, enabling autonomous decisions without user interaction. The obtained level of smartness is tightly coupled to the quality (i.e., accuracy) and quantity of contextual data. On the other hand, context is usually linked to individuals (e.g., location of a person) and is of main interest to track people daily behaviour, e.g., before providing them insurance contracts or offering a job position. The goal of this work is to enable a suitable compromise between smartness and privacy preservation for AmI. We introduce the concept of Life-Cycle Policies (LCP) specifying a progressive degradation of context histories. Thanks to LCP, the AmI system only retains the desired "souvenir" of individuals past actions [24], [21]. As a prerequisite, we study the notion of minimal data retention wrt. database grants. The problem is to characterize the minimal amount of information collected by sensors that the database must actually store to adequately calculate the result of an authorized database view. Existing techniques to degrade the data are based on data anonymisation, suppression, generalization, or introduction of (controlled) noise, but have the side effect of producing fuzzy results. Hence, they are mainly used to produce statistics. By contrast, our retention model preserves adequacy wrt. grants: any degradation operated on the collected data does not prevent the DBMS for producing correct and complete answers while calculating authorized queries or views.

6.3. Tamper-resistant XML access control model

Keywords: *access control models*, *data confidentiality*, *query processing*, *secure computing platforms*.

Participants: Nicolas Anciaux, Mehdi Benzine, Luc Bouganim, François Dang Ngoc, Vincent Jantet, Philippe Pucheral, Dennis Shasha.

Our study on tamper-resistant data management has been conducted in two directions: (1), selective data dissemination and (2) management of database mixing public and sensitive data.

While digital piracy is threatening the global multimedia content industry, applying blindly coercive Digital Right Management (DRM) policies do nothing but legitimizing piracy. We extended previous works [7] on tamper-resistant XML access control and proposed a solution aiming at reconciling the content providers and consumers point of views by giving the ability to develop fair DRM models. Digital rights, i.e., licenses are enforced depending both on the digital content and on personal data (historical records, user profile, etc.) stored securely on a tamper-resistant device. Embedding the license evaluator prevents any tampering to occur, thereby giving strong anti-piracy guarantees to the content provider. Embedding personal data brings also strong guarantees about users privacy preservation. Combined together, these principles allow a tamper-resistant and ethical selective data dissemination [17].

People talk about privacy, but give it up very easily, especially when faced with complex security procedures that offer only conditional guarantees. This implies that for people's sensitive data to be protected, the cost to protect it must require little physical effort and must perform well. We proposed a system whereby people carry hidden sensitive data on a tamper-resistant USB key and they plug that key into a personal computer when they need to link their hidden data with visible public data, all with the assurance that no hidden data will ever go out in the open. The principal novelties follow directly from the challenges of implementing this mode of operation: (1) how to declare which data should be visible and hidden simply and how to query it, (2) how to index the data, and (3) which query processing strategies to use to link public and private data hosted on extremely unequal devices (standard computer and smart USB key). This work has been submitted for publication and will be pursued in 2007.

7. Contracts and Grants with Industry

7.1. National grants

7.1.1. Industrial collaborations

The SMIS project has a long lasting cooperation with Axalto, recently merged with Gemplus to form Gemalto, the world's leading providers of microprocessor cards. Axalto provides SMIS with advanced hardware and software smart card platforms which are essential to validate numbers of our research results. In return, SMIS provides Axalto with application examples for their future smart card platforms as well as important technical feedbacks that help them adapting these platforms towards data intensive applications.
SMIS is also starting a cooperation with UniMedecine, a hightech SME developing software platforms of on-line medical services. Uni-Medecine is associated with ATOS ORIGIN and HP France in SANTEOS, one of the six consortia selected by the French Ministry of Health to develop the future DMP (the national Personal Medical Folder initiative). This cooperation will help us in tackling one of our targeted application, namely the protection of medical folders (see next section).

7.1.2. PlugDB RNTL project

Category: RNTL project
Duration: December 2006 - December 2009
Partners: INRIA-SMIS (coordinator), Univ. Versailles, Gemalto, UniMedecine, ALDS

Description: The goal of the PlugDB project is to design new technologies dedicated to a secure and ubiquitous management of personal data. Personal data will be embedded in a new secured device named SSMSC (Smart Secure Mass Storage Card) combining the security of smart cards with the storage capacity of USB keys. These data are replicated in an untrusted server in an encrypted form. The SSMSC can act either as a secure portable server or as a trusted client to get access to the data stored in the untrusted server. In the frame of the project, the proposed technology will be validated by an experimentation in the medical context (management of portable healthcare folders for elderly people who need home care).

8. Other Grants and Activities

8.1. National grants

8.1.1. ACI CASC

Category: ACI Sécurité
Duration: July 2003 - July 2006
Partners: INRIA-SMIS (coordinator), ENS Ulm, LRI, ENST-Bretagne, Univ. Pau
Description: The CASC project is interested in access control management and data confidentiality, with a particular focus on: (i) abstraction of the fundamental concepts participating in an access control policy declaration, (ii) definition of a powerful and sound access control model for XML and (iii) definition of secured data access and administration architectures. Link: http://www-smis.inria.fr/~bouganim/CASC.

8.2. International and national cooperations

The SMIS members have developed international cooperations with the following persons/teams:

- Dennis Shasha (Professor at the University of New-York): collaboration on tamper-resistant data management issues (see details in Section 6.3). Dennis Shasha is doing a sabbatical stay in SMIS (July 2006 to June 2007).
- Xiaofeng Meng (Professor at Renmin University of China, Beijing): collaboration on embedded data management issues (see details in Section 6.1). Shaoyi Yin, member of X. Mengs team, is doing an internship in SMIS (October 2006-March 2007). This work is partly funded by a Franco-Chinese research program (PRA SI-05604).
- P.G.M. Apers (Professor at the University of Twente): collaboration on data confidentiality issues (see details in Section 6.2). H.J.W. van Heerde, member of P. Apers team, is doing a PhD in co-supervised by P. Apers and N. Anciaux.

At the national level, SMIS members cooperate with different French labs and university through national projects (see sections 7.1 and 8.1).

9. Dissemination

9.1. Scientific activity and coordination

9.1.1. Collective responsibilities within INRIA

Philippe Pucheral is member of the Bureau du Comité des Projets (project council) of INRIA Rocquencourt since September 2004. He is correspondent for the Mission Formation par la Recherche (Training through Research) and then responsible for the relationships between INRIA Rocquencourt and the Parisian universities.

Luc Bouganim is member of the Commission Délégations-Détachements of INRIA Rocquencourt since November 2004. He is the INRIA representative for the summer schools in computer science co-organized by INRIA, CEA and EDF. He is also co-responsible for the organization of the monthly scientific seminars at INRIA Rocquencourt.

9.1.2. Collective responsibilities outside INRIA

The SMIS members have conducted, or participated to, the following actions in the research community:

- Philippe Pucheral
  - PC member of XSym06, ICPS06, SWAN06, EuDiRight06.
  - Co-chair of UbiMob06.
  - Area Editor of the Information Systems international journal.
  - Member of the Scientific Board of the SETIN program (Sécurité et Informatique) launched by the French Research Agency (ANR).
  - Member of the BDA Board (Bases de Données Avancées).
  - Member of the Laboratory council of the PRiSM research Lab (Univ. Versailles CNRS).
  - Member of the commission de spécialistes 27th section of the University of Cergy.
  - Referee for the HDR (Habilitation à Diriger des Recherches) of S. Gancarski (Univ. Paris 6) and D. Donsez (UJF Grenoble) and jury member of the HDR of K. Zeitouni (Univ. Versailles) and the PhD thesis of S. Monnet (Univ. Rennes I) and C. Saita (Univ. Versailles) and F. Dang Ngoc (Univ. Versailles).
  - Tutor (i.e., advisor) for the HDR of L. Bouganim (Univ. Versailles) and B. Finance (Univ. Versailles).
- Luc Bouganim
  - Coordinator of the ACI "Sécurité Informatique" CASC
  - PC member of VLDB06, COOPIS06, SBBD06, EXPDB06, UbiMob06, DASFAA06
  - Member of the Editorial Board of TSI Journal (Technique et Science Informatiques)
  - Referee for the PhD thesis of David Coquil (INSA Lyon) and jury member for the PhD thesis of D. Bromberg (Univ. Versailles) and F. Dang Ngoc (Univ. Versailles).
- Béatrice Finance
  - Member of the Scientific Board of the UFR de sciences of the University of Versailles/St-Quentin.
  - Member of the Administration Board of the ISTY engineering school since 1998.
  - Jury member of the PhD thesis of T-T. VU (UJF Grenoble)
- Dennis Shasha has made several tutorials in France (3), Switzerland (1), The Netherlands (1) and India (1).
- Nicolas Anciaux and Luc Bouganim were invited for a tutorial on Data management in embedded smart devices at the Smart University event (Sophia Antipolis).

9.2. Teaching activity

The SMIS members have tight links with the University of Versailles/St-Quentin (UVSQ). Philippe Pucheral is professor at UVSQ, on secondment at INRIA. The list of the main courses given by each staff member in 2006 is given below:

- P. Pucheral: co-director of the research Master COSY (Univ. Versailles), courses on DBMS architecture and database security (45h/y).
- L. Bouganim: DBMS architecture, data security, database technology (90h, given at Univ. Versailles, ENST Paris, CNAM Paris)
- N. Anciaux: DBMS internal mechanisms, database Technology (48h, given at Univ. Versailles)
- M. Benzine: Architecture, database concepts (64h, given at Univ. Versailles)
- C. Salperwyck: database technology (16h, given at Univ. Versailles)

10. Bibliography

Major publications by the team in recent years

[1] M. ABDALLAH, R. GUERRAOUI, P. PUCHERAL. *Dictatorial Transaction Processing : Atomic Commitment without Veto Right*, in "Distributed and Parallel Database Journal (DAPD)", vol. 11, n^{O} 3, 2002.

[2] N. ANCIAUX, L. BOUGANIM, P. PUCHERAL. *Memory Requirements for Query Execution in Highly Constrained Devices*, in "Proc. of the 29th Int. Conf. on Very Large Data Bases (VLDB)", 2003.

[3] L. BOUGANIM, F. FABRET, C. MOHAN, P. VALDURIEZ. *A Dynamic Query Processing Architecture for Data Integration Systems*, in "IEEE Data Engineering Bulletin", vol. 23, n^{O} 2, 2000.

[4] L. BOUGANIM, F. FABRET, F. PORTO, P. VALDURIEZ. *Processing Queries with Expensive Functions and Large Objects in Distributed Mediator Systems*, in "Proc. of the 17th Int. Conf. on Data Engineering (ICDE)", 2001.

[5] L. BOUGANIM, F. FABRET, P. VALDURIEZ, C. MOHAN. *Dynamic Query Scheduling in Data Integration Systems*, in "Proc. of the 16th Int. Conf. on Data Engineering (ICDE)", 2000.

[6] L. BOUGANIM, P. PUCHERAL. *Chip-Secured Data Access : Confidential Data on Untrusted Servers*, in "Proc. of the 28th Int. Conf. on Very Large Data Bases (VLDB)", 2002.

[7] L. BOUGANIM, F. DANG NGOC, P. PUCHERAL. *Client-Based Access Control Management for XML Documents*, in "Proc. of the 30th Int. Conf. on Very Large Databases (VLDB)", 2004.

[8] B. FINANCE, S. MEDJDOUB, P. PUCHERAL. *The Case for Access Control on XML Relationships*, in "Proc. of the ACM Int. Conf. on Information and Knowledge Management (CIKM)", 2005.

[9] P. PUCHERAL, L. BOUGANIM, P. VALDURIEZ, C. BOBINEAU. *PicoDBMS : Scaling down Database Techniques for the Smartcard*, in "Very Large Data Bases Journal (VLDBJ), Best Paper Award VLDB'2000", vol. 10, n^{O} 2-3, 2001.

[10] P. PUCHERAL, ET AL. *Mobile Databases : a Selection of Open Issues and Research Directions*, in "ACM Sigmod Record", collective report written under the supervision of P. Pucheral, vol. 33, n^{O} 2, 2004.

Year Publications

Doctoral dissertations and Habilitation theses

[11] L. BOUGANIM. *Sécurisation du Contrôle d'Accès dans les Bases de Données*, Habilitation à Diriger des Recherches, University of Versailles, January 2006.

[12] F. DANG NGOC. *Sécurisation du Contrôle d'Accès pour des Documents XML*, Ph. D. Thesis, University of Versailles, January 2006.

[13] B. FINANCE. *Accès Transparent et Sécurisé à des Données Largement Distribuées*, Habilitation à Diriger des Recherches, University of Versailles, January 2006.

[14] C. SAITA. *Groupement d'Objets Multidimensionnels Etendus avec un Modèle de Coût Adaptatif aux Requêtes*, Ph. D. Thesis, University of Versailles, January 2006.

Articles in refereed journals and book chapters

[15] N. ANCIAUX, L. BOUGANIM, P. PUCHERAL. *SGBD Embarqué dans une Puce : retour d'expérience*, in "Revue Technique et Science Informatiques (TSI)", to appear.

[16] N. ANCIAUX, L. BOUGANIM, P. PUCHERAL. *Data Confidentiality: to which extent Cryptography and Secured Hardware can help*, in "Annals of Telecom", Special issue on database security, vol. 61, n^{o} 3-4, 2006.

[17] L. BOUGANIM, F. DANG NGOC, P. PUCHERAL. *Fairness Concerns in Digital Right Management Models*, in "International Journal of Internet and Enterprise Management (IJIEM)", to appear.

[18] F. CUPPENS, P. PUCHERAL. *French Encyclopedia of Computer Sciences*, chap. Sécurité des Bases de Données, Vuibert Editions, ISBN 2-7117-4846-4, 2006.

Publications in Conferences and Workshops

[19] N. ANCIAUX, L. BOUGANIM. *Data Management in Embedded Smart Devices*, Tutorial, Smart University collocated with the 7th International e-smart Conference, 2006.

[20] D. SHASHA. *StrangerDB: Safe Data Management with Untrusted Servers*, Keynote Speech, 13th Int. Conf. on Management of Data (COMAD), Delhi, India, 2006.

[21] H.J.W. VAN HEERDE, N. ANCIAUX, L. FENG, P. APERS. *Balancing Smartness and Privacy for the Ambient Intelligence*, in "European Conference on Smart Sensing and Context (EuroSSC)", LNCS 4272 Springer 2006, ISBN 3-540-47842-6, 2006.

[22] H.J.W. VAN HEERDE. *Balancing Smartness and Privacy for the Ambient Intelligence*, in "Dutch-Belgian Database day", 2006.

Miscellaneous

[23] N. ANCIAUX, L. BOUGANIM, P. PUCHERAL. *Smart Card DBMS: where are we now?*, INRIA Technical Report 80840, 2006, http://hal.inria.fr/inria-00080840.

[24] N. ANCIAUX, H.J.W. VAN HEERDE, L. FENG, P. APERS. *Implanting Life-Cycle Privacy Policies in a Context Database*, CTIT Technical Reports, ISSN 1381-3625, University of Twente, 2006.

[25] L. BOUGANIM, ET AL. *ACI CASC Final Report*, 2006.

[26] L. BOUGANIM, ET AL. *Security of Information Systems*, Contribution to the Strategic Plan, 2006.

[27] B. FINANCE. *Contrôles d'accès dans XML*, Journées du GDR I3, 2006.

[28] B. FINANCE. *Protecting the Confidentiality of Electronic Health Records*, 13ièmes Journées INRIA- Industrie, 2006.

[29] D. SHASHA. *Biocomputational Puzzles*, Seminar, Ecole Polytechnique de Lausanne, Switzerland, 2006.

[30] D. SHASHA. *The Nature of Invention in Computer Science: a collaborative reflection based on the book: Out of their Minds*, Seminar, French Ministry of Research, Paris, France, 2006.

[31] H.J.W. VAN HEERDE. *Life-Cycle Privacy Policies for the Ambient Intelligence*, CTIT Symposium Poster Competition, 2nd price, 2006.

References in notes

[32] R. AGRAWAL, J. KIERNAN, R. SRIKANT, Y. XU. *Hippocratic Databases*, in "Proc. of the Int. Conf. on Very Large Data Bases (VLDB)", 2002.

[33] N. ANCIAUX. *Systèmes de Gestion de Bases de Données Embarqués dans une Puce Electronique*, Ph. D. Thesis, University of Versailles, France, 2004.

[34] N. ANCIAUX, C. BOBINEAU, L. BOUGANIM, P. PUCHERAL, P. VALDURIEZ. *PicoDBMS : Validation and Experience*, in "Proc. of the Int. Conf. on Very Large Data Bases (VLDB)", 2001.

[35] A. BARAANI, J. PIEPRZYK, R. SAFAVI-NAINI. *Security In Databases: A Survey Study*, 1996, http://citeseer.ist.psu.edu/baraani-dastjerdi96security.html.

[36] P. BONNET, J. GEHRKE, P. P. SESHADRI. *Towards Sensor Database Systems*, in "Proc. of Int. Conf. on Mobile Data Management", 2001.

[37] L. BOUGANIM, C. CREMARENCO, F. D. NGOC, N. DIEU, P. PUCHERAL. *Safe Data Sharing and Data Dissemination on Smart Devices*, in "Proc. of the ACM Sigmod Int. Conf. on Management of Data", 2005.

[38] F. CUPPENS. *Modélisation Formelle de la Sécurité des Systèmes d'Informations*, Habilitation à Diriger des Recherches, Université Paul Sabatier, 2000.

[39] H. HACIGUMUS, B. IYER, C. LI, S. MEHROTRA. *Executing SQL over Encrypted Data in the Database-Service-Provider Model*, in "Proc. of the ACM SIGMOD Int. Conf. on Management of Data", 2002.

[40] J. HE, M. WANG. *Cryptography and Relational Database Management Systems*, in "Proc. of the Int. Database Engineering and Application Symposium (IDEAS)", 2001.

[41] T. IMIELINSKI, B. NATH. *Wireless Graffiti – Data, data everywhere*, in "Proc. of the Int. Conf. on Very Large Data Bases (VLDB)", 2002.

[42] C. S. INSTITUTE. *CSI/FBI Computer Crime and Security Survey*, 2004, http://www.crime-research.org/news/11.06.2004/423/.

[43] S. MADDEN, M. FRANKLIN, J. HELLERSTEIN, W. HONG. *The design of an Acquisitional Query Processor for Sensor Networks*, in "Proc. of the ACM Sigmod Int. Conf. on Management of Data", 2003.

[44] ORACLE CORPORATION. *Advanced Security Administrator Guide*, in "Release 10.1", 2003.

[45] T. ÖZSU, P. VALDURIEZ. *Principles of Distributed Database Systems*, Second Edition, Prentice Hall, 1999.