INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Project-Team SMIS

Secured and Mobile Information Systems

Rocquencourt

THEME SYM

Activity Report

2005

Table of contents

1. Team

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

Vice-head of project team
Luc Bouganim [CR1 - INRIA]

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

Administrative assistant
Elisabeth Baque [AI - INRIA]

Ph. D. students
François Dang Ngoc [UVSQ - INRIA]
Saïda Medjdoub [UVSQ - INRIA]
Aurelian Lavric* [Paris 6 - Medience]
Cristian-Augustin Saita* [UVSQ - ATER]

Project technical staff
Nicolas Dieu [engineer ENSEEIHT, up to Oct. 2005]
Christophe Salperwyck [engineer Polytechnic Nantes, from Sept. 2005]

Graduate student intern
Mehdi Benzine [Master UVSQ]
François Boisson [ISTY3 engineer school]
Cosmin Cremarenco [Ecole Polytechnique de Bucarest]
Sonia Guehis [Master Dauphine]
Christophe Schmitz [Master UVSQ]

Previous members
Nicolas Anciaux [Post-doc position, Univ. Twente, Netherland, in P. Apers' team]
Sophie Giraud [Student IUFM, Toulouse]

2. Overall Objectives

2.1. Overall Objectives

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

The emergence of ubiquitous computing (access data anywhere, anyhow, anytime) and pervasive computing (smart objects, aware of their environment and able to transparently interact with it) 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 the data confidentiality and the definition of secured 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 device's 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 application's 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: 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., user's consent), 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's 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 [37]. 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 [33] are evolving towards real distributed databases in which each sensor acts as an active node (i.e., as a micro-data server queryable remotely) [39]. 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) [10]. 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 (location-aware queries, 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 [41], considering a reduced collection of homogeneous and more recently heterogeneous data sources managed by high-end servers. These methods are clearly 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 again, these works do not consider lightweight devices. The first works to consider distributed queries over lightweight devices have been conducted in the sensor network field. In this context, the data sources are however rather simple (collection of sensed data), the queries are usually filters and/or aggregations and the challenge in on organizing the data flow among sensors in order to reduce power consumption induced by radio frequency communications. 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 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 [38]. 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 control management and on the way access 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 [34]. The Discretionary Access Control model (DAC) gives the creator of an object the privilege to define the policy regulating access to this object, and granted privileges can be transmitted between users. The Mandatory Access Control Model (MAC) attaches security level to objects and clearance level to users in a centralized way. Other models like RBAC and TMAC introduce the concepts of Roles and Teams to improve the administration of access control policies for a large population of cooperating users. OrBAC proposes new abstractions to manage global access control policies in decentralized organizations. Each access control model is then instantiated in different ways depending on the underlying database model. 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 [29]. 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 also a very important issue. Server-enforced access control is widely accepted [32] but remains inoperative against insider attacks. Several attempts have been made to strengthen server-based security with database encryption [40] [36]. 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 [35]. Client-based decryption is also used in the field of selective data dissemination (e.g., Digital Right Management, P2P data exchange). 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 itself 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*, *home networks*, *sensor networks*.

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 to complement smart objects with Hippocratic features, a term introduced in [29] to denote DBMSs able to keep secret the data for which the owner did not give explicit delivery consent. The second one 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 chips can also help reducing the risk.

5. Software

5.1. Introduction

We present below two main prototyping activities started before 2005 but still active in 2005.

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 [31]. 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 [30] [21]. These experiments demonstrate the maturity of the PicoDBMS technology to manage portable folders fully embedded in secured chips. 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. 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. Link: http://www-smis.inria.fr/Eprototype_PicoDBMS.html.

5.3. Chip-Secured XML Access

Participants: François Dang Ngoc [correspondent], Luc Bouganim, Cosmin Cremarenco, Nicolas Dieu, 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 [8]. 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 [18]. An application scenario dealing with selective disseminations of multimedia content has been developed on top of this engine and has been the recipient of an international software award (see below). Link: http://www-smis.inria.fr/Eprototype_C-SXA.html.

5.4. Software Award

MobiDiQ is a fair Digital Right Management (DRM) engine embedded in a SIM card (cell phone smart card). Fair DRM means preserving the interest of all parties in a lucrative or non-profit dissemination of digital contents (e.g., free access to cultural contents for students or artists, parental or teacher control prohibiting access to non-ethical contents). MobiDiQ is nothing but an application scenario relying on the C-SXA technology. Complex and dynamic access control policies are defined on XML digital contents depending on personal data (e.g., history, user profile, etc.) stored securely on the SIM card.

This project has been rewarded by the Gold Award of the SIMagine'05 international software contest organized by Sun Microsystems, Axalto and Samsung Electronics (more than 300 participating teams). http://www.simagine.axalto.com/simagine2005_results.asp.

6. New Results

6.1. Embedded data management

Keywords: *benchmarks*, *co-design*, *query processing*, *storage and indexation models*, *ubiquitous and pervasive data management*.

Participants: Nicolas Anciaux, Luc Bouganim, Philippe Pucheral.

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 difficult problem is more on tackling the asymmetry between hardware resources (e.g., powerful CPU, tiny RAM) than simply on tackling the resource scarcity. This hardware setting entails a thorough re-thinking of existing database techniques [10]. 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. Since then (i.e., during the evaluation period), a benchmark dedicated to Pico-style databases has been designed and used to assess the relative performance of candidate storage and indexation data structures, both on a real smart card platform and on a cycle-accurate simulator. This study gives hints to select the appropriate storage and indexation structure for a given application according to the volume of embedded data, the required access rights and the expected response time. We also analyzed to which extent the introduction of secured chips in usual computing infrastructures broaden the scope of PicoDBMS applications and we identified important research perspectives in terms of data management on secured chips. This work has been submitted to ACM TODS [21] and concludes the PicoDBMS study. Our new research directions concern the management of large databases embedded in Smart Secured Mass Storage Cards.

6.2. Relationship-aware XML access control model

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

Participants: Béatrice Finance, Saïda Medjdoub, Philippe Pucheral.

The problem of regulating access to XML documents has attracted a considerable attention in recent years. Existing access control models attach authorizations to nodes of an XML document but disregard relationships between them. However, ancestor and sibling relationships may reveal information as sensitive as the one carried out by the nodes themselves (e.g., classification, correlation). We shown that these models hurt in a number of situations the basic need-to-know and user's consent principles enacted in most directives and laws related to the safeguard of personal information [12]. To tackle this important issue, we advocated the integration of ancestor and sibling relationships as first class citizen in the access control models for XML. We characterized three classes of relationship authorizations and identified the mechanisms required to translate them accurately in an authorized view of a source document. We introduced a rule-based formulation for expressing these classes of relationship authorizations and defined an associated conflict resolution strategy. Finally, we extended a public domain XML access control algorithm and conducted performance measurements showing the small overhead induced by the control of relationship authorizations [20]. The applicability of the proposed model was studied in the context of Electronic Health Record (HER) systems [19]. This work is a first step towards our research perspectives aiming at designing more powerful access control models and privacy models.

6.3. Tamper-resistant XML access control model

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

Participants: Luc Bouganim, François Dang Ngoc, Philippe Pucheral.

The erosion of trust put in traditional database servers and in Database Service Providers and the growing interest for different forms of selective data dissemination are different factors that lead to move the access control from servers to clients [13]. Different data encryption and key dissemination schemes have been proposed to serve this purpose. By compiling the access control rules into the encryption process, all these methods suffer from a static way of sharing data. We proposed a tamper-resistant, client-based, XML access right controller supporting flexible and dynamic access control policies. The access control engine is embedded in a hardware secure device and therefore must cope with specific hardware resources. This work, initiated in 2004 [8], has been pursued in 2005 with two main contributions [25]. First, we proposed a solution to solve pending situations where the delivery of a subpart of the input XML document is conditioned by predicates applying on values encountered afterward in the document stream; we shown that this situation is unfortunately frequent and must be tackled carefully. Second, we proposed a secure mechanism to refresh the access rights from a potentially malicious server which could use replay attacks to gain access to forbidden data. A prototype of the solution has been built and demonstrated at SIGMOD'05 [18]. An application scenario has also been developed on top of this prototype and has been the recipient of the gold award of the SIMagine 2005 international contest (see Section 5.4).

7. Contracts and Grants with Industry

7.1. National grants

7.1.1. Axalto (Schlumberger)

The SMIS project has a long lasting cooperation with Axalto (formerly Bull-CP8, then SchlumbergerSema). Axalto is one of 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. A CIFRE PhD thesis (PhD co-founded by an industrial partner and the French ministry of research) should start at the end of 2005 to study data management issues in the Smart Secured Mass Storage Card context.

7.1.2. UniMedecine

UniMedecine is a 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). While no formal cooperation exists yet, we are involved in a joint proposal to develop an experimental EHR platform with UniMedecine, Axalto, PRiSM lab, ALDS (a physician association). This project is under negotiation with the Yvelines district (conseil général des Yvelines).

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 (CASC coordinator: L. Bouganim), 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 cooperation with the following persons/institutions:

- Alejandro Gutiérrez (INCO, Uruguay): long lasting cooperation with INCO. Juan Diego Ferre has spent 3 months at INRIA (first quarter 2005) thanks to the INRIA-INCO internship program to work on embedded data management.
- Dennis Shasha (Professor at the University of New-York): Collaboration on secured data management issues. Dennis will do a sabbatical stay at SMIS from July 2006 to June 2007.

At the national level, SMIS members cooperate with several French labs and universities through national projects (see sections 7. and 8.).

Béatrice Finance, member of PRiSM, works as external partner in SMIS and Philippe Pucheral is still involved in PRiSM. A formal agreement of cooperation is under discussion between INRIA and UVSQ.

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. Five agreements have been signed in 2005 between INRIA and Parisian universities (Paris 1, Paris VI, Paris VII, Paris IX, UVSQ) to provide a financial support to research masters and doctoral schools.

Luc Bouganim is member of the Commission Délégations-Détachements of INRIA Rocquencourt since November 2004. He is the Scientific Coordinator (Informatics) of the CEA-EDF-INRIA summer schools.

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 VLDB'05, ICPS'06, UbiMob'05.
  - Member of the Scientific Board of the ARA 'Systèmes Embarqués et Intelligence Ambiante' (research program launched by the French ministry of research).
  - Member of the Scientific Board of the ACI 'Masses de données' (research program launched by the French ministry of research).
  - Member of the CNRS expert committee which evaluated the LRI Lab (Univ. of Orsay).
  - Member of the BDA Board (Bases de Données Avancées).
  - Member of the commission de spécialistes 27th section of the University of Cergy.
  - Referee for the PhD thesis of M. Thilliez (Univ. Valenciennes), L. Seitz (INSA Lyon) and C. Lepape (Univ. Paris 6).
- Luc Bouganim

  - PC member of VLDB’06, DASFAA’06, DMSN’05, SSI’05, BDA’05.
  - Member of the Editorial Board of TSI Journal (Technique et Science Informatiques).
  - Coordinator of the CASC ACI "Sécurité Informatique" project (2003-2006).

- Béatrice Finance

  - PC member of BDA’05.
  - Member of the Scientific Board of the UFR de sciences of the University of Versailles/St-Quentin.
  - Member of the commissions de spécialistes 27th section of the University of Versailles/St-Quentin.
  - Member of the PhD jury of T. T. Vu (Univ. J.F. Grenoble).

9.2. Teaching activity

The SMIS members have tight links with the University of Versailles/St-Quentin (UVSQ). Béatrice Finance is indeed assistant professor at UVSQ and Philippe Pucheral is professor at UVSQ, on secondment at INRIA. The list of the main courses given by each staff member in 2005 is given below:

- P. Pucheral: co-director of the research Master COSY (UVSQ), course on DBMS architecture (18h/y). Seminar on Database Confidentiality at ENS Cachan (Bretagne unit).
- L. Bouganim: DBMS architecture, data security, database technology (90h/y, given at UVSQ, ENS Cachan, ENST Paris)
- B. Finance: database technology, programming languages, mediation systems, distributed object systems (192h/y, given at UVSQ). She is also responsible for the 3rd year of the ISTY engineering school and member of the Administration Board of ISTY.

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] C. Bobineau, L. Bouganim, P. Pucheral, P. Valduriez. *PicoDBMS : Scaling down Database Techniques for the Smartcard*, in "Proc. of the 26th Int. Conf. on Very Large Data Bases (VLDB)", 2000.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] B. Finance, P. Dechamboux, G. Lebrun, Y. Lepetit, T. Delot. *LDAP, Databases and Distributed Objects : Towards a Better Integration*, in "Int. Workshop on Databases in Telecommunications, colocated with the Int. Conf. on Very Large Data Bases (VLDB), LNCS 2209, Springer 2001, ISBN 3-540-42623X", 2001.

[10] 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.

[11] 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.

Doctoral dissertations and Habilitation theses

[12] S. Medjdoub. *Modèle de contrôle d'accès pour XML : Application à la protection des données personnelles*, Ph. D. Thesis, University of Versailles, December 2005.

Articles in refereed journals and book chapters

[13] N. Anciaux, L. Bouganim, P. Pucheral. *Data confidentiality: to which extent cryptography and secured hardware can help*, in "Annals of telecom", vol. 60, 2005.

[14] L. Bouganim, F. D. Ngoc, P. Pucheral. *Sécurisation matérielle du contrôle d'accès à des documents XML*, in "Ingénierie des Systèmes d'Information (ISI)", vol. 10(2), 2005.

[15] L. Bouganim, F. D. Ngoc, P. Pucheral. *Tamper-Resistant Ubiquitous Data Management*, in "International Journal of Computer Systems Science and Engineering (IJCSSE)", vol. 20(2), 2005.

[16] F. Cuppens, P. Pucheral. *Encyclopédie Vuibert de l'informatique*, chap. “Sécurité des bases de données", Editions Vuibert, to appear, 2005.

[17] P. Pucheral. *Paradigmes et enjeux de l'informatique*, chap. “Ubiquité et confidentialité des données", published by the STIC Department of CNRS, Editions Hermès, ISBN 2-7462-1035-5, 2005.

Publications in Conferences and Workshops

[18] L. Bouganim, C. Cremarenco, F. D. Ngoc, N. Dieu, P. Pucheral. *Safe data sharing and data dissemination on smart devices*, in "Proceedings of the 24th ACM Sigmod International Conference on

Management of Data (demo session)", June 2005.

[19] B. FINANCE, S. MEDJDOUB, P. PUCHERAL. *Privacy of Medical Records: From Law Principles to Practice*, in "Proceedings of the 18th IEEE International Symposium on Computer-Based Medical Systems", June 2005.

[20] B. FINANCE, S. MEDJDOUB, P. PUCHERAL. *The Case for Access Control on XML Relationships*, Proceedings of the 14th ACM International Conference on Information and Knowledge Management (CIKM), November 2005.

Miscellaneous

[21] N. ANCIAUX, L. BOUGANIM, P. PUCHERAL. *Smart Card DBMS: where are we now?*, Submitted to ACM Transactions on Database Systems (ACM TODS), 2005.

[22] N. ANCIAUX, L. BOUGANIM, P. PUCHERAL. *SGBD Embarqué dans une Puce - étude de PicoDBMS*, Submitted to Techniques et Sciences Informatiques (TSI), 2005.

[23] L. BOUGANIM. *MobiDiQ: Mobile Digital Quietude, 3GSM World congress*, Invited talk, February 2005.

[24] L. BOUGANIM, N. DIEU, P. PUCHERAL. *MobiDiQ: Mobile Digital Quietude, Gold Award of the SIMagine 2005 international software contest*, 2005, http://www.simagine.axalto.com.

[25] L. BOUGANIM, F. D. NGOC, P. PUCHERAL. *Dynamic access control policies on encrypted XML data*, Submitted to ACM Transactions on Information and System Security (ACM TISSEC), 2005.

[26] L. BOUGANIM, ET AL.. *ACI CASC Mid-term deliverable*, 2005.

[27] B. FINANCE, S. MEDJDOUB, P. PUCHERAL. *The Case for Access Control on XML Relationships*, Rapport INRIA n°RR-5446, Le Chesnay, Rocquencourt, 2005, http://www.inria.fr/rrrt/rr-5446.html.

[28] P. PUCHERAL. *A Data-Centric Approach of Smart Devices, International Workshop on Construction and Analysis of Safe, Secure and Interoperable Smart Devices*, Invited talk, March 2005.

Bibliography in notes

[29] R. AGRAWAL, J. KIERNAN, R. SRIKANT, Y. XU. *Hippocratic Databases*, in "Proceedings of the International Conference on Very Large Data Bases (VLDB)", 2002.

[30] N. ANCIAUX. *Systèmes de gestion de bases de données embarqués dans une puce électronique*, Ph. D. Thesis, University of Versailles, France, December 2004.

[31] 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.

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

[33] P. BONNET, J. GEHRKE, P. P. SESHADRI. *Towards Sensor Database Systems*, in "Proceedings of the Mobile Data Management", 2001.

[34] F. CUPPENS. *Modélisation formelle de la sécurité des systèmes d'informations, Habilitation à Diriger les Recherches, Université Paul Sabatier*, 2000.

[35] H. HACIGUMUS, B. IYER, C. LI, S. MEHROTRA. *Executing SQL over encrypted data in the database-service-provider model*, in "Proceedings of the ACM SIGMOD International Conference on Management of Data", 2002.

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

[37] T. IMIELINSKI, B. NATH. *Wireless Graffiti – Data, data everywhere*, in "Proceedings of the International Conference on Very Large Data Bases (VLDB)", 2002.

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

[39] S. MADDEN, M. FRANKLIN, J. HELLERSTEIN, W. HONG. *The design of an acquisitional query processor for sensor networks*, in "Proceedings of the ACM Sigmod International Conference on Management of Data", 2003.

[40] ORACLE CORPORTION. *Advanced Security Administrator Guide*, in "Release 10.1", 2003.

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