# Canada-France Planning Meeting on Security
# December 6-8, 2007
# Simon Fraser University, Vancouver, BC
# Minutes

## Participants

Bill Aiello, University of British Columbia

(http://www.cs.ubc.ca/people/profile.jsp?id=aiello0)

Pierre Dusart, (http://www.unilim.fr/laco/perso/pierre.dusart/)

Eric Filiol, INRIA (http://www-rocq.inria.fr/codes/Eric.Filiol/English/index.html)

Arvind Gupta, MITACS

Guillaume Hanrot, INRIA (http://www.loria.fr/~hanrot/)

Bruce Kapron, University of Victoria (http://webhome.cs.uvic.ca/~bmkapron/)

Claude Kirchner, INRIA (http://www.inria.fr/personnel/Claude.Kirchner.en.html)

Evangelos Kranakis, Carleton University (http://www.scs.carleton.ca/~kranakis/)

Pascal Lafourcade, (http://www-verimag.imag.fr/~plafourc/Pascal_index_en.php)

Rebeccah Marsh, MITACS

Laurence Meadows, MITACS

Alfred Menezes, University of Waterloo (http://www.math.uwaterloo.ca/~ajmeneze/)

Rei Safavi-Naini, University of Calgary (http://pages.cpsc.ucalgary.ca/~rei/)

Phong Q. Nguyen, École normale supérieure ( http://www.di.ens.fr/~pnguyen/)

Prakash Panangaden, McGill University (http://www.cs.mcgill.ca/~prakash/)

Danielle Ziebelin, French Ministry of Foreign Affairs

## Thursday, December 6, 2007

### 1. Introduction and goals of meeting, Evangelos Kranakis

### 2. Overview of MITACS, Arvind Gupta

- have workshops where industrial partners are present to help explore this type of collaboration - perhaps not that easy in the area of security, but need to think about how to structure it to encourage companies to attend

### 3. French Consulate programs, Danielle Zibbelin

- Discussed funding for research exchanges
- France-Canada Research Fund: research grant money for joint France-Canada projects; starts with pre-proposal, then each university picks at most 3 to submit a full proposal; 15 projects selected and funded at $10K per year for two years; 3 of these projects will get a PhD grants for 3 years ($40K per year) for French or Canadian students who are "co-supervised"
- Graduate grants have 1 call per year, travel grants have 2 calls per year
- More info: http://www.ambafrance-ca.org/scientifique

### 4.MITACS International Initiatives, Rebeccah Marsh

- There is interest by INRIA in international internships
- Codirection of the student is key
- Separate programs for MSc, PhD, postdoc?
- If possible, make it as part of a research project

### 5. Security Research in France, Claude Kirchner

- INRIA and CEA
- Security: by the time people realize there is a problem, it's too late
- Projects funded ~200K for 3 years
- 25% of 160 INRIA teams work in security
- Total funding: ~5M
- Very broad range of projects

  - Ex: formal methods, proof and verification
  - Ex: Link between safety and security (interface between computer system and infrastructure system) - airport security
- They ask for proposals in English, but get many in French
- ANR: French funding agency created in 2005 – no projects directly in security
- Could explore an NSERC-ANR connection
- INRIA Website: lists collaborations between French and Canadian researchers
  - 20K Euros for a couple years to start a project (no requirement for Canadian contribution)
  - List visitors as # and length of visits in # persons*months
  - Number of INRIA -> Canada visitors and number of Canadians -> France visitors
- INRIA internship program
  - INRIA selects university partners and program and then advertizes the programs; students from those partners can then do an internship at INRIA
  - 50% paid by INRIA and 50% paid by the INRIA research team
  - Knowledge transfer
- INRIA has agreement with FQRNT (FQRNT gives some money for visits, events, etc.)
- McGill (VP Research) has a direct agreement with INRIA and provides funding
- INRIA-Industry Security Day has 120 industry people show up
- Strategic directions: security law, viruses, defense and attack, safety and security, smart cards, OS and security, network management and security, crisis management, e-vote, medical files

**6. Security Research in Canada, Evangelos Kranakis**

- Goals of security research: strengthen emerging areas, amplify strengths in Canada, incorporate security research within existing projects, study and research all mathematical aspects of security
- Overview of MITACS projects in the security theme
- Suggestion: invite NRC researchers working on information security to next meeting

**7. Cryptography and Number Theory, Alfred Menezes**

- Some existing collaborations with French researchers

## Friday, December 7, 2007

**1. Cryptology, Phong Nguyen**

- Cryptography in France and ENS
- Two INRIA teams: CODES and TANC
- ENS Crypto team, leader is David Pointcheval (CNRS), became an INRIA team this year
- Focus on public-key crypto
- Would like minimal administration of a joint program
- Interested in exchanges
- Too many conferences already, but interested in a satellite meeting before or after an existing conference

**2. Arithmetic and Cryptology, Guillaume Hanrot**

**3. Formal Methods and Verification, Pascal Lafourcade**

- Possibility of exchanges with Alfred's group

4. **Formal Methods and Verification, Prakash Panangaden**
    - Already working with Catuscia Palamidessi at INRIA
    - Other possible collaborations include Jean Gombault, Josee Descharnais, Vincent Danos

5. **Tools for Specifying and Verifying Software, Claude Kirchner**

6. **Formal Methods and Verification, Bruce Kapron**

7. **Computer Virology, Eric Filiol**
    - Already working with John Aycock at University of Calgary and Jose Fernandez at Ecole Polytechnique (who has no students)

8. **Components for Smartcards, Secure and Modular Operating Systems, Pierre Dusart**
    - Industrial partners: Gemalto, Trusted Labs and Trusted Logic, Thales Security

9. **Security Applications, Rei Safavi-Naini**

10. **Network Security, Bill Aiello**

11. **Network Security and Vehicular Security**

## Saturday December 8, 2007

**Henry Lee**
Manager, Security Policy and Officer
Office of the Chief Information Officer

- Building an information security policy and an Information Security Program (developed in 2006, implemented in 2007)
- Goals: promote research, build a network to facilitate research in province, enhance info sharing among the community and between academia and government
- Areas of interest: cyber crime, network security, identity management
- Activities: ISR grants, postsecondary curriculum development (with UVIC CS and ECE, and Security Option within BEng), conference and workshops, internal research, build research centres of excellence
- Issued 2.5M for 30+ projects in BC

**IDEA: technical training or networking event for ABC, in conjunction with OCIO (they could provide teaching, MITACS could cover student and event costs)

- Events: Privacy and Security, Feb
- West Coast Security Forum, Nov
- Security Day (semi-annual)
- Protection of Information Awareness (as requested)

Research Centre of Excellence: what does this mean exactly?

## Brainstorming Session

**Joint Activities:**

**1. Canada-France Congress**

- possible approaches:
    - pick a few themes with an “organizing committee”, who will develop a road map for research, activities, exchanges, etc
    - or start with a document describing the entire project, with one leader, plan for activities, etc.
    - or pick a problem area and use various methods to solve it (organize by a problem or techniques)
    - or do a bottom up approach (start with student exchange to build trust and relationships, bootstrap off common interests)

**2. “Canada-France Information Security Program”**

- May-June: current topics (crypto, formal methods, malware, network security) plus discussion of new topics (call for general presentations)
- then write short document/proposal describing way to move forward (2 pages per topic)
- include student talks
- plenary speaker in each session?
- organizing committee: 2 Canadians + 2 French + 2-3 from user community (Guillaume and Pascal, Evangelos Kranakis and Bill Aiello, Loic Duflot from French Security Agency, Henry Lee, Alcatel in both countries, Bell Canada)

**3. Summer/Fall School**

- one week school
- potential dates: October 13-19, 2008

- advertize at June meeting
- alternate Canada then France each year, focusing on the strengths of the country
- potential topics: "trusted platforms" hardware or secure systems (focus on TPM and smart cards), software engineering focused on security, software verification, virtual machines
- invite people from the TPM industry (contact Bill to get suggested names)
- have someone from both countries on organizing committee
- need to advertize by April 2008
- organizers: maybe David Lee (U of T) from Canada
- ALTERNATIVE: run a short school at Canada-France Congress, then another school in France in 2009, then another one in Banff in 2010

**4. Exchange Program:**

- support travel and accommodation costs
- 5 going and 5 coming
- idea is for France to pay for Canadians and MITACS to pay for French students
- need budget (maybe $25K per year)
- student internship program

**4. Joint graduate students, cosupervised by supervisors in Canada and France**

- French prof can be on committee of Canadian students

**Funding from the French side:**

- French consulate: can only pay for CDN students to go to France
- INRIA: http:///www-direction.inria.fr/international
- associated team, Oct deadline

- internship program, 2 calls per year at preselected universities (INRIA pays 50% of costs)
- PhD mobility program (CORDI with requested mobility)
- postdoc programs at INRIA
- sabbatical money for INRIA profs and Explorators to go outside France
- CNRS PhD program to work at CNRS

**Suggestion:** make a map of security research in Canada (similar to that presented by France)

### Administration

- MITACS will take the lead on the administration in Canada

### Actions Points

- Sign funding agreement between countries
  - envision $50K per country for joint events, and each country is responsible for coming up with the
- Website for collaboration (Rebeccah)
- Canada-France summer school attached to Congress
  - Form the organizing committee (Dec 19, 2007)
  - Scope of the program + list of invitations (Jan 15, 2008)
  - Invitations and posters sent out (Feb 1, 2008)
  - Evangelos is Chair of steering committee
- Need working agreement between Canada and INRIA (Arvind and Claude)
- Set up steering committee (1 MITACS staff, 1 MITACS scientist, 1 INRIA staff, INRIA scientist) to help organize next activities

    - Designate scientific chair of committee

**Questions:**

- Funding through European Framework 7
    - funding for exchanges
    - takes a lot of work to prepare