

GURVAN LE GUERNIC

13 rue du douet
35510 Cesson-Sévigné
France

Born in January 1979

@: gleguern@gmail.com
🌐: www.Le-Guernic.info

INRIA-Microsoft Research Joint Center
Parc Orsay Université
28, rue Jean Rostand
91893 Orsay Cedex
France

☎: (+33) 6 33 84 36 62
☎: (+33) 1 69 35 69 90
📠: (+33) 1 69 35 69 69

ÉDUCATION

- 2002–2007 **PhD thesis** in computer science from [Université de Rennes 1](#) and [Kansas State University](#).
- Title: Confidentiality Enforcement Using Dynamic Information Flow Analyses
- Advisors: [Thomas Jensen](#), [David Schmidt](#) and [Anindya Banerjee](#)
- Grants: **Research Grant** from the French research government department, **Mobility Grant** from the French research government department, **Graduate Research Assistantship** from Kansas State University and **Graduate Teaching Assistantship** from Université de Rennes 1 (ATER).
- Defense: 27th of September 2007 in France and 25th of October 2007 in the US
- 2003 One year of studies spent at **Kansas State University**.
Course work includes: “*Formal Language Theory*”, “*Software Specification*”, “*Programming Language Design*”, “*Verification and Validation*”, and “*Language Based Security*”.
- 2002 **Research Master** (Diplôme d’Études Approfondies — DEA) in computer science from [INSA Rennes](#) and [IRISA](#).
Course work includes: “*Logical Programming*”, “*Temporal and Spatial Reasoning*”, “*Analyses of Reactive and Distributed Systems*”, “*Programs Semantics and Analyses*”, “*Complexity*”, “*Cryptography*”, “*Processors Architectures and Optimizations*”, and “*Advanced Programming*”.
- 2002 **Professional Master** (Diplôme d’ingénieur) in computer science from [INSA Rennes](#).

POSTDOC

2007-2009

At [INRIA-Microsoft Research Joint Center](#) with [Cédric Fournet](#) and [Tamara Rezk](#).

The goal of the project is to cryptographically secure information flows of distributed programs. We build and prove the correctness of a translation mechanism from sequential source programs to distributed target programs. The source program is a sequential program with annotations regarding the distribution of the target program. The source program uses a shared memory whose protection mechanism relies on security labels associated to variables. The translation mechanism returns a distributed program whose threads use local memory for their execution. Communication of values between threads of the target language is achieved through a shared memory of encrypted and signed values.

THESIS RESEARCH

Keywords

Program Analyses, Semantics, Confidentiality, Noninterference, Information Flows, Monitoring, Dynamic Analyses.

Subject

With the intensification of communication in information systems, interest in security has increased. Security is usually partitioned into three domains: *confidentiality* focuses on controlling the dissemination of secret information, *integrity* is concerned with maintaining the incorruptibility of trusted information, and *availability* ensures the accessibility of resources to legal users. My thesis work deals with the problem of confidentiality from the point of view of *noninterference*. This notion is based on ideas from classical information theory. It has first been introduced by Goguen and Meseguer as the absence of *strong dependency*.

“One group of users, using a certain set of commands, is noninterfering with another group of users if what the first group does with those commands has no effect on what the second group of users can see.”

A program is said to be *noninterfering* if the values of its public outputs do not depend on the values of its secret inputs. If that is not the case then there exist illegal information flows that allow an attacker to gain information about the secret inputs of the program by looking at values of its public outputs.

I started my thesis by a thorough bibliographic research which showed that the vast majority of noninterference analyses are based on static analyses (especially type systems). In 2002, there were few dynamic noninterference analyses. The majority of which dated from the seventies. However, dynamic analyses can be more precise than static analyses by benefiting from a more precise knowledge of the control flow of the program analyzed. This has been demonstrated in a paper published in the proceedings of [ASIAN'06](#). My thesis concerns the development of dynamic information flow analyses following two approaches. The first one is based on a security automaton directing a noninterference monitoring semantics. The second approach is semantics-based and uses context-sensitive static information flow analyses. Noninterference monitors have been developed for a sequential language and a concurrent language including synchronization commands. Those monitors have been proved to be sound with regard to the notion of noninterference. They also have been proved to be more precise than their equivalent type systems developed by Volpano, Smith et Irvine.

PUBLICATIONS

International Refereed Conferences and Workshops

- CCS'09 Cédric Fournet, Gervan Le Guernic and Tamara Rezk (2009). **A Security-Preserving Compiler for Distributed Programs**. In *Proceedings of the ACM Conference on Computer and Communications Security*. pp 432–441. Chicago, USA. Acceptation rate: 58 articles out of 315 submitted (18%).
- VERIFY'08 Gervan Le Guernic (2008). **Precise Dynamic Verification of Confidentiality**. In *Proceedings of the International Verification Workshop*. CEUR Workshop Proceedings 372, pp 82–96. Sydney, Australia.
- ASIAN'07 Gervan Le Guernic (2007). **Information Flow Testing**. In *Proceedings of the Annual Asian Computing Science Conference*. LNCS 4846, pp 33–47. Doha, Qatar. Acceptation rate: 15 long articles (including this one) and 10 short articles out of 112 submitted and 65 reviewed (22%).
- CSF'07 Gervan Le Guernic (2007). **Automaton-based Confidentiality Monitoring of Concurrent Programs**. In *Proceedings of the IEEE Computer Security Foundations Symposium*. pp 218–232. Venice, Italy. Acceptation rate: 25 articles out of 101 submitted (25%).
- RULE'07 Gervan Le Guernic and Julien Perret (2007). **FLIC: Application to Caching of a Dynamic Dependency Analysis for a 3D Oriented CRS**. In *Proceedings of the International Workshop on Rule-Based Programming*. Paris, France.
- ASIAN'06 Gervan Le Guernic, Anindya Banerjee, Thomas Jensen and David Schmidt (2006). **Automata-based Confidentiality Monitoring**. In *Proceedings of the Annual Asian Computing Science Conference*. LNCS 4435, pp 75–89. Tokyo, Japan. Acceptation rate: 17 long articles (including this one) and 10 short articles out of 115 submitted (23%).
- FCS'05 Gervan Le Guernic and Thomas Jensen (2005). **Monitoring Information Flow**. In *Proceedings of the Workshop on Foundations of Computer Security*. pp. 19–30. Chicago, IL, USA. Published by DePaul University. Acceptation rate: 11 articles out of 30 submitted (37%).

International French-speaking Refereed Conferences

- MajecSTIC'06 Nicolas Bonnel and Gervan Le Guernic (2006). **Système de recherche de méthodes Java basé sur leur signature**. In *Proceedings of Majecstic 2006*. Lorient, France.
- MajecSTIC'05 Gervan Le Guernic and Julien Perret (2005). **FL-system's Intelligent Cache**. In *Proceedings of Majecstic 2005*. pp 79–88. Rennes, France. Acceptation rate: 43 articles out of 92 submitted (47%).

Technical Reports

- [Precise Dynamic Verification of Noninterference.](#)
- [Dynamic Noninterference Analysis Using Context Sensitive Static Analyses.](#)
- [Automaton-based Non-interference Monitoring of Concurrent Programs.](#)
- [Automaton-based Non-interference Monitoring.](#)

PROTOTYPES

- CFlow** *Lead developer (F#, .NET). Compiler for distributed programs enforcing safe information flows via cryptography.*
- JMBrowser** *Lead developer (Java, SWT, Derby). Java method browser based on method signature distances.*

TEACHING EXPERIENCE

- Computer Hardware Architecture**
Undergraduate level, 48h of lab work in 2007
- Introduction to the PHP language**
Undergraduate level, 10h of course work in 2007
- Introduction to XML**
Graduate level, 6h of lab work in 2007
- Internet Networks and Communications**
Graduate level, 6h of course work and 20h of lab work in 2006
- Methodologies for Object Oriented Design**
Graduate level, 8h of course work and 24h of lab work in 2006
- Initiation to Algorithms**
Undergraduate level, 18h of lab work in 2004 and 28h of lab work in 2002

OTHER EXPERIENCES

- February to June 2002 Internship at [IRISA](#) on the analysis of concurrent Java programs.
- July and August 2001 Development of a network supervision tool at ReefEdge, USA.
- July and August 2000 Development and maintenance of web sites at [MBA multimédia](#).
- August 1999 Summer job at [France Telecom](#), France.
- July and August 1998 Summer job at [Yellowstone National Park](#), USA.

CERTIFICATIONS

- TOEFL®** *Test Of English as a Foreign Language*
Scores in September 2002: Listening - 26 / 30, Structure/Writing - 26 / 30, Reading - 30 / 30. Total - 273 / 300. Essay Rating - 4.5 / 5.
<http://www.ets.org/toefl>
- GRE®** *Graduate Record Examinations*
Scores in September 2002: Verbal - 400 / 800, Quantitative - 780 / 800, Analytical - 700 / 800.
<http://www.ets.org/gre>