CoChaT

Covert Channels in Timed Systems

Responsable : Béatrice Bérard

Partenaires.
LIP6 (Laboratoire d'Informatique de Paris 6), Université Pierre et Marie Curie,
EDITE de Paris (Ecole Doctorale Informatique, Télécommunications et Electronique) pour le rattachement du doctorant impliqué dans le projet,
LSV (Laboratoire Spécification et Vérification), Ecole Normale Supérieure de Cachan.

Scientific description.
The description consists of four sections.

1. Description of the joint research activities of the two researchers involved in the project : B. Bérard (LIP6) and S. Haddad (LSV).
2. Project setting as a PhD's subject, planning and deliverables.
3. Motivations for the CoChaT project.
4. Scientific objectives of the project.

1. Former joint activities

Serge Haddad was professor at Université Paris-Dauphine when I obtained a position of professor there in september 2004. We did some research work together from this time on, and this cooperation went on after our respective position changes : in Ecole Normale Supérieure de Cachan (feb. 2008) for S. Haddad and in Université Pierre et Marie Curie (sept. 2008) for me.

More precisely, a first step of this cooperation, which was joint work with researchers from laboratory IRCCyN in Nantes, was devoted to the study of relations between two classes of timed models which were well known in our respective communities : Time Petri Nets (TPN) and Timed Automata (TA). This led to three communications in international conferences and a journal paper [BCH$^+$05c, BCH$^+$05a, BCH$^+$05b, BCH$^+$08]. The first problem concerned the usual semantics of TPN, which did not seem to fit the specification of some classes of timed systems. We proposed two variants for the semantics of TPN and compared their expressive power [BCH$^+$05a]. We then investigated the comparisons between TPNs and TA, from the point of view of language equivalence an bisimulation. While bounded TPNs and TA are language-equivalent, we proved that TA are more powerful when considering bisimulation [BCH$^+$05c], and we gave a characterization of the subclass of TA which are bisimilar to a TPN.

Following this work, we became part of the ANR-SETIN project DOTS (Distributed Open Timed Systems) whose aim is to study complex systems where two features appear among the three (or the three together). Concerning open timed systems, we proposed [BH09a] a new model of so-called Interrupt Timed Automata, well suited to the modeling of timed systems with several interrupt levels. Since interrupt clocks are a special case of stopwatches, this class can be viewed as a subclass of hybrid automata. However, while the reachability problem is undecidable for hybrid automata, we proved [BH09b] that it is decidable in 2-NEXPTIME.

A second cooperation, related to the PhD thesis of L. M. Hillah, was started later with the MoVe team of laboratory LIP6. This work concerns the area of Intelligent Transport Systems (ITS), for which the current approach is centered on safety strategies to ensure properties such as Collision Avoidance. In [BHH$^+$08], we propose a (discrete time) model of an automatic motorway system and a control algorithm to ensure collision avoidance.

Finally, with F. Kordon (LIP6) and L. Petrucci (LIPN), we started in 2005 the organisation of the research group MeFoSyLoMa (Méthodes Formelles pour les Systèmes Logiciels et Matériels), where 8 laboratorie join their effort to compare points of views about Formal Methods for Hardware and Software Systems : CEDRIC (Cnam), IBISC (Univ. Evry), LACL (Univ. Paris 12), LAMSADE (Univ. Paris-Dauphine), LIP6 (UPMC), LSV (ENS de Cachan) and LTCI (Télécom Paris Tech). In this context, we were involved in a collective work producing a survey [HKP06], we participated in the organisation of the conference FORTE'06 (26th conference on Formal Techniques for Networked and Distributed Systems), we prepare the conference ATPN'09 (30rd International Conférence on Application and Theory of Petri Nets and Other Models of Concurrency), for next june in Paris, and we co-organise, with L. Pautet (Télécom Paris Tech) the next edition of the Summer School on Real Time (ETR'09, september 2009).

2. Project setting, planning and deliverables

This cooperation, which started in 2004 and went on in the ANR project DOTS, will be strengthened by the specific activity in the CoChaT project (Covert Channels in Timed Systems), for which we propose a PhD's subject. The problem considered in CoChaT is loosely connected to DOTS and to some activities in the MeFoSyLoMa group.

The cooperation will also involve joint work with :

- Olivier H. Roux and D. Lime, researchers from IRCCyN (Research Institute in Communication and CYbernetics, Nantes) who have already worked on timed non-interference and are currently supervising a PhD on this subject,
- John Mullins from Ecole Polytechnique de Montréal (Canada), who is an expert on cryptographic protocols and system security.

As a PhD subject, the project is intended for a duration of three years with expected results in terms of publications. The planning can be divided into four steps :

1. Consitution of state of the art on covert channels, with an accent on case studies describing timing channels ;
2. Formal framework for the description and properties of timing channels ;
3. Decision problems for the design of detection and verification algorithms ;
4. Manuscript redaction.

Deliverables will include :

1. A half term report to present the current state of the work, mostly about the first two phases of the project ;
2. The PhD manuscript at the end of the three years which will constitute the final report of the project.

3. Motivations

Many systems today are designed for large scale communications and resource sharing, allowing users to send or fetch programs for calculation tasks or IO operations. When these programs deal with communication of secret or classified data, they must ensure that no information leak occur, either maliciously or inadvertently. This is one of the key aspects of the security concerns, that is often called *secrecy*. The *information flow analysis* addresses this question by clarifying conditions ensuring that a flow of information in a program is safe.

Different conditions have been defined to reach this goal. The first one, *non interference*, was proposed in [GM82] with the aim to capture causal dependencies between actions from different user groups. Roughly speaking, they require that high-level information never flows into low-level channels. Verification of information flow security has thus become an emergent field of research in computer science with a success story in its application to the analysis of cryptographic protocols where numerous uniform and concise characterizations of information flow security properties (*e.g.* confidentiality, authentication, non-repudiation or anonymity) in terms of non-interference have been proposed. Generalized notions of non-interference were then designed to include (nondeterministic) labeled transition systems and finer notions of observational semantics like bisimulation [FG01, Rya01, PR99].

However, it has been argued that non-interference is too strong a requirement and, more recently, the notion of *opacity* [BKMR06, BBB$^+$07] has proved to be another promising technique for describing security properties, both for Petri nets and classical transition systems, and it was applied to a simple voting system.

Finally, a still weaker condition was proposed as the absence of a *covert channel*. A covert channel has been described in [HZJ03, HZD04, Hél04, Deg05] as a kind of *iterated* interference, when an arbitrary long sequence of information leaks can occur.

It is well known that timing observations can be specifically exploited to transmit information. Thus, abstracting quantitative time constraints from a system can hide the fact that the system is not secure. While non interference conditions have been partly investigated recently [RFM03, BT03, GMR05] in a timed setting, not much attention has yet been devoted to timing channels.

4. Scientific objectives

Attacks with timing channels have been described and simulated for instance on TCP/IP protocols [CBS04], Web communications [FS00] or cryptographic operations [Koc96, Ber05b, Ber05a]. The scientific objective of the CoChaT project is to study the conditions under which such attacks can occur in timed systems, with two main directions.

a. The first step consists in defining a theoretical framework, in which timing channels can be formally described.

b. A second part of the work concerns the design of detection and verification algorithms, for which decidability issues are involved.

Progress in both steps will have to take into account practical examples like the case studies mentionned above, in order to validate the formal approach.

a. Timed models for timing channels. This part of the work is centered on expressivity questions : how to capture the notion of timing channel in a given formalism ?

Natural models to start with are the timed extensions of classical transition systems or logics, which have been largely studied, for both discrete and dense time, for the last twenty years. For instance, timed automata, introduced by Alur and Dill [AD94], handle real valued variables called clocks. The value of a clock evolves synchronously with time, and can be compared with a constant or reset by the firing of discrete transitions. Timed extensions of Petri nets have also been defined [Mer74, Ram74] and proved useful for the description of timed concurrent systems. In Time Petri Nets (TPN), a time interval controls the firing of a transition. Both models have also been extended with more powerful variables, which may evolve with an arbitrary rate (hence not always equal to 1) [ACH$^+$95, RD02, BLRV04], like for instance *stopwatches*, for which the slope can be 1 or 0.

While the previous models are used to describe systems with timing constraints, the properties related to timing channels can be expressed in timed logics, for instance extended versions of LTL [OW05]. On the other hand, timing channels can be naturally expressed in terms of games between attackers and the communication system. Based on the untimed logic ATL [AHK97], which takes into account agent strategies for games, the timed extension TATL [BLMO07, LMO08] has been defined for the timed setting and will be used for these specification purposes.

b. Detection and verification. Timed automata constitute the simplest class of timed models, in which various verification problems like reachability or model-checking turned out to be decidable [ACD93]. For TPNs, the reachability problem is undecidable, but the k-boundedness problem and thus the reachability problem for bounded TPNs are decidable [BD91]. In the extended classes, for instance with general stopwatches, most verification problems are undecidable [ACH$^+$95, RD02, BLRV04] and semi-algorithms have been designed in these cases. As verification techniques were lifted from untimed to timed models, several timed model-checkers could then be developed and successfully applied to industrial cases : CMC [LL98], KRONOS [Yov97], UPPAAL [LPY97] for timed automata, HYTECH [HH95] for hybrid automata, and ROMEO [GLMR05], TINA [BRV04] for time Petri nets and time Petri nets with stopwatch.

Detection algorithms are closely related to decidability properties of a subclass of formulas in the timed logics mentioned above. We intend to identify those subclasses for which efficient algorithms could be designed. This would help characterize secure systems where no timing channel can be implemented. More prospective research directions include :

- the control problems, which asks if there exists a program (the controller) able to restrict the system so that no timing channel can occur ;
- the design of a high level formalism with semantics in terms of timed transition systems, in which verification traces could be expressed to help user friendly diagnosis.

These subject will most probably be investigated only after the end of the PhD work, in a possible sequel of the project.

Références

[ACD93] R. Alur, C. Courcoubetis, and D. Dill. Model-checking in dense real-time. *Information and Computation*, 104(1) :2–34, May 1993.

[ACH$^+$95] R. Alur, C. Courcoubetis, N. Halbwachs, T. A. Henzinger, Pei-Hsin Ho, X. Nicollin, A. Olivero, J. Sifakis, and S. Yovine. The algorithmic analysis of hybrid systems. *Theoretical Computer Science*, 138(1) :3–34, 1995.

[AD94] R. Alur and D. Dill. A theory of timed automata. *Theoretical Computer Science B*, 126 :183–235, 1994.

[AHK97] R. Alur, T. A. Henzinger, and O. Kupferman. Alternating-time temporal logic. In *Proc. 38th Symposium on Foundations of Computer Science (FOCS'97)*, pages 100–109, 1997.

[BBB$^+$07] E. Badouel, M. Bednarczyk, A. Borzyszkowski, B. Caillaud, and P. Darondeau. Concurrent secrets. *Discrete Event Dynamic Systems*, 2007.

[BCH$^+$05a] B. Bérard, F. Cassez, S. Haddad, D. Lime, and O.H. Roux. Comparison of different semantics for time Petri nets. In *Automated Technology for Verification and Analysis (ATVA'05)*, volume 3707 of *Lecture Notes in Computer Science*, pages 293–307, Taipei, Taiwan, October 2005. Springer.

[BCH$^+$05b] B. Bérard, F. Cassez, S. Haddad, D. Lime, and O.H. Roux. When are timed automata weakly timed bisimilar to time Petri nets ? In *25th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2005)*, volume 3821 of *Lecture Notes in Computer Science*, Hyderabad, India, December 2005. Springer.

[BCH$^+$05c] B. Bérard, F. Cassez, S. Haddad, O.H. Roux, and D. Lime. Comparison of the Expressiveness of Timed Automata and Time Petri Nets. In P. Pettersson and W. Yi, editors, *Proceedings of the third International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS'05)*, volume 3829 of *Lecture Notes in Computer Science*, pages 211–225, Uppsala, Sweden, September 2005. Springer.

[BCH$^+$08] B. Bérard, F. Cassez, S. Haddad, D. Lime, and O. (H.) Roux. When are timed automata weakly timed bisimilar to time Petri nets ? *Theoretical Computer Science*, 403(2-3) :202–220, 2008.

[BD91] B. Berthomieu and M. Diaz. Modeling and verification of time dependant systems using time petri nets. *IEEE Transactions on Software Engineering*, 17(3) :259–273, March 1991.

[Ber05a] D. J. Bernstein. Cache-timing attacks on AES. Technical Report 1109, 2005.

[Ber05b] D. J. Bernstein. The Poly1305-AES message authentication code. In *Proc. of FSE 2005*, number 3557 in Lecture Notes in Computer Science, 2005.

[BH09a] Beatrice Bérard and Serge Haddad. Interrupt Timed Automata. In *Proceedings of the 12th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS'09)*, volume 5504 of *Lecture Notes in Computer Science*, pages 197–211, York, GB, March 2009. Springer.

[BH09b] Beatrice Bérard and Serge Haddad. Interrupt Timed Automata : a step further. Technical Report LSV-09-1, Lab. Specification and Verification, ENS de Cachan, Cachan, France, January 2009. 24 pages.

[BHH$^+$08] B. Bérard, S. Haddad, L. M. Hillah, F. Kordon, and Y. Thierry-Mieg. Collision Avoidance in Intelligent Transport Systems : towards an Application of Control Theory. In *Proceedings of the 9th International Workshop on Discrete Event Systems (WODES'08)*, pages 346–351, Göteborg, Sweden, May 2008. IEEE Press.

[BKMR06] Jeremy Bryans, Maciej Koutny, Laurent Mazaré, and Peter Y. A. Ryan. Opacity generalised to transition systems. In Theo Dimitrakos, Fabio Martinelli, Peter Y. A. Ryan, and Steve A. Schneider, editors, *Revised Selected Papers of the 3rd International Workshop on Formal Aspects in Security and Trust (FAST'05)*, volume 3866 of *Lecture Notes in Computer Science*, pages 81–95, Newcastle upon Tyne, UK, 2006. Springer.

[BLMO07] Th. Brihaye, F. Laroussinie, N. Markey, and G. Oreiby. Timed concurrent game structures. In *Proceedings of the 18th International Conference on Concurrency Theory (CONCUR'07)*, volume 4703 of *Lecture Notes in Computer Science*, pages 445–459. Springer, 2007.

[BLRV04] Bernard Berthomieu, Didier Lime, Olivier (H.) Roux, and Francois Vernadat. Reachability problems and abstract state spaces for time Petri nets with stopwatches. Technical Report LAAS number 04483, October 2004. also in conference MSR'05 to appear.

[BRV04] B. Berthomieu, P.-O. Ribet, and F. Vernadat. The tool TINA – construction of abstract state spaces for petri nets and time petri nets. *International Journal of Production Research*, 42(14), July 2004.

[BT03] R. Barbuti and L. Tesei. A decidable notion of timed non-interference. *Fundamenta Informaticae*, 54 :137–150, 2003.

[CBS04] S. Cabuk, C. E. Brodley, and C. Shields. IP covert timing channels : design and detection. In *ACM Conference on Computer and Communications Security*, pages 178–187, 2004.

[Deg05] A. Degorre. Caractérisation des canaux cachés en logique temporelle alternante. Master's thesis, Matisse, 2005.

[FG01] Riccardo Focardi and Roberto Gorrieri. Classification of security properties (part I : Information flow). In Riccardo Focardi and Roberto Gorrieri, editors, *Foundations of Security Analysis and Design I : FOSAD 2000 Tutorial Lectures*, volume 2171 of *Lecture Notes in Computer Science*, pages 331–396, Heidelberg, 2001. Springer-Verlag.

[FS00] Edward W. Felten and Michael A. Schneider. Timing attacks on web privacy. In *CCS '00 : Proceedings of the 7th ACM conference on Computer and communications security*, pages 25–32, New York, NY, USA, 2000. ACM Press.

[GLMR05] Guillaume Gardey, Didier Lime, Morgan Magnin, and Olivier (H.) Roux. Roméo : A tool for analyzing time Petri nets. In *17th International Conference on Computer Aided Verification (CAV 2005)*, Lecture Notes in Computer Science, Edinburgh, Scotland, UK, July 2005. Springer-Verlag.

[GM82] J.A. Goguen and J. Meseguer. Security policy and security models. In *Proc.of IEEE Symposium on Security and Privacy*, pages 11–20. IEEE Computer Society Press, 1982.

[GMR05] G. Gardey, J. Mullins, and O.H. Roux. Non-interference control synthesis for security timed automata. In *3rd International Workshop on Security Issues in Concurrency (SecCo'05)*, 2005. submitted.

[HH95] T. A. Henzinger and Pei-Hsin Ho. HYTECH : The Cornell HYbrid TECHnology tool. In *Proc. Hybrid Systems II, Ithaca, NY, USA, Oct. 1994*, volume 999 of *LNCS*, pages 265–293. Springer, 1995.

[HKP06] S. Haddad, F. Kordon, and L. Petrucci, editors. *Méthodes Formelles pour les Systèmes Répartis et Coopératifs*. Hermes/Lavoisier, September 2006.

[HZD04] L. Hélouët, M. Zeitoun, and A. Degorre. Scenarios and covert channels : another game. In *Proc of Games in design and Verification*, 2004.

[HZJ03] L. Hélouët, M. Zeitoun, and C. Jard. Covert channels detection in protocols using scenarios. In *Security Protocols Verification*, 2003.

[Hél04] L. Hélouët. Finding covert channels in protocols with message sequence charts : the case of rmtp2. In *SAM'04, Conference on SDL and MSCs*, 2004.

[Koc96] P. C. Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss and other systems. In *Proc. 16th International Cryptology Conference (CRYPTO'96)*, number 1109 in Lecture Notes in Computer Science, pages 104–113, 1996.

[LL98] F. Laroussinie and K. G. Larsen. CMC : A tool for compositional model-checking of real-time systems. In *FORTE-PSTV'98*, pages 439–456. Kluwer Academic Publishers, 1998.

[LMO08] F. Laroussinie, N. Markey, and G. Oreiby. On the expressiveness and complexity of ATL. *Logical Methods in Computer Science*, 4(2 :7), 2008.

[LPY97] K. G. Larsen, P. Pettersson, and W. Yi. UPPAAL in a Nutshell. *Journal of Software Tools for Technology Transfer*, 1(1/2) :134–152, October 1997.

[Mer74] P. M. Merlin. *A study of the recoverability of computing systems*. PhD thesis, University of California, Irvine, CA, 1974.

[OW05] J. Ouaknine and J. Worrell. On the decidability of Metric Temporal Logic. In *Proc. 20th IEEE Symposium on Logic in Computer Science (LICS'05)*, 2005.

[PR99] S. Schneider P.Y.A. Ryan. Process algebra and noninterference. In *Proc. of 12th Computer Security Foundations Workshop*. IEEE CS Press, 1999.

[Ram74] C. Ramchandani. *Analysis of asynchronous concurrent systems by timed Petri nets*. PhD thesis, Massachusetts Institute of Technology, Cambridge, MA, 1974.

[RD02] Olivier (H.) Roux and Anne-Marie Déplanche. A t-time Petri net extension for real time-task scheduling modeling. *European Journal of Automation (JESA)*, 36(7) :973–987, 2002.

[RFM03] R. Gorrieri R. Focardi and F. Martinelli. Real-time information flow analysis. *IEEE Journal on Selected Areas in Communications*, 21(1) :20–35, 2003.

[Rya01] P.Y.A. Ryan. Mathematical models of computer security. In *Foundations of Security Analysis and Design - Tutorial Lectures (R. Focardi and R. Gorrieri, Eds.)*, number 2171 in Lecture Notes in Computer Science, 2001.

[Yov97] S. Yovine. Kronos : A Verification Tool for real-Time Systems. *Journal of Software Tools for Technology Transfer*, 1(1/2) :123–133, October 1997.