# Curriculum Vitæ

Nadia Bel Hadj Aissa

---

# CURRICULUM VITÆ SYNTHÉTIQUE

## Informations personnelles

- ▷ Nom : Bel Hadj Aissa épouse Amamou
- ▷ Prénom : Nadia
- ▷ Date et lieu de naissance : 02/07/1979 à Tunis (Tunisie)
- ▷ Nationalité : Tunisienne
- ▷ Situation familiale : Mariée
- ▷ Téléphone : 24697569
- ▷ E-mail : nadia.belhadjaissa@gmail.com

## Diplômes

**2004–2008** **Doctorat d'informatique** *(mention très honorable)*
Université des Sciences et Technologies de Lille
*« Maîtrise du temps d'exécution de logiciels déployés dans des dispositifs personnels de confiance »*

**2002–2003** **DEA d'informatique** *(mention assez bien)*
Université des Sciences et Technologies de Lille

**1998–2002** **Diplôme d'Ingénieur en Réseaux Informatiques et Télécommunications** *(mention bien)*
Institut National des Sciences Appliquées et de Technologies (Tunisie)

**1997–1998** **Baccalauréat spécialité Mathématiques** *(mention bien)*
Lycée Pilote de l'Ariana, Tunisie

## Expériences professionnelles

| | |
|---|---|
| **2010–Présent** | Maitre Assistante<br>Faculté des Sciences de Bizerte |
| **2009–2010** | Enseignante/chercheuse permanente<br>Esprit (Ecole Supérieure Privée d'Ingénierie et de Technologie) |
| **2008–2009** | Vacations d'enseignement en informatique<br>INSAT, Esprit |
| **2007–2008** | Attaché Temporaire d'Enseignement et de Recherche (ATER) en informatique<br>IUT A, Université des Sciences et Technologies de Lille |
| **2006–2007** | ATER en poste complet à partir du mois de Mars de l'année universitaire courante<br>UFR d'IEEA, Université des Sciences et Technologies de Lille |
| **2004–2006** | Vacations d'enseignement en informatique<br>IUT A et UFR d'IEEA, Université des Sciences et Technologies de Lille |
| **2003** | Stage de DEA au sein de l'équipe NOCE de<br>Trigone, des Sciences et Technologies de Lille |

# ACTIVITÉS D'ENSEIGNEMENTS

## Introduction

Durant mes trois premières années de thèse, j'ai régulièrement sollicité auprès de l'INRIA une autorisation de cumul pour effectuer des vacations. Cela m'a permis de me familiariser avec les activités d'enseignement, qui me motivent depuis longtemps. À noter que cet organisme dont dépend ma bourse de thèse autorise seulement un nombre maximal de 32h équivalent TD d'enseignement par an. Ensuite, j'ai pu intégrer un poste d'attaché temporaire d'enseignement et de recherche à plein temps à partir de mars de l'année universitaire 2006-2007 auprès de l'UFR d'IEEA et j'ai eu un poste similaire durant toute l'année universitaire 2007-2008 au sein de l'Institut Universitaire de Technologie (IUT) A de l'Université de Lille 1 au département informatique. Dès mon retour en Tunisie, j'ai souhaité enseigner et j'ai pris en charge en tant que vacataire deux modules à l'Institut National des Sciences Appliquées et de Technologie (INSAT) et à l'Ecole Supérieure Privée d'Ingénierie et de Technologies (Esprit). Au fur et à mesure, les cours que j'ai pu donner ont renforcé mon désir d'enseigner, et je pense maintenant avoir une expérience suffisamment riche pour le faire sereinement. Au cours de l'année universitaire 2009-2010, j'ai occupé un poste d'enseignante permanente à l'Ecole Supérieure Privée d'Ingénierie et de Technologies (Esprit). Actuellement, je suis maitre assistante à la Faculté des Sciences de Bizerte. J'assure depuis l'année universitaire 2010-2011 les cours d'Atelier Système d'Exploitation, Systèmes d'exploitation I et Architecture des Ordinateurs. J'ai par ailleurs assuré un module intitulé *Systèmes Pervasifs Intelligents et Ingénierie du Web* en mastère recherche 2 option SPI à la faculté des sciences de Tunis.

## Enseignements dispensés

**Architecture des ordinateurs : 2003-04**

| | |
|---|---|
| Responsable : | Alain Rauch |
| Statut : | Vacataire |
| Caractéristiques : | **TD/TP** avec **24 étudiants** en **1re année DUT informatique** |
| Description : | Programmation en langage assembleur sur des microprocesseurs de la famille Intel 80X86 : Modèle de programmation, registre, jeu d'instruction, mémoire, modes d'adressage, appel de sous-programme, pile d'exécution. |

**Réseaux informatiques : 2004-05**

| | |
|---|---|
| Responsable : | Jean Carle |
| Statut : | Vacataire |
| Caractéristiques : | **TD/TP** avec **24 étudiants** en **1re année DUT informatique** |
| Description : | Présentation des principes fondamentaux des réseaux informatiques : Modèle OSI. Détail de toutes les couches réseaux, de la couche physique aux couches applicatives. Codage du signal, FTP, HTTP, TCP, UDP, IP |

**Programmation Java : 2005-06**

| | |
|---|---|
| Responsable : | Bruno Bogaert |
| Statut : | Vacataire |
| Caractéristiques : | **Cours/TD** avec **12 étudiants** en **Licence MIAGE** [1], **Formation Continue et Alternance - mention Informatique** |
| Description : | Le public était constitué d'étudiants ayant des difficultés à se familiariser avec la programmation objet et notamment Java. Mon intervention auprès d'eux était complémentaire au cours de Mr Bruno BOGAERT. J'ai donc pris la responsabilité de ce module en préparant moi-même les sujets et en orientant le cours afin de combler les lacunes que rencontraient les étudiants. |

**Introduction à l'algorithmique et programmation en langage C : 2006-07**

| | |
|---|---|
| Responsable : | Emmanuel Renaux |
| Statut : | ATER |
| Caractéristiques : | **TD/TP** avec **27** en **1re année TELECOM LILLE 1** |
| Description : | introduction à l'algorithmique (notion de variable, instruction de contrôle de base, pseudo langage) et introduction au langage C (mise en oeuvre des notions vues en algo) |

**Systèmes d'exploitation : 2007-08**

| | |
|---|---|
| Responsable : | Bruno Beaufils |
| Statut : | ATER |
| Caractéristiques : | **TD/TP** avec **26 étudiants** en **1re année DUT informatique** |
| Description : | Systèmes d'exploitations multi-tâches (concepts et utilisations) : i5/OS : Système de Gestion des Données/Commandes, Prise en main de l'iSeries, L'éditeur de source SEU, Messages/Travaux, Outils de développement (PDM/SDA). Unix : Premier contact, Éditeurs de texte (ed/vi), Processus et communications, Processus et redirections, Variables - Protections |

**Programmation orientée objet : 2007-08**

| | |
|---|---|
| Responsable : | François Clautiaux |
| Statut : | ATER |
| Caractéristiques : | **TP** avec **26 étudiants** en **1re année DUT informatique** |
| Description : | Paradigme Objet : structuration, paquetages, agrégation, encapsulation, interfaces, héritage, généricité, collections, exceptions, entrées/sorties. |

**Structure de données : 2007-08**

| | |
|---|---|
| Responsable : | Annie-Françoise Mouyart |
| Statut : | ATER |
| Caractéristiques : | **TP** avec **24 étudiants** en **1re année DUT informatique** |
| Description : | Collections génériques, tas, files, listes, arbres, tris et parcours de structures, complexité. |

**Apprentissage de la programmation : 2007-08**

| | |
|---|---|
| Responsable : | Yann Secq |
| Statut : | ATER |
| Caractéristiques : | **TD/TP** avec **24 étudiants** en **1re année DUT informatique** |
| Description : | Notion d'algorithme, variables, structures de contrôle, récursivité. |

**Réseaux Informatiques : 2007-08**

Responsable : Jean Carle
Statut : ATER
Caractéristiques : **Cours/TD intégré** avec **26 étudiants** en **1re année DUT informatique**
Description : J'ai complètement en charge le cours de Réseaux en semestre décalé mis en place au département informatique et je me suis investie dans la réorganisation du contenu du cours.

**Programmation par composants et services : 2008-09**

Responsable : Nadia bel Hadj Aissa
Statut : Vacataire
Caractéristiques : **Cours/TD intégré** avec 2 groupes de **35 étudiants** en **5ème année spécialité Génie Logiciel à l'INSAT**
Description : C'est un module de 15 semaines que je prend en charge complètement incluant la préparation des cours, examens et corrections de copies. Le cours introduit la programmation par composants à travers des techniques telles que les java beans, les EJB, CORBA, etc... ainsi que la programmation par services.

**Sécurité des codes mobiles : 2008-09**

Responsable : Nadia bel Hadj Aissa
Statut : Vacataire
Caractéristiques : **Cours/TD intégré** avec 1 groupes de **30 étudiants** en **4ème année spécialité Informatique à Esprit**
Description : C'est un module de 21 heures qui a pour objectif de faire comprendre aux étudiants les menaces qui peuvent émaner d'un code mobile en termes de confidentialité, intégrité et disponibilité. Il présente par ailleurs les principales techniques permettant de se prémunir contre ces dangers. Enfin, il se focalise sur une approche particulière consistant à vérifier les propriétés de sécurité au moment du chargement du code mobile.

**Systèmes d'exploitation avancés : 2009-10**

Responsable : Nadia bel Hadj Aissa
Statut : Enseignante permanente
Caractéristiques : **Cours/TD intégré** avec 2 groupes de **30 étudiants** en **4ème année spécialité Télécommunications à Esprit**
Description : C'est un module de 42 heures qui a pour objectif d'asseoir les bases et fondements théoriques des systèmes d'exploitation. Les mécanismes d'ordonnancement, de gestion de mémoires, de synchronisation font partie des éléments enseignés dans ce cours. J'ai pris en charge complètement le module (i.e. préparation de cours, TD, examens ....

**Fonctionnement de l'ordinateur : 2009-10**

Responsable : Nadia bel Hadj Aissa
Statut : Enseignante permanente
Caractéristiques : **Cours/TD intégré** avec 6 groupes de **30 étudiants** en **1ème année à Esprit**
Description : C'est un module de 21 heures qui a pour objectif de présenter le fonctionnement de l'ordinateur à un étudiant novice. Ce module introduit les notions de numérations ainsi que des notions plus poussées en architecture c'est à dire les performances des processeurs, le pipeline, la mémoire cache. J'ai pris en charge complètement le module (i.e. préparation de cours, TD, examens ....

**Sécurité des codes mobiles : 2009-10**

Responsable : Nadia bel Hadj Aissa
Statut : Enseignante permanente
Caractéristiques : **Cours/TD intégré** avec 4 groupes de **30 étudiants** en **4ème année spécialité Informatique à Esprit**
Description : C'est un module de 21 heures qui a pour objectif de faire comprendre aux étudiants les menaces qui peuvent émaner d'un code mobile en termes de confidentialité, intégrité et disponibilité. Il présente par ailleurs les principales techniques permettant de se prémunir contre ces dangers. Enfin, il se focalise sur une approche particulière consistant à vérifier les propriétés de sécurité au moment du chargement du code mobile.

**Atelier Systèmes d'exploitation : 2010-Présent**

Responsable : Nadia bel Hadj Aissa
Statut : Responsable de cours
Caractéristiques : **Cours/TP** avec les étudiants en Licence Fondamentale SI1
Description : Il s'agit d'une initiation aux systèmes d'exploitation pour les étudiants en SI1. L'objectif est de définir la notion de système d'exploitation d'étudier de manière théorique et pratique la partie Système de Gestion de Fichiers des systèmes et d'apprendre aux étudiants les techniques de sécurisation des systèmes et les techniques de protection. J'ai assuré le cours et quelques séances de TP.

**Systèmes d'exploitation I : 2010-Présent**

Responsable : Nadia bel Hadj Aissa
Statut : Responsable de cours
Caractéristiques : **Cours** avec les étudiants en Licence Appliquée TRT1
Description : Il s'agit d'une initiation aux systèmes d'exploitation pour les étudiants en TRT1. L'objectif est de définir la notion de système d'exploitation d'étudier de manière théorique et pratique la partie Système de Gestion de Fichiers des systèmes et d'apprendre aux étudiants les techniques de sécurisation des systèmes et les techniques de protection. J'ai assuré le cours et préparé les sujets de TP.

**Architecture des ordinateurs : 2010-Présent**

Responsable : Nadia bel Hadj Aissa
Statut : Responsable de cours
Caractéristiques : **Cours/TD** avec les étudiants en Licence Appliquée TRT1
Description : Il s'agit d'une initiation à l'architecture des ordinateurs TRT1. L'objectif est de présenter le fonctionnement de l'ordinateur à un étudiant novice. Ce module introduit les notions de numérations ainsi que des notions plus poussées en architecture c'est à dire les performances des processeurs, le pipeline, la mémoire cache. j'ai pris en charge complètement le module en assurant le cours et les séances de TD.

**Systèmes pervasifs intelligents et ingénierie du Web : 2011-2012**

Responsable : Nadia bel Hadj Aissa
Statut : Responsable de cours
Caractéristiques : **Cours intégré** avec les étudiants en M2 Recherche option SPI
Description : Aujourd'hui, beaucoup d'objets du monde réel sont enrichis de capacités de traitement de l'information. Les objets intelligents peuvent se souvenir des événements importants, présentent un comportement dépendant du contexte et sont interactifs. Les systèmes pervasifs correspondent à un fonctionnement global de la communication où une informatique diffuse permet à des objets intelligents et communicants de se reconnaitre entre eux et de se localiser automatiquement. Des exemples de systèmes pervasifs et intelligents seront étudiés dans le cadre de ce cours tels que les réseaux de capteurs sans fil, les étiquettes RFID, .... Des ateliers pratiques permettront aux étudiants d'étudier concrètement le fonctionnement de ces cas d'étude.

## Encadrements

La réalisation de stages et projets individuels est à mon avis primordiale dans la formation des étudiants en informatique. L'encadrement de ces stages et projets est en conséquence un aspect important du travail de l'enseignant. C'est pourquoi j'y ai consacré un temps non négligeable, à travers l'encadrement d'étudiants de différentes formations.

- Année 2005-06. Suivi de projet technique (150 heures), 2 étudiants en **Master 2 TIIR** [2], "Calcul du pire temps d'exécution dans un environnement Java" ;
- Année 2006-07. Suivi de stage en entreprise, 2 étudiants en **maîtrise MIAGE**, 6 mois chez Aptelia, "stage en nouvelles technologies J2EE" ;
- Année 2006-07. Suivi de stage en entreprise, 2 étudiants en **Master 1 Informatique parcours GMI**, 4 mois chez Sopra Group , "Analyse et développement d'une application sur le fret maritime", " Outils de gestion commerciale d'une enseigne de distribution" ;
- Année 2006-07. Suivi de stage en entreprise, 2 étudiants en **L3 Informatique parcours MIAGE**, "Refonte du site internet et sur la création de l'intranet de Tape à l'oeil." ;
- Année 2006-07. Suivi de **stage de fin d'études**, 3 étudiants en **Master 2 TIIR**, 6 mois chez Atos Origin, "Réalisation de l'interface d'administration d'un outil de supervision", "Sécurisation d'une plateforme VOIP" ;
- Année 2006-07. Suivi de **stage de fin d'études**, 1 étudiant en **Master 2 TIIR**, 6 mois chez Gemalto, "Développement de services webs dynamiques basés sur AJAX et Web 2.0"

Dans le cadre de mes activités de recherche, j'ai eu l'occasion d'encadrer avec Mme Hela Ben Ayed un projet de fin d'étude d'un étudiant de la fac des sciences. Le sujet s'intitule *Service web embarqué pour le suivi environnemental*. Ce projet visait à exploiter les technologies des réseaux de capteurs et du Web of Things dans le suivi environnemental.

## Synthèse des enseignements

J'ai enseigné à des étudiants de **structures différentes** (IUT, IEEA, école d'ingénieur) et de **publics variés**, (première année après le baccalauréat et formation continue). J'ai effectué des **enseignements variés** : les **réseaux informatiques**, l'**apprentissage de la programmation**, la **programmation par objets**, les **systèmes d'exploitation**, les **structures de données**, et l'**architecture des ordinateurs**. En outre, j'ai eu l'occasion d'**encadrer** les travaux de nombreux étudiants (en projet technique ou stage de fin d'étude). Le tableau ci-dessus illustre la distribution de mes activités d'enseignement jusqu'à l'année universitaire 2009-2010.

| | **03/04** vacataire | **04/05** vacataire | **05/06** vacataire | **06/07** ATER | **07/08** ATER | **08/09** vacataire | **09/10** permanente | **total** sur 6 ans |
|---|---|---|---|---|---|---|---|---|
| Cours/TP/TD | 32 | 32 | 32 | 72 | 192 | 81 | 294 | 441 |
| Encadrement | | | | 24 | | | 48 | 24 |
| Total annuel | 32 | 32 | 32 | 96 | 192 | 81 | 342 | 807 |

2. Technologies pour les Infastructures de l'Internet et leurs Robustesses

# ACTIVITÉS DE RECHERCHE

## Travaux effectués pendant le DEA

Mon stage de DEA était centré autour de l'étude des infrastructures nécessaires au contexte d'apprentissage collaboratif, mobile et ubiquitaire et de montrer les bénéfices qu'on peut tirer des plateformes pair à pair dans ce genre de contexte.

### ▷▷ Résumé

Depuis plusieurs années, l'interaction des utilisateurs avec l'outil informatique a été fortement conditionnée par les contraintes technologiques. Aujourd'hui, les avancées technologiques réalisées aussi bien dans les réseaux sans fil que dans la miniaturisation des processeurs et des capteurs, appellent de nouvelles formes d'interaction où s'estompent progressivement les frontières entre les mondes physiques et numériques. Le domaine de l'éducation a toujours été un terrain propice pour le développement ou la validation de nouvelles technologies numériques. Dans le cadre de ce stage, nous avons proposé d'étudier les infrastructures nécessaires au contexte d'apprentissage collaboratif, mobile et ubiquitaire et de mettre en évidence les limites des solutions actuelles. Par ailleurs, nous avons proposé à partir de cette étude de l'existant quelques ébauches de solutions basées sur l'utilisation d'une infrastructure de type Pair à Pair. Nous avons essayé de démontrer que ce type d'infrastructure est susceptible de répondre à nos attentes tant sur le plan des réseaux ad hoc pour la communication directe entre mobiles, qu'en terme des mécanismes sociaux d'échange et de collaboration. Un prototype, l'outil Ubi-View que nous avons développer, nous a permis de valider techniquement le bien-fondé et l'efficacité des tels environnements d'apprentissage.

**Mots clés :** Apprentissage collaboratif, mobile, ubiquitaire, Middleware, Roomware, Navigation collaborative, Pair à Pair, JXTA, UML

## Travaux effectués pendant le doctorat

Ma thèse a débuté en janvier 2004 sous la direction de David Simplot-Ryl et de Gilles Grimaud. Elle se rapporte au calcul de pire temps d'exécution pour des codes mobiles notamment destinés à être exécutés sur des plateformes fortement contraintes telles que la carte à puce.

– **Thèse soutenue le 29 Octobre 2008**

| | |
|---|---|
| Titre | Maîtrise du temps d'exécution de logiciels déployés dans des dispositifs personnels de confiance |
| Lieu de soutenance | Villeneuve d'Ascq |
| Mention | Très honorable |

– **Composition du jury**

| | |
|---|---|
| Président | Pr. Jean-Louis Lanet (XLIM, Limoges) |
| Rapporteurs | Pr. Isabelle Puaut (IRISA, Université de Rennes I, Rennes) |
| | Pr. Jean-Dominique Decotignie (EPFL/CSEM) |
| Examinateurs | Jean-Jacques Vandewalle (Ingénieur de recherche à Gemalto) |
| Directeur de thèse | Pr. David Simplot-Ryl (LIFL, USTL, Lille) |
| Encadrant | Dr. Gilles Grimaud (LIFL, USTL, Lille) |

## ▷▷ Problématique

Les constants progrès techniques de l'électronique en terme de miniaturisation ont mené à un fort développement de l'informatique ubiquitaire. Parallèlement à ce développement, le nombre et la diversité des petits systèmes informatiques sont en plein essor depuis quelques années. Nous avons, ainsi, assisté à l'apparition et la prolifération des téléphones portables, des assistants personnels (PDA [1]), étiquettes électroniques (RFID [2]), capteurs de terrains et autres cartes à puce. Ces petits systèmes informatiques, que nous désignons désormais par *Petits Objets Portables et Sécurisés*, sont les cibles principales des travaux de recherche menés au sein de l'équipe-projet POPS [3]. Ces travaux traitent conjointement les domaines des réseaux mobiles et des systèmes d'exploitation embarqués et visent à endiguer les difficultés de programmation de logiciels pour les POPS. Plus précisément, produire des logiciels sûrs destinés à ce type de cibles — plateformes non conventionnelles et souvent propriétaires — requiert un haut-niveau d'expertise de la part du développeur. Le défi de l'équipe-projet POPS consiste, dans ce cadre, à placer l'intelligence dans les outils plutôt que de s'appuyer sur la seule expertise du programmeur. De façon générale, la problématique de recherche explorée dans cette thèse repose sur le savoir-faire développé au sein de l'équipe-projet POPS. Mes travaux constituent un prolongement de ceux déjà entrepris sur la conception de systèmes d'exploitation ouverts pour carte à microprocesseur.

Par ailleurs, mes travaux de thèse s'inscrivent dans le projet européen INSPIRED [4]. L'objectif de ce projet était de porter un regard sur le futur de la carte à puce à l'horizon des cinq voire dix prochaines années afin de prendre de la distance avec le carcan historique imposé par le standard ISO7816 [5]. La notion de *dispositif personnel de confiance*, ou ce que nous appellerons TPD [6], a ainsi vu le jour avec pour objectif de remplacer dans un futur proche la carte à puce. Le projet INSPIRED s'est achevé au début de l'année 2007. Néanmoins, le consortium formé par les différents partenaires est resté actif et a contribué, en l'occurrence, à la spécification de la nouvelle version de JAVA CARD. Je me suis attelée, dans ce cadre, à développer une méthodologie et à fournir une chaîne d'outils permettant aux TPDs de maîtriser la consommation des ressources des logiciels et en particulier les temps d'exécutions au pire cas ou WCET.

Bien qu'il soit difficile de retenir une définition exacte des systèmes embarqués, la littérature nous renseigne sur leurs propriétés générales. En opposition aux systèmes généralistes, ces systèmes embarqués sont dédiés à un domaine d'application spécifique. Ils sont conçus pour une utilisation très précise. Les différents composants matériels et logiciels intervenant dans leur mise au point sont choisis dans le but de répondre au mieux à cette utilisation. Dans le même but, logiciel et matériel sont fortement couplés. Le matériel et le logiciel sont utilisés de façon autonome, ou en interaction avec leur environnement. Ils sont

1. PDA est l'acronyme de Personal Digital Assistant.
2. RFID est l'acronyme de Radio Frequency IDentification.
3. POPS est l'acronyme de Petits Objets Portables et Sécurisés.
4. INSPIRED est l'acronyme de INtegrated Secure Platform for Interactive tRusted pErsonal Devices.
5. ISO est l'acronyme de International Organization for Standardization.
6. TPD est l'acronyme de Trusted Personal Device.

généralement inclus dans un système plus vaste qu'ils contribuent à faire fonctionner. Il faut néanmoins faire la distinction entre les systèmes embarqués ouverts (e.g. TPDs) et fermés. Ces derniers sont des objets de la vie courante munis de capacités de calcul fournies par des composants intelligents enfouis tels qu'une carte embarquée dans une voiture pour contrôler l'injection. Cette carte ne sera pas accessible pour d'éventuelles mises à jour de son logiciel. Ces systèmes embarqués fermés souffrent ainsi, d'un manque de flexibilité dû à la limitation de l'intervention humaine a posteriori pour changer, augmenter les fonctionnalités disponibles.

À l'opposé, la prolifération de nouveaux équipements ouverts et programmables (e.g. TPD) a favorisé l'essor des environnements d'exécution dynamiquement adaptables ayant la possibilité de déployer à la volée de nouveaux services après leurs émissions. C'est la notion de *post-issuance* se définissant comme la capacité d'enrichir les fonctionnalités des TPDs après leurs mises en circulation (i.e. après qu'ils soient déployés donc délivrés à leurs porteurs). Afin de permettre cette flexibilité, il est indispensable de disposer d'un mécanisme de chargement dynamique de code, tel que les librairies dynamiques ou le chargement dynamique de classes dans les machines virtuelles JAVA ou encore le moteur d'exécution CLR[7].

Dans ce cadre, l'utilisation des mécanismes issus de la programmation orientée objet, et notamment les notions d'héritage et de polymorphisme, s'impose. En effet, la programmation objet fournit le substrat nécessaire permettant la réutilisation mais aussi l'extensibilité. Loin du logiciel monolithique développé sur mesure d'un ancien temps, les applications doivent désormais être évolutives et correspondent souvent à un assemblage de briques logicielles fournies par des sources diverses qui ne se font pas mutuellement confiance. L'utilisation des cadres applicatifs[8] objets dans lesquels les logiciels destinés aux TPDs viennent intégrer leur code spécifique est l'un des principes clés que nous avons défendus au sein du consortium INSPIRED.

L'enjeu majeur de cette nouvelle tendance consiste principalement à trouver un compromis avantageux entre une flexibilité accrue et la nécessité d'apporter à la fois sûreté de fonctionnement et sécurité. En effet, la flexibilité permet à l'utilisateur de déployer de nouveaux services à la volée, quand le besoin s'en ressent. Néanmoins, le TPD doit être en mesure de garantir l'absence de défaillance au cours de l'exécution des logiciels — tant les nouveaux que ceux préalablement déployés. Elle ne doit pas non plus ouvrir des brèches de sécurité menaçant l'intégrité et la confidentialité des données (ou traitements) confidentielles contenues dans le TPD, ou encore la disponibilité des services offerts.

Un large pan de la littérature sur ce sujet se limite aux deux premières préoccupations. Nous avons choisi de nous intéresser à la maîtrise des temps d'exécution des logiciels en vue d'assurer la disponibilité des services offerts par le TPD.

## ▷▷ Contributions

Dans mes travaux de thèse, je me suis préoccupé d'une composante importante et rarement traitée de la sécurité et de la sûreté de fonctionnement qui consiste à maîtriser le temps d'exécution des logiciels destinés à s'exécuter sur un vaste nombre de dispositifs personnels de confiance déjà déployés auprès de leurs utilisateurs. Les dispositifs de confiance auxquels nous faisons référence sont la nouvelle génération de carte à puce, que nous avons désigné par le terme TPD au sein du consortium INSPIRED.

J'ai commencé par pointer les incompatibilités des solutions de calcul de WCET existantes avec une logique de déploiement a posteriori alors que les TPDs sont en cours d'utilisation par leurs porteurs. De plus, nous avons favorisé dans nos travaux d'apporter les garanties au plus tôt, afin que l'installation échoue si l'environnement d'exécution n'est pas en mesure de répondre aux exigences temporelles exprimées. Ainsi, l'usager est assuré du bon fonctionnement du service auquel il a souscrit en toutes circonstances. En ce sens, nos travaux apportent une réponse aux problème de disponibilité des services, faisant partie des critères de sécurité.

Nous avons mis à profit les avantages de l'analyse statique pour apporter notre première contribution. Celle-ci a permis d'adapter le calcul de WCET en définissant un schéma de calcul distribué entre le producteur de code, d'une part, et le consommateur de code, d'autre part. Le producteur, c'est à dire la station de travail sur laquelle est produit le logiciel, dispose d'importantes ressources matérielles et de tout le temps nécessaire lui permettant d'exécuter des calculs complexes. De son coté, le consommateur (

7. CLR est l'acronyme de Common Language Runtime
8. Le terme anglo-saxon est *framework*.

i.e. TPD) dispose d'un environnement d'exécution fortement contraint en ressources matérielles et ayant des exigences en terme de sécurité.

Le TPD doit être en mesure de garantir l'innocuité des applications chargées *post-issuance*. En sa qualité de dispositif de confiance, il doit offrir en son sein (i.e. sans reposer sur la sécurité d'un tiers) l'infrastructure nécessaire pour éviter qu'un nouveau logiciel ne vienne monopoliser le microprocesseur et ainsi diminuer les performances globales de tout le système et de ses applications. Une des contributions de ce travail consiste à embarquer un vérifieur des bornes des boucles qui permet d'assurer que le TPD peut déterminer une borne majorante sur le temps d'exécution du traitement chargé. Ainsi, le TPD est en mesure d'assurer à chacune de ses applications les ressources de calcul nécessaires pour qu'elles s'exécutent dans les délais impartis quelles que soient les conditions d'utilisation. Cette garantie est un critère important de sécurité qui permet de maintenir la disponibilité des services.

Au moment du déploiement d'un nouveau logiciel sur la plateforme cible et en vue de son admission, le TPD doit être en mesure de vérifier sa capacité à fournir les ressources nécessaires à son fonctionnement. Ce besoin en ressources est décrit par le biais d'un contrat. Une approche consiste à surveiller à l'exécution que le logiciel ne va pas utiliser plus de ressources que spécifié dans son contrat. Une autre consiste à formuler les contrats d'une manière statique et figée sous forme de pré et post conditions et de prouver formellement que l'application s'y tient. Nous avons esquissé une approche originale de la maîtrise du temps d'exécution en monde ouvert. Selon cette approche, il suffit d'extraire des logiciels à installer les contrats à vérifier, de les stocker sur le système sous forme d'équations qui seront vérifiées par le TPD et qui pourront être affinées au fur et à mesure de l'installation de nouvelles extensions.

Mes travaux ont donné lieu à plusieurs publications dans des évènements d'audience internationale avec comité de sélection : Dans [1] et [2], nous avons présenté notre schéma distribué de calcul de WCET. Puis, dans [3], nous avons décrit d'un manière plus formelle le calcul de bornes de boucles et sa vérification. Dans [4], nous avons présenté nos résultats expérimentaux dans les conditions expérimentales au plus près des exigences d'un Consortium formé par les principaux acteurs de l'industrie. Dans [5], le bénéfice des contrats pour deux problématiques différentes l'une traitant du flot implicite d'information et l'autre traitant de la disponibilité est démontré.

## ▷▷ Perspectives de recherche

Mes travaux de thèse ouvrent la voie à plusieurs pistes directes particulièrement intéressantes.

En premier lieu, la solution que nous avons présenté est portable. D'une part, elle ne repose pas sur un langage particulier mais plutôt sur une forme intermédiaire. D'autre part, elle est indifférente au regard des architectures matérielles sous-jacentes. Néanmoins, les outils que nous avons implémenté aussi bien pour déterminer les bornes des boucles que pour le comptage de cycles ne sont pas portables. Un effort de génie logiciel pourrait être fait afin d'accroître la généricité de ces outils notamment grâce à une description formelle du CPU en VHDL. En second lieu, nous avons utilisé l'approche du code porteur de preuve pour borner les boucles sur le producteur de code et de permettre au consommateur de vérifier les informations annoncées. Pour cet effet, nous avons joint au code une preuve inférant le type des variables à chaque point de saut. La preuve sur les bornes des boucles n'est pas la première qui existe sur le système. Elle vient, en effet, se rajouter à la preuve de typage correct qui garantit des propriétés d'intégrité et de confidentialité. En d'autres termes, pour chaque propriété que l'on veut garantir, le code se voit adjoindre une nouvelle preuve. On ne peut que s'inquiéter que la taille du code ne devienne négligeable devant l'amoncellement de preuves qui l'accompagnent. En outre, nous avons pu démontrer que les preuves ne sont pas forcément indépendantes. Nous avons notamment démontré que l'utilisation des informations de typage pouvait améliorer les résultats sur le comptage de cycles. Donc, en vue d'assurer un ensemble de propriétés prédéfinies, il est possible d'imaginer qu'une seule preuve où toute redondance est éliminée vienne se rattacher au code.

À plus long terme, nous avons proposé une solution basée sur les contrats afin de contrôler l'admission de nouveaux logiciels sur le système. Dans cette proposition, nous avons admis une hypothèse stipulant que l'ordre de déploiement et prioritaire. C'est à dire qu'une application B pourrait voir son installation échouer si une application A préalablement déployée sur le système a instauré un contrat contraignant. Cet ordre pourrait ne pas correspondre aux voeux de l'usager qui se verrait ainsi priver des services de l'application B alors qu'il n'a peut être même plus besoin de A. Il s'agit dans ce cas d'un conflit dans

le sens où deux applications A et B ne peuvent pas cohabiter sur le TPD au même moment. C'est cette gestion de conflits que nous voyons en perspective des investigations menées sur les contrats. Ainsi, pour gérer ces conflits, on pourrait imaginer de remonter des informations au développeur afin qu'il prenne conscience des causes du rejet de son application. De même, on pourrait donner à l'utilisateur un moyen de décider quelle application il voudrait garder sur son système.

## Travaux effectués après le doctorat

Au cours de l'année universitaire 2009/2010, j'ai intégré le département de recherche Espritec. Au sein de cette structure de recherche, j'ai eu l'occasion de concentrer mes efforts autour de la problématique réseaux de capteurs. J'ai pu ainsi participer à l'école SensorNets2009 organisée par le laboratoire ENIS à Monastir. Dans le cadre de ces travaux de recherche, j'encadre un étudiant en projet de fin d'étude d'ingénieur sur le sujet *Serveur web embarqué pour le suivi environnemental*. J'ai aussi participé à un tutoriel de prise en main de la plateforme SensLab à Grenoble. Enfin, j'ai participé aux journées de la RFID organisées par le laboratoire 6'Com de l'ENIT.

## Liste de publications

### ▷▷ Conférences internationales avec comité de lecture et actes


[1] N. Bel Hadj Aissa, C. Rippert, D. Deville and G. Grimaud. A Distributed WCET Computation Scheme for Smart Card Operating Systems. In *Proceedings of the 4th International Workshop on Worst-Case Execution Time Analysis (WCET 2004), in association with the 16th ECRTS conference*, Catania, Italy, 2004.

[2] N. Bel Hadj Aissa, C. Rippert, and G. Grimaud. Distributing the WCET Computation for Embedded Operating Systems. In *Proceedings of the 25$^{th}$ IEEE International Real-Time Systems Symposium (RTSS), Work In Progress Session*, Lisbon, Portugal, 2004.

[3] N. Bel Hadj Aissa, G. Grimaud, and D. Simplot-Ryl. A Distributed and Verifiable Loop Bounding Algorithm for WCET Computation on Constrained Embedded Systems. In *Proceedings of the 14$^{th}$ International Conference on Real-Time and Network System*, Poitiers, France, 2006 .

[4] N. Bel Hadj Aissa, G. Grimaud, and V. Bénony. Bringing Worst Case Execution Time Awarness to an Open Smart Card OS. In *Proceedings of the 13$^{th}$ IEEE International Conference on Embedded and Real-Time Computing Systems and Applications*, Daegu, Korea, 2007.

[5] N. Bel Hadj Aissa, D. Ghindici, G. Grimaud, and I. Simplot-Ryl. Contracts as a support to static analysis of open systems. In *1$^{st}$ Workshop on Formal Languages and Analysis of Contract-Oriented Software*, Oslo, Norway, 2007.


### ▷▷ Conférences nationales avec comité de lecture et actes


[6] N. Bel Hadj Aissa and G. Grimaud, Calcul de temps d'exécution au pire cas pour code mobile. *Actes des 1$^{ères}$ Rencontres Jeunes Chercheurs en Informatique Temps Réel*, Nancy, France, 2005.


### ▷▷ Publications universitaires


[7] N. Bel Hadj Aissa. *Ubi-View : Outil P2P de visualisation et d'interaction dans un environnement d'apprentissage mobile.* Mémoire de DEA, Université des Sciences et Technologies de Lille, 2003.

[8] N. Bel Hadj Aissa. *Maîtrise des temps d'exécution de logiciels déployés dans des dispositifs personnels de confiance.* Mémoire de thèse, Université des Sciences et Technologies de Lille, 2008.


## Divers

### Participations à des projets de recherche

Au cours de ma thèse, j'ai eu l'occasion de participer à des projets de recherche impliquant divers laboratoires :

- **InspireD :** Mon sujet de thèse s'inscrit dans le cadre d'un projet européen InspireD (Integrated secure platform for interactive Trusted Personal Device). Ce consortium regroupe un groupe de fabricants de carte à puce ainsi que des académiques. J'ai pu dans le cadre de ce projet participer aux réunions de travail et intervenir activement dans la rédaction de délivrables qui sont soumis à l'approbation de la commission européennne.
- **ACI securité SPOPS** - Sécurité et sûreté des systèmes d'exploitation ouverts pour petits objets portables sécurisés - projet ayant pour but final de obtenir un compromis acceptable qui maximise la flexibilité des TPDs (Trusted Personal Devices), en garantissant au même temps la securité des applications.

## Participations aux séminaires, écoles, et conférences

- **Conférences internationales**
  - RTCSA'07 (Daegu, Korea), RTNS'06 (Poitiers, France), RTSS'04 (Lisbon, Portugal), WCET'04 (Catania, Italy)
- **Conférences nationales**
  - CFSE'04 (Croisic, France)
- **Ecoles thématiques du GDR ASR, pôle ResCom (anciennement TAROT et ING)**
  - ING'05 (Le Touquet, France), Ecotel'04 (Zarzis, Tunisie)
- **Ecole thématique du GdR ARP - Thème StrQdS (Systèmes Temps Réel - Qualité de Service)**
  - ETR'05 (Nancy, France)

## Charges collectives

- **Ecole d'été Internet Nouvelle Génération 2005 (ING)**
  - Membre du comité d'organisation
  - Chargée de la communication (site web et charte graphique)
- **Fête de la science 2004**
  - Présentations et vulgarisation devant des groupes scolaires et du grand public.
- **EuroDocInfo 2008 (Rencontre Franco-Belge des doctorants en informatique et des industriels)**
  - Membre du comité d'organisation
  - Chargée d'hébergement, événements culturels et sportifs, accueil

## Relectures et évaluations d'articles scientifiques

- **Conférences**
  - CFSE'05, HiPC'05