

L'INRIA inaugure le premier laboratoire de haute sécurité de la recherche académique française dédié à des travaux dans le domaine de la sécurité informatique

Nancy, le 1^{er} juillet 2010 – Situé au cœur du centre INRIA Nancy-Grand Est, le laboratoire de haute sécurité informatique (LHS) est voué à accueillir des travaux de recherche déterminants pour sécuriser le réseau, les échanges sur internet et les équipements de télécommunications associés. Aux côtés de ses partenaires, l'INRIA inaugure aujourd'hui cet équipement de recherche inédit. Le LHS offre le cadre technologique et réglementaire nécessaire aux avancées scientifiques accompagnant les évolutions de notre société numérique. Ouvert aux partenaires industriels, le laboratoire représente également un cadre propice aux tests de fiabilité requis avant toute mise sur le marché de différents produits ou solutions technologiques.

Un équipement inédit pour accompagner des travaux de pointe en sécurité informatique

Placé dans un environnement fermé avec un réseau Internet isolé et des locaux protégés accessibles par reconnaissance biométrique, le laboratoire offre **un cadre technologique et réglementaire fiable pour mener des expérimentations et manipulations à caractères sensibles**. Il est conçu pour garantir la sécurité des données, des phénomènes et des équipements analysés.

Il est constitué de trois espaces distincts :

- une salle de travail qui accueille les chercheurs
- une salle de clusters dotée de trois unités :
 - **un télescope virtuel** qui recueille des codes malveillants, des traces d'attaques et qui permet l'expérimentation de sondes sur l'Internet ;
 - **un réseau fermé dit « éprouvette »** qui permet de mener des expériences sensibles comme l'analyse de codes malveillants sans risque de contamination de l'ensemble du réseau ;
 - **une unité de production** pour distribuer les outils développés au sein du LHS : anti-virus, outils d'analyses...
- **Une salle dite « rouge »**. Non connectée au réseau, elle concerne le traitement d'informations et de données très sensibles. Cette salle permet d'accueillir les équipements ou matériels à étudier en toute confidentialité dans le cadre de partenariats avec les industriels.

Trois grands domaines d'expertise : virologie, analyse et protection du réseau, et détection de vulnérabilités dans les systèmes communicants.

- **Virologie : comment reconnaître les virus de demain ?**

Les chercheurs de l'équipe CARTE analysent des codes malveillants et élaborent les anti-virus du futur. Ils ont mis au point **une nouvelle méthode de détection de virus qui prend en compte un paramètre fondamental : la capacité des virus à muter, tout comme des virus vivants**. Primée au **concours national d'aide à la création d'entreprises de technologies innovantes 2009** dans la catégorie « Emergence », leur



méthode permet d'extraire la signature ou squelette du virus, c'est-à-dire le bout de programme qui ne change pas malgré les mutations.

« Ce résultat permet d'envisager des anti-virus plus efficaces puisque capables de reconnaître les virus même lorsqu'ils ont muté. D'autres défis scientifiques sont à relever, par exemple la mise au point de méthodes pour identifier les nouveaux virus, ceux dont on ne connaît pas le squelette ! Avec le LHS, nous disposons du cadre nécessaire pour mener nos expérimentations futures. », souligne Jean-Yves Marion, directeur de l'équipe CARTE.

D'autre part, l'équipe CARTE travaille sur la neutralisation des botnets, réseaux d'ordinateurs infectés qui servent à envoyer du spam mais qui pourraient aussi servir à attaquer des services Internet. Les chercheurs s'intéressent aussi à d'autres plateformes technologiques vulnérables comme les téléphones et les systèmes embarqués (exemple : voiture, ...)

➤ **Supervision du réseau : comment analyser et sécuriser les échanges sur le réseau ?**

Les chercheurs de l'équipe MADYNES étudient les grands systèmes de communication pour comprendre leur fonctionnement et mettre en place des systèmes d'analyse et de contrôle, notamment pour lutter contre les failles de sécurité.

Parmi leur derniers résultats : la conception d'un **algorithme permettant de placer des sondes sur un grand réseau pair à pair et d'observer l'activité sur ce réseau**. Les chercheurs ont réussi à analyser le trafic sur un réseau de 4 millions de machines, en plaçant une vingtaine de sondes et sans recourir à de grandes capacités de calcul.

« Plusieurs domaines d'applications sont d'ores et déjà envisagés notamment dans le cadre du programme ANR MAPE, pour aider les autorités compétentes dans la lutte contre la cybercriminalité » précise Olivier Festor, directeur de l'équipe.

➤ **Détection de vulnérabilités dans les systèmes communicants : permettre aux industriels de mener des tests de fiabilité**

En phase de conception et de certification, les équipementiers ont besoin de pouvoir tester la fiabilité de leurs équipements, d'évaluer leur résistance à différents types d'attaques ou de menaces.

Avec un réseau internet isolé et des équipements ultrasécurisés, le LHS est un cadre propice pour réaliser ce type de tests.

Parmi les risques identifiés figurent notamment les services de téléphonie sur internet. Dans ce domaine, les chercheurs de l'équipe MADYNES ont mis au point une suite logicielle baptisée KIF qui permet de détecter automatiquement les failles sur la téléphonie sur IP.

Une structure inédite en France impliquant de nombreux partenaires

Le Laboratoire de haute sécurité informatique du Centre INRIA Nancy Grand Est a bénéficié des financements du FEDER, de la Région Lorraine, de la Communauté urbaine du Grand Nancy et du Ministère de l'Enseignement Supérieur et de la Recherche via la Délégation Régionale à la Recherche et à la Technologie. Les recherches entreprises sont menées en partenariat avec les universités lorraines, le CNRS et la Délégation Générale à l'Armement.



À propos de l'INRIA

Établissement public à caractère scientifique et technologique, sous tutelle des ministères chargés de la Recherche et de l'Industrie. Budget annuel (2009) : 217 M€ dont 21% de ressources propres. Centres régionaux de recherche : Paris - Rocquencourt, Sophia Antipolis – Méditerranée, Grenoble – Rhône-Alpes, Nancy – Grand Est, Rennes – Bretagne Atlantique, Bordeaux – Sud Ouest, Lille – Nord Europe, Saclay – Île-de-France. 3 150 chercheurs, dont plus de 1000 doctorants, travaillant dans plus de 170 équipes-projets dont la plupart sont communes avec d'autres organismes, des grandes écoles, des universités. 80 équipes associées dans le monde. Une centaine d'entreprises créées depuis 1984.

Pour en savoir plus : **www.inria.fr**

Contacts presse INRIA

INRIA

Laurence Hermant

+ 33 (0)1 39 63 57 29 / 06 82 82 29 46

laurence.hermant@inria.fr

GolinHarris pour l'INRIA

Cécile Lardillon

+ 33 (0)1 40 41 54 83

cecile.lardillon@golinharris.com

