# Simulation d'Attaques sur les Systèmes Distribuées

(informatique distribuée, systèmes d'exploitation, sécurité/cryptologie, réseaux)

*Lieu du stage* : LIP6, 104 avenue du Président Kennedy, 75016 Paris, France
*Équipe* : NPA, Projet INRIA Grand Large
*Directeur de stage* : Sébastien Tixeuil (Sebastien.Tixeuil@lip6.fr)

**Présentation générale du domaine :**

Dans un réseau comprenant plusieurs milliers de machines, l'apparition de défaillances est inévitable. Certaines applications dites "pair à pair" impliquent de grandes quantités d'utilisateurs, par exemple pour échanger des fichiers ou pour exécuter de longs calculs (SeTi@Home, Decrypthon, Xtremweb, Boinc...). Dans ce type d'application, l'apparition et la disparition des nœuds participants sont imprévisibles, extrêmement fréquentes et s'effectuent inévitablement pendant un calcul.

Un autre point important est l'essor actuel de la mobilité dans les réseaux. Il est fondamental de vérifier le comportement d'une application dans un environnement où des fautes intermittentes apparaissent de façon non déterministe. De plus, les fautes ont généralement tendance à se propager localement (par exemple lorsqu'un ver réussit à contourner le pare-feu d'un réseau, toutes les machines de ce réseau seront très probablement touchées).

Pouvoir simuler les attaques de programmes néfastes permet de tester la résistance des applications distribuées que l'on conçoit, et par suite d'améliorer leur robustesse.

**Objectifs du stage :**

Le but du stage est de développer un simulateur d'attaques sur les systèmes distribués. Pour simuler les attaques, on améliorera un outil développé par l'équipe (écrit pour sa plus grande partie en C++). Cet outil permet de spécifier des scénarios d'apparition de fautes (pannes crash et redémarrage) dans un langage de haut niveau à base d'automates communicants, et de les injecter dans l'application sous test. Une première extension est de permettre un contrôle plus précis des applications testées, et en particulier :

1. On souhaite pouvoir modifier la valeur des variables d'un programme situé sur une machine particulière en cours d'exécution (pour modéliser le fonctionnement de certains virus ou chevaux de Troie) ;
2. On souhaite pouvoir modifier la valeur du pointeur de programme (c'est-à-dire ce qui spécifie le code qui va être prochainement exécuté) d'un programme, de manière à modéliser une attaque par dépassement de tampon (*buffer overflow*).

Les extensions développées seront ensuite testées sur des applications réelles, soit programmées de manière *ad hoc*, soit réutilisées à partir de codes sources existants.

**Compétences espérées :**

C++