Thèse : Résilience et cybersécurité dans le cloud

Directeurs de thèse :

Philippe Owezarski, LAAS-CNRS (owe@laas.fr)
Pascal Berthou, LAAS-CNRS (berthou@laas.fr)

Sujet :

Le Cloud Computing a bouleversé la façon dont nous développons et déployons les logiciels. De nos jours, les applications Cloud sont conçues comme des systèmes distribués en permanente évolution, hébergés dans des data-centers, et potentiellement même dispersés dans le monde entier. Ce changement de paradigme augmente de facto la surface d'attaque des systèmes cloud, et leur importance stratégique en fait une des cibles privilégiées des pirates informatiques de tous bords. La protection des systèmes cloud est d'autant plus difficile que ce même changement de paradigme a également eu un impact considérable sur la façon dont les logiciels sont monitorés : les applications Cloud peuvent se composer de plusieurs centaines de services, et les outils de monitoring ont rapidement rencontré des problèmes de passage à l'échelle. De plus, il faudrait que ces outils de monitoring soient désormais également capables de traiter les défaillances et les pannes inhérentes aux systèmes distribués, comme par exemple, les pannes partielles, les configurations incohérentes, les goulots d'étranglement ou même la vampirisation de ressources, qu'ils soient inhérents au comportement d'un ordonnanceur cloud comme Kubernetes ou la conséquence d'actions malveillantes provenant de l'intérieur ou de l'extérieur du cloud..

Cette thèse a donc pour objectif de concevoir de nouvelles méthodes de tracing distribué pour la détection et la mitigation d'anomalies et d'attaques dans le cloud. Le tracing distribué (via OpenTelemetry par exemple) devra permettre de collecter les événements se produisant à tous les niveaux du cloud (containers, machines virtuelles, zones, clusters). L'objectif sera alors d'exploiter ces événements grâce à des modèles d'analyse de séries temporelles, de graphes, de logiques, etc. afin de représenter le fonctionnement du cloud. Par des techniques d'apprentissage automatique (par exemple), des déviations suspectes pourront être détectées et analysées afin d'identifier des erreurs de configuration ou des attaques, et les contrer.