Proposition de recherche doctorale

Rapid securisation of operating system kernels

Mots clés :

- Directeur de thèse : Julia LAWALL
- Co-encadrant(s) :
- Unité de recherche : INRIA-Paris
- École doctorale : École Doctorale Informatique, Télécommunications, Électronique de Paris
- Domaine scientifique principal : Sciences et technologies de l'information et de la communication

Résumé du projet de recherche (Langue 1)

A quick glance at the news shows that computing systems are increasingly under attack. Attackers exploit bugs in software to mount security attacks, access and release confidential information, destroy critical information, and otherwise break the functionality of systems on which all levels of society rely. Fixing bugs in software, rapidly and reliably, is thus of critical importance. This is particularly the case of operating systems, such as Linux, Windows, etc. All aspects of computing rely on the operating system for essential services, implying that any vulnerability at the operating system level can have potentially catastrophic consequences. Today, the Linux operating system and the ecosystem around it represent an attractive platform for individuals, companies, governments, and organizations, as it offers high reliability, fast evolution, and little or no startup cost. In practice, however, Linux is not a single operating system, but rather a collection of variants: the mainline release, with all of the latest features but limited testing; the stable versions, which are variants of recent releases that have been augmented with bug-fixing patches; the distributions such as Debian or Fedora, which are stable versions that have been customized for a particular ecosystem; variants such as Android that target computing platforms with specific needs; and a plethora of old versions that continue to be used to ensure stability or to support local customizations. This introduces a major maintenance challenge. Bug fixes, including security fixes, have to be propagated from the latest mainline release to the stable versions, the distributions, and so on. Each step potentially requires adaptation of the fix to a new usage context. This adaptation is currently manual, time-consuming, and error-prone, implying that fixing one bug can introduce another. Ultimately, the fixing cost becomes too high, leaving code vulnerable to attacks. The Whisper team at Inria has been developing tools to aid in understanding code changes and the automated updating of source code, targeting the Linux kernel. The goal of this PhD is to build on these tools to understand the challenges of porting bug fixes across different Linux kernel variants, and to design approaches to automate this process. This research will lead to a tool suite that allows system maintainers to rapidly secure their systems with the latest bug fixing patches, despite local customizations.