

## Android Security

Mobile market is now dominated by the Android Operating system. Malware development has become a full time job where attackers steal private data, erase or block the devices, or even sell the controlled devices for further attacks. Studying malware at large scale is a difficult task because each malware is technically different and uses multiple techniques to escape automatic analysis. Thus, new tools have to be designed to help security experts to investigate malware.

Additionally, designing new malware that may have high impact in the near future helps to prepare countermeasures. For example, piggybacked applications repackage a regular applications and include malicious code in the library parts. Such malicious applications are now commonly found on application markets. Thus, it is important to work on new generations of malware that may be developed in the next years.

For critical applications, the industry tries to introduce more secure hardware components embedded in the smartphone. Some devices have TEE and support an isolated operating systems. Such environments may be used in the future for applications that require a high level of trust. Additionally, such components may offer new techniques of programming applications that would increase the defense of a normal application that is run in the regular operating system.

Different research directions can be investigated during a PhD thesis:

- Interactive visualization of malware: can we learn from a running malware when browsing its inside ?
- Steganography and Malware: how modern malware can build invisible channels to leak data from a mobile ?
- Are the TEE technologies sensible to steganographic malware ?
- Abuse of regular applications: is it possible to abuse regular apps when knowing about their bytecode ?
- Are the TEE technologies able to propose defensive programming techniques to applications of the rich OS ?

**Laboratory & Team:** LIFO, Systems and Data Security

**Host institution:** INSA Centre Val de Loire

**Advisors:** Dr. Jean-Francois Lalande

**Contacts:** jean-francois.lalande@insa-cvl.fr

<http://www.univ-orleans.fr/lifo/Members/Jean-Francois.Lalande/>