Valentin Manès
Information Security Researcher

Contact
valentinmanes@outlook.fr

Profil
Researcher in
Information Security.
Specialized in System
and Software security

Programming
C, Go, Python
Assembly

Languages
French Mother Tongue
English: Near Native
Spanish: Fluent
Korean: Basics
Japanese: Basics

Interests
Languages
History
Travel

Experience

2016-2018   **Cyber Security Research Center - KAIST**   Daejeon, South Korea
Following the year I spent in KAIST as an exchange student, I decided to pursue the research I started in CSRC. I have worked on developing a kernel hardening solution by limiting its attack surface (see below). Recently, I changed my focus to binary analysis and fuzzing in particular.

Education

2015-2016   **KAIST - One Year Exchange**   Daejeon, South Korea
In KAIST, I continued studying Information Security and started focusing in Hardware-based trusted execution environment and kernel hardening. I also developed an interest in binary analysis.

2013-2016   **Telecom ParisTech - Master's degree**   Paris, France
Telecom ParisTech, one of France's top five graduate sciences schools (*grandes écoles*), is considered the leading French school in Information and Communication Technology (ICT). I have specialized myself in **Information Security**.

2011-2013   **Lakanal - Preparatory School**   Sceaux, France

Projects & Publications

2017   **Domain Isolated Kernel (DIKernel)**   CSRC - KAIST
Computer & Security, Elsevier
We identify kernel extensions (i.e. modules, drivers) as the weakest kernel part concerning its security. Thus, DIKernel isolate extensions by lowering their memory access permission and their execution privilege. We keep our solution convenient for both the end users, by ensuring a low performance cost, and developers, by not requiring any change in extensions' code.

2016   **Twisted Fate**   KAIST
Twisted Fate is a gcc plugin that injects the stack diversifier routine to randomly change the stack before call and ret instructions. Designed to mitigate ROP chain and return-into-libc attacks. Inspired by Isomeron (fine-grained ASLR) and shadow-stack solutions.

2015   **Defeating Flush+Reload Attack**   KAIST
In a cloud computing environment, the Flush+Reload attack allows for an attacker to extract sensitive information hosted on a Virtual Machine. In this project, we focused on the *clFlush* instruction used for flushing a CPU cache line. We proposed a detection scheme with low overhead in the case of an usual usage of *clFlush*.