Kévin Szkudłapski

Personal Data

France 1st May 1987
blog szkudl.k@gmail.com @wiskitki wisk

Work experience

09/2011 - Now	Low level reverse engineer at Quarkslab, Paris reverse engineering: Windows, Linux, RTOS, software assessment, vulnerability research: baseband, bootrom, ECU, ..., training, malware analysis, development of tools: code analyzer, desobfuscation, debugging features for an undocumented DSP.
05/2010 - 10/2010	Internship at EADSW IW, Suresnes Implementation of *GDB stub* for DynaMIPS emulator, development of *forensic* tool for Linux kernel (X86-32, ARMv7), *unpacking* with miasm, VNC client exploitation (Linux), analysis of USB *debug port* in Windows, analysis of *BitLocker* and developement of a *FUSE* module to mount this filesystem on Linux.
07/2008 - 12/2008	Internship at ESL (EPITECH Security Lab.), Kremlin-Bicêtre Compilation and decompilation technics in heterogeneous software environment.

Grades

2012	Master degree at Epitech Paris (computer science school) at Kremlin-Bicêtre
2010	Bachelor degree at Epitech Paris (computer science school) at Kremlin-Bicêtre
2007	Baccalauréat S option SI (*Engineering Sciences*) *Lycée* Jules Ferry at Versailles

Languages

French:	Mother tongue
English:	Fluent

Computer Skills

Assembly:	6502/65c816, ARMv7, MIPS, PowerPC, x86 16/32/64
Libraries:	standard C, STL, Qt, Boost, Win32 API, LLVM
CMS:	Git, SubVersion, Mercurial
Development:	C, C++, Python, Ruby, Bourne Shell, CMake
IDE and text editor:	Visual Studio, Sublime, VIM
Tools:	IDA Pro, WinDBG, OllyDbg, x64dbg, GDB, medusa
Writing:	MS Office, MS Visio, LaTeX, RST/Sphinx
Operating system:	Windows, ArchLinux/Ubuntu, FreeBSD/OpenBSD

Personal projects

Medusa, tool to analyze executable by disassembling, emulating, symbolic execution, recompiling, viewing control flow graph, ...	
Analysis of a game named Shovel Knight and discovery of a *DevMenu*	
Development of a Nintendo Super NES ROM to test HDMA effect	
DOSBox port for Nintendo Wii and writing of a dynamic-recompiler for it	You Tube
Development of IDA loader for Nintendo GameBoy	unavailable
Analyze of the network protocol for the game *Rune of Magic* and development of a basic *proxy*	unavailable

Publications

How to emulate executable with Medusa and python (en)	↗
AppContainer analysis (en)	📄
RTTI information on program compiled in C++ (en)	↗
Feedback on how to write a processor module for IDA in C++ (en)	↗
Undocumented mitigation analysis (en)	↗
Windows 8 mitigations analysis (fr)	↗
PowerPC shellcoding (en)	unavailable

Hobbies

Systema (russian martial art), reverse engineering, retro-gaming, travels