Andrea Fioraldi

Quickly translated and incomplete copy of the curriculum vitae in Italian, please refer to the English curriculum for a complete version.

Via [REDACTED], [REDACTED]
Pontinia, LT. 04014 Italia.

Telefono: +39 [REDACTED]

email: andreafioraldi@gmail.com
blog: andreafioraldi.github.io
GITHUB: andreafioraldi
TWITTER: @andreafioraldi

Nato: [REDACTED], 1996—[REDACTED], Italy
Nazionalità: Italiana

Posizione corrente

Studente magistrale in Engineering in Computer Science, Sapienza Università di Roma.

Area di specializzazione

System Security • Binary analysis and exploitation

Riconoscimenti e premi

2017 Primo posto in Binary Analysis (ex aequo) a CyberChallenge.IT 17.
2017 Secondo posto in Penetration Testing a CyberChallenge.IT 17.
2017 Terzo posto con il Team Nazionale di Cybersecurity alla European CyberSecurity Challenge (ECSC).
2018 Settimo post al DEF CON 26 CTF (finale mondiale) con il team mHACKeroni.
2018 Primo posto al Chaos Communication Congress CTF con il team mHACKeroni+KJC.
2019 Quinti posto al DEF CON 27 CTF (finale mondiale) con il team mHACKeroni.

Laurea triennale

Ho ottenuto una laurea triennale in Ingegneria Informatica e Automatica all'università Sapienza di Roma con voto 110/110 e lode.
La mia tesi è "Symbolic Execution and Debugging Synchronization", disponibile su ResearchGate

Progetti rilevanti

Organizzazioni ed eventi

2017 Co-fondatore del team accademico di Capture The Flag TheRomanXploit (TRX).

2018 Co-fondatore del mega-team italiano di Capture The Flag mHACKeroni.

2018 Fondatore del DEF CON 11396 Rome, un gruppo che si riunisce ogni mese per talk su argomenti avanzati di computer security al di fuori del comune piano di studi.

Software

2017-2018 *Carbonara*, a malware research platform designed to recognize duplicated functions between binaries at scale and speed-up the static malware analysis process

2018 *angrdbg*, an abstract library used to implement synchronization between a concrete execution environment (tipically a debugger) and the angr symbolic execution engine

2018 *IDAngr*, an IDA Pro debugger plugin that implements the angrdbg API in IDA with an user-friendly GUI

2018 *angrgdb*, create an angr state from the current GDB state on top of angrdbg

2019 *AFL++*, AFL 2.56b with community patches, AFLfast power schedules, QEMU 3.1 upgrade + laf-intel support, MOpt mutators, InsTrim instrumentation, Unicorn mode and a lot more!

Interessi di ricerca

Il mio principale interesse in security è scrivere strumenti per automatizzare la Binary Analysis usando tecniche avanzate come l'Esecuzione Simbolica, l'Istrumentazione Dinamica dei binari, il Taint Tracking e altro.
Ad'ora ricerco nuove metodologie per lo Smart Fuzzing.
Sono bravo nella ricerca di vulnerabilità, nella binary exploitation e nella malware analysis poichè sono i topic di applicazione della mia attività di ricerca.
Sono anche un entusiasta della teoria dei linguaggi di programmazione. Ho sviluppato diversi linguaggi di programmazione educazionali sia per la mia stessa educazione che per l'educazione del giovani compagni di team in TRX riguardo le vulnerabilità e l'exploitation dei Linguaggi di Programmazione.

Competenze tecniche

Linguaggi di programmazione

Sono molto proficuo con il C, C++, Python, ASM x86 ed ho familiarità con Javascript, Java, Scala, C#.

Sistemi operativi

Sono bravo nello scrivere codice per sistemi POSIX e non male con MS Windows (sviluppo userspace).
Conosco gli internals del sistema GNU/Linux e ho familiaritò con la codebase del kernel.

Strumenti di secruity

Conosco molto bene come usare IDA Pro, GDB, Frida, ed Intel PIN ad, inoltre, so usare e conosco il funzionamento interno di American Fuzzy Lop, QEMU TCG ed angr. Ho esperienza limitata con radare2.

Volontariato

2018 Ho insegnato Binary Exploitation a CyberChallenge.IT 2018 e 2019 a Roma.

Hobbies and Passions

Tromba • Birra fatta in casa • Trekking • Mountain bike

Last updated: September 2, 2020 • Typeset in XeLaTeX

https://raw.githubusercontent.com/andreafioraldi/CurriculumVitae/master/cv.pdf