Marco Cianfriglia

Presentazione:
Attualmente ho una posizione da postDoc presso Istituto per le Applicazioni del Calcolo 'Mauro Picone' del CNR. Ho una laurea Magistrale in Informatica e un dottorato in Matematica. Sono specializzato su sicurezza informatica, crittografia, digital forensics, GPGPU, HPC.

ESPERIENZA LAVORATIVA

31/10/2017 – ATTUALE – Roma, Italia
PHD RESEARCH FELLOW – ISTITUTO APPLICAZIONI PER IL CALCOLO (IAC) "MAURO PICONE" - CNR

I miei interessi di ricerca riguardano la crittografia e la crittanalisi, digital forensics, la sicurezza dei dati e dei sistemi, Big Data, Graph analytics, GPGPU e HPC.
Lavoro su diversi progetti che spaziano dalla crittanalisi su GPU, all'analisi di grafi di grandi dimensioni, arrivando all'indicizzazione efficiente di grandi moli di dati eterogenei.
Mi occupo di sviluppo e progettazione di codici efficienti e ad alto livello di parallelismo, e dell'ottimizzazione e messa in sicurezza di codice esistente. Mi occupo anche della configurazione e manutenzione di diversi sistemi di produzione.

03/2019 – Roma, Italia
DOCENTE A CONTRATTO – LUISS - LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI GUIDO CARLI

Docente del corso "Security Management" presso School of Law - Master in Cybersecurity

03/2018 – 09/2019 – Roma, Italia
DOCENTE UNIVERSITARIO A CONTRATTO – UNIVERSITÀ DEGLI STUDI DI ROMA TRE

Docente del corso di "Abilità Informatiche e telematiche" Laurea Magistrale in Informazione, Editoria e Giornalismo

05/2018 – Modena, Italia
DOCENTE A CONTRATTO – UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Corso "Digital and Mobile Forensics" presso Cyber Academy

03/2018 – Modena, Italia
DOCENTE A CONTRATTO – UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Corso "Forensics on Android" presso Master in Digital Forensics e Tecnologie Cyber

05/2016 – 07/2016
ASSISTENTE ALLA DIDATTICA – UNIVERSITÀ DEGLI STUDI DI ROMA "LA SAPIENZA"

Master I livello Cybercrime e Informatica Forense - Corso "Analisi dei sistemi compromessi"

05/2017 – 08/2017 – Cambridge, Regno Unito
RESEARCH INTERN – DIVIDITI L.T.D.

Ho sviluppato un framework che utilizza tecniche di Machine Learning per ottimizzare in maniera automatica applicazioni Data-Driven.
Mi sono inoltre occupato dell'ottimizzazione di librerie scientifiche per System-on-Chip SoC (ad esempio ARM) ed ho sviluppato alcuni moduli per il software Collective Knowledge per gestire workflow di simulazioni scientifiche.
Il mio internship e' stato finanziato dal programma "HiPEAC Industrial PhD Mobility Programme".

11/2014 – 10/2017 – Roma, Italia
BORSA DI STUDIO DI DOTTORATO – UNIVERSITÀ DEGLI STUDI ROMA TRE

- Vincitore borsa di studio del M.I.U.R.
- Argomenti di ricerca : crittanalisi, GPGPU, digital forensics, HPC

02/2014 – 10/2014 – Roma, Italia
BORSA DI STUDIO DI RICERCA – ISTITUTO DELLE APPLICAZIONI DEL CALCOLO (IAC) - CNR

- Analisi di testi su GPU
- Ho partecipato al progetto europeo ISODAC (Indexing and Search Of Data Against Crime)

03/2013 – Roma, Italia
ASSISTENTE ALLA DIDATTICA – UNIVERSITÀ DEGLI STUDI ROMA TRE

Mi sono occupato delle sessioni di laboratorio per il corso "Advanced Course in Digital Forensics" organizzato nell'ambito del progetto europeo EATEP_FIT: European Antitrust Training and Exchange Programs in Forensic IT

ISTRUZIONE E FORMAZIONE

11/2014 – 04/2018 – Roma, Italia
DOTTORATO IN MATEMATICA - CRITTOGRAFIA E SICUREZZA DELLE INFORMAZIONI – Università degli Studi Roma Tre

Ho ridisegnato un attacco algebrico, chiamato Cube Attack, per renderlo utilizzabile in maniera efficiente su GPU. Ho inoltre sviluppato un framework che implementa questo attacco; questa variante dell'attacco specifica per GPU è stata chiamata kite-attack.
Inoltre durante il mio dottorato ho lavorato come Research Intern presso Dividiti L.t.d.

Advisor: Massimo Bernaschi
Reviewer: Prof. Giuseppe Ateniese, Prof. Roberto Di Pietro

Indirizzo Largo San Leonardo Murialdo 1, Roma, Italia |

Sito Internet https://matematicafisica.uniroma3.it/dottorato/2021/matematica-dott528/ |

Tesi Exploiting GPUs to speed up cryptanalysis and machine learning

09/2011 – 12/2013
LAUREA MAGISTRALE – Università degli Studi di Roma "La Sapienza"

Ho sviluppato lo Standard Analyzer e lo Standard Tokenizer di Apache Lucene in CUDA. ApacheLucene è la libreria standard-de-facto per l'indicizzazione.
I moduli che ho sviluppato sono stati integrati all'interno del porting C++ di Lucene, chiamato CLucene.

Advisor: Massimo Bernaschi

Campo di studio Computer Science | **Voto finale** Cum laude | **Tesi** Text analysis on Graphics Processing Unit

09/2005 – 04/2011
LAUREA TRIENNALE – Università degli Studi di Roma "La Sapienza"

Tesi: "Virtualization Security: definition, implementation and evaluation of kernel protection mechanisms of a Windows guest"

Ho sviluppato un agent basato su Qemu dedicato al tracciamento delle chiamate che vanno a modificare le strutture dati del kernel di un guest Windows7.

Advisor: Prof. Luigi V. Mancini

Campo di studio Computer Science | **Voto finale** 105/110 | **Tesi** Virtualization Security

COMPETENZE LINGUISTICHE

Lingua madre: **ITALIANO**

Altre lingue:

	COMPRENSIONE		ESPRESSIONE ORALE		SCRITTURA
	Ascolto	Lettura	Produzione orale	Interazione orale	
INGLESE	C1	C1	C1	C1	C1

Livelli: A1 e A2: Livello elementare B1 e B2: Livello intermedio C1 e C2: Livello avanzato

COMPETENZE DIGITALI

Le mie competenze digitali

Source code versioning (Git / SVN) | Operative Systems: Unix, Linux, Windows, Android | Programming and scripting languages: C, C++, CUDA-C, OpenCL, Java, PHP, Python, Bash | Versioning system: git, svn | Virtualization: KVM, Qemu, Virtualbox, VMware, XEN | Parallel and Concurrent Programming with MPI | Anonimity Networks

PUBBLICAZIONI

Reducing Bias in Modeling Real-world Password Strength via Deep Learning and Dynamic Dictionaries

https://arxiv.org/abs/2010.12269 – 2020
Authors: Dario Pasquini, Marco Cianfriglia, Giuseppe Ateniese, and Massimo Bernaschi

Critical nodes reveal peculiar features of human essential genes and protein interactome

https://doi.org/10.1109/BIBM47256.2019.8983221 – 2019
Authors: A. Celestini, M. Cianfriglia, E. Mastrostefano, A. Palma, F. Castiglione, and P. Tieri
2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)

Kite attack: reshaping the cube attack for a flexible GPU-based maxterm search

https://doi.org/10.1007/s13389-019-00217-3 – 2019
Authors: M. Cianfriglia, S. Guarino, M. Bernaschi, F. Lombardi, and M. Pedicini.
Journal of Cryptographic Engineering

On the Anatomy of Predictive Models for Accelerating GPU Convolution Kernels and Beyond

https://doi.org/10.1145/3434402 – 2018
Authors: Paolo Sylos Labini, Marco Cianfriglia, Damiano Perri, Osvaldo Gervasi, Grigori Fursin, Anton Lokhmotov, Cedric Nugteren, Bruno Carpentieri, Fabiana Zollo, and Flavio Vella.
ACM Transactions on Architecture and Code Optimization

Cryptanalysis on GPUs with the Cube Attack: Design, Optimization and Performance Gains

https://doi.org/10.1109/HPCS.2017.114 – 2017
Authors: M. Cianfriglia and S. Guarino
2017 International Conference on High Performance Computing
Simulation - HPCS 2017

A Novel GPU-Based Implementation of the Cube Attack

https://doi.org/10.1007/978-3-319-61204-1_10 – 2017

Authors: M. Cianfriglia, S. Guarino, M. Bernaschi, F. Lombardi, and M. Pedicini
Applied Cryptography and Network Security. ACNS 2017. Lecture Notes in Computer Science, vol 10355. Springer, Cham.

ISODAC: a High Performance Solution for Indexing and Searching Heterogeneous Data

https://doi.org/10.1016/j.jss.2015.11.043 – 2015
Authors: G. Totaro, M. Bernaschi, G. Carbone, M. Cianfriglia, and A. Di Marco
Journal of Systems and Software

PATENTE DI GUIDA

Patente di guida: B

CONFERENZE E SEMINARI

Ancora - Italia
ITASEC 2020 - Workshop on cryptanalysis

Ho presentato alcune applicazioni HPC e GPU che possono essere utilizzate per testare la sicurezza dei cifrari.

Europol - The Hague (NL)
Europol Forensic Expert Forum (FEF) 2019

Ho presentato alcune applicazioni di HPC che possono essere utilizzate dalle forze dell'ordine per accellerare il processi di analisi di dati forensi.

Genova - Italia
11st International Workshop on Security and High Performance ComputingSystems (SHPCS 2017)

Ho presentato i risultati del mio lavoro "Cryptanalysis on GPUs with the Cube Attack: Design, Optimization and Performance Gains"

UK Manycore Developer Conference (UKMAC 2017)

Ho presentato alcuni risultati ottenuti durante la mia internship presso Dividiti L.t.d.

Lugano - Switzerland
Summer School on Effective High Performance Computing 2016

Ho partecipato a questa scuola estiva organizzata da ETH Zurigo e dal Centro di Calcolo Italo Svizzero CSCS

Pula - Italia
Summer School on Computer Security and Privacy 2016

Sibenik - Croatia
Summer School on Real World Crypto and Privacy 2015

Roma - Italia
Introduction to Parallel Computing with MPI and OpenMP - 2014