Hany Ragab

Resume

Personal Information

First name	**Hany**.
Last name	**Ragab**.
Date of birth	**13.10.1991**.
Place of birth	**Milan, ITALY**.
Citizenship	**Italian**.

Education

2015 – Now	**Master of Science in Computer Science**, *University of Milan*, Milan, Italy.
2014	**Bachelor of Science in Computer Science**, *University of Milan*, Milan, Italy.
2010	**High School Diploma in Digital Communications**, *I.T.S.O.S. Albe Steiner*, Milan, Italy.

Bachelor Thesis

Title	***A KEY RECOVERY ATTACK ON SIX ROUNDS OF AES***
Supervisor	**Andrea Visconti**, Associate Professor at University of Milan.
Assistant Supervisor	**Silvia Mella**, PhD. student at University of Milan, Cryptographer at STMicroelectronics.
Description	I designed and implemented a CUDA C version of the Partial Sum Attack on a reduced version of AES block cipher.

Work Experience

Georgia Institute of Technology

Nov 2017 – Apr 2018	**Security Research Scholar**, *at* ***Georgia Institute of Technology***, **Systems Software & Security Lab, SSLab**. Klaus Advanced Computing Building, 266 Ferst Dr NW, Atlanta GA 30332-0765, Atlanta, Georgia, USA
Supervisor	**Taesoo Kim**, Assistant Professor at Georgia Tech. and leader in the SSLab, Georgia Institute of Technology.
Description	Macro topic: Intel SGX ... Work in progress.

☎ *(+39) 3391906535* • ✉ *hany.ragab.91@gmail.com* • *www.ragab.cc*
linkedin.com/in/hanyragab *@hanyrax* *hany.ragab91*

École Polythechnique Fédérale de Lausanne EPFL

Jul – Oct 2017 **Security Research Intern**, *at* ***École Polythechnique Fédérale de Lausanne***, **Laboratory for computer Communications and Applications 1, LCA1**.
EPFL IC IINFCOM LCA1, BC 207 (Bâtiment BC), Station 14, CH-1015 Lausanne, Switzerland

Direct Supervisor **Juan Ramón Troncoso-Pastoriza**, Post-doctoral Researcher at LCA1, École Polythechnique Fédérale de Lausanne.

Supervisor **Jean-Pierre Hubaux**, Full Professor at EPFL and head of the LCA1, École Polythechnique Fédérale de Lausanne.

Description A detailed theoretical and practical study of Intel® Software Guard Extensions (Intel® SGX), in particular I studied a wide range of side-channel attacks that has been attempted on the Intel SGX architecture, both from an offensive and defensive view point, along with different countermeasures. The target of this internship was attacking through a side-channel a genome data processing application based on Intel SGX, in order to extract and expose the sensitive data being processed by the application at run-time.

STMicroelectronics

Feb – Aug 2015 **Cryptanalysis Intern**, *at* ***STMicroelectronics***, **Advanced System Technology - Security Division**.
Via Camillo Olivetti 2, 20864 Agrate Brianza, MB, Italy

Direct Supervisor **Filippo Melzani**, Security Engineer at AST-Security, STMicroelectronics.

Supervisors **Guido Bertoni**, Cryptographer at AST-Security, STMicroelectronics.
Ruggero Susella, Security Engineer at AST-Security, STMicroelectronics.

Description A detailed study of hardware side-channel attacks, in particular, differential power analysis attacks against smart cards hardware implementation of AES block cipher. Analysis of both univariate and multivariate attacks, design and development of an evaluation tool for masking countermeasures schemes against High-order DPA.

Activities

Teaching Assistance

Mar 2017 **Laboratory of Operating Systems**, *University of Milan*, course link.

Supervisor **Mattia Monga**, Associate Professor at University of Milan.

Laboratories & Research Groups

2015 – Now **Member of LASER - Computer and Network Security Laboratory**, *University of Milan*, security.di.unimi.it.

Supervisors **Danilo Mauro Bruschi**, Full Professor at UNIMI and head of LASER, University of Milan.
Andrea Lanzi, Associate Professor at UNIMI, University of Milan.

2015 – Now **Member of Fuffateam - LASER CTF team**, *University of Milan*, l4ser.github.io.

2014 – Now **Co-Founder of CryptCoffee - A research group that focuses on applied cryptography and information security**, *Milan*, crypt.coffee.

2012 – 2015 **Member of CLUB - Cryptography and Coding Laboratory**, *University of Milan*, club.di.unimi.it.

Supervisors **Andrea Visconti**, Associate Professor at UNIMI, University of Milan.

Publications

2015 **On the weaknesses of PBKDF2**, *Visconti A., Bossi S., Ragab H., Calò A.*, The 14th International Conference on Cryptology and Network Security.

Code Contributions

Cryptsetup v1.7.0, *Security bug report & patch*, link.
Libgcrypt, *Security bug report & patch review*, link.
MbedTLS, *Security bug report*.

Projects

Mar 2016 **Skul**, *A password recovery tool that was born as a proof-of-concept to attack the Cryptsetup implementation of Linux Unified Key Setup (LUKS)*.

Github page: https://github.com/cryptcoffee/skul
Blog page: http://crypt.coffee/research/luks.html

Skul has been integrated within the BlackArch Linux cracking tools.
https://blackarch.org/tools.html

Security Meetings

Sep 2017 **BSides Zurich Conference**, *Open Systems AG, Global Headquarters, Zurich, Switzerland*.

Nov 2016 **Black Hat Europe**, *London Design Center, London, UK*.

I was awarded one of 100 worldwide scholarships to attend the Black Hat briefings on November 3rd and 4th.

Nov 2016 **CANS16, the 15th International Conference on Cryptology and Network Security**, *Palazzo Greppi, Milan, Italy*.

I participated as an organizing staff member.

Computer Science Related Skills

Programming Languages

Advanced	C, Python
Intermediate	x86/x86-64 Assembly, Java, Shell Scripting, C++

Operating Systems

Advanced	Linux, Mac OS
Intermediate	Microsoft Windows

Software Development Applications

Z3 sat solver, radare2, IDA Pro, Nvidia Nsight, Eclipse, Git, Vim

Relevant Coursework

Grade	
30CL/30	**Security and Privacy**.
30CL/30	**Advanced Computer Security**.
30CL/30	**Advanced Cryptography**.
30/30	**Cryptography**.
	Operating Systems
	Algorithms and Data structures
	Algorithms and Data structures II
	Algorithms and Complexities
	Web Algorithmics
	Heuristic Algorithms
	Distributed Systems

**CL = Cum Laude*

Languages

Native	Italian
Native	Arabic
C1	English
Basics	French

Extra interests

- Wingsuite base jumping
- Skydiving
- Boxing
- Football
- Traveling