

Personal information

Surname(s) / First name(s)

Address(es)

Telephone(s)

Email(s)

WWW

Nationality

Date of birth

Gender

Paleari, Roberto

Via Vittorio Emanuele 9, 20023, Cerro Maggiore (MI), Italy

(+39) 0331 421653 Mobile: (+39) 328 5751770

roberto.paleari@gmail.com

<http://roberto.greyhats.it/>

Italian

July 4, 1982

M



Desired employment / Occupational field

Computer security and networking

Education and training

Dates

March 25, 2011

Title of qualification awarded

Philosophy doctor in Computer Science, with dissertation titled "*Dealing with next-generation malware*"

Name and type of organization
providing education and training

Università degli Studi di Milano

Level in national or international
classification

PhD (Dottorato di Ricerca)

Dates

April 16, 2007

Title of qualification awarded

Master Degree in Information and Communication Technologies with a final grade of 110/110 *cum laude*
and a work on "*Dynamic analysis of executable code*"

Name and type of organization
providing education and training

Università degli Studi di Milano

Level in national or international
classification

Master Degree (Laurea Magistrale)

Dates

December 14, 2004

Title of qualification awarded

Bachelor Degree in Computer Science at the University of Milan with a final grade of 110/110

Name and type of organization
providing education and training

Università degli Studi di Milano

Level in national or international
classification

Bachelor Degree (Laurea Triennale)

Dates

December 01, 2004 – December 31, 2004

Title of qualification awarded

FSE (European Social Fund) course on Java Network Programming

Principal subjects / occupational skills

The course provides a general background in network fundamentals, as well as a detailed discussion of Java's facilities for network programming

Name and type of organization
providing education and training

Università degli Studi di Milano

Level in national or international
classification

Training course

Dates

A.S. 2001/2002

Title of qualification awarded

High School Diploma, Computer Science specialization, with a final grade of 100/100

Name and type of organization providing education and training

ITIS S. Cannizzaro, Rho (MI)

Work experience

Dates
Main activities and responsibilities
Name and address of employer
Type of business or sector

April 2008 – May 2008
Penetration testing and vulnerability assessment
Freelance
ICT security

Dates
Occupation or position held
Main activities and responsibilities
Name and address of employer
Type of business or sector

July 2006 – April 2007
Stageur
Analysis and development of a framework for finding security vulnerabilities in x86 executables
CERT-IT (Computer Emergency Response Team, Italy)
Research

Dates
Occupation or position held
Main activities and responsibilities
Name and address of employer
Type of business or sector

March 2004 – October 2004
Stageur
Analysis and development of a semi-automated incident management system
CERT-IT (Computer Emergency Response Team, Italy)
Research

Dates
Main activities and responsibilities
Name and address of employer
Type of business or sector

2004 – 2006
IT assistance and maintenance in small offices
Freelance
IT assistance

Personal skills and competences

Mother tongue(s)

Italian

Self-assessment
European level^(*)

English

French

Understanding				Speaking				Writing	
Listening		Reading		Spoken interaction		Spoken production			
B2	Independent user	C2	Proficient user	B2	Independent user	B2	Independent user	C1	Proficient user
A2	Basic user	A2	Basic user	A1	Basic user	A1	Basic user	A1	Basic user

^(*) Common European Framework of Reference (CEF) level

Social skills and competences

I like to work in dynamic environments and multi-cultural teams. During my stages at CERT-IT and during my Ph.D. studies I have acquired good skills in working in medium-size teams, but I have always kept a good working autonomy. My teaching experiences significantly contributed to develop my social skills.

Organizational skills and competences

During my research Ph.D. projects I developed good organizational and problem-solving skills. I also supervised several students during their Bachelor and Master of Science theses.

Technical skills and competences

ICT security

- * Very good knowledge of ICT security issues and their countermeasures.
- * Very good knowledge of techniques for the exploitation of security-relevant flaws and countermeasures.
- * Experience in vulnerability analysis (both in web application, source code and machine code).
- * Experience in malicious code analysis. Very good knowledge of techniques used by malicious code for infection, hiding and propagation. Very good knowledge of anti-malware approaches (both signature-based and behavioral-based).
- * Experience in incident handling, developed in the CERT-IT incident response team. Good knowledge of recent spamming and phishing techniques and countermeasures.
- * Experience in the reverse engineering of binary (IA-32) programs.
- * Good knowledge of network attacks and application security issues (both in web and binary applications). Good knowledge of basic cryptography.

Operating systems

- * Very good knowledge and good management expertise on Linux systems.
- * Good knowledge and fairly good management expertise on Windows systems (of different versions).
- * Good knowledge of the internals of Linux and Windows operating systems.
- * Experience in the development, analysis and testing of CPU emulators.

Networking

- * Good knowledge of the most important network infrastructures and protocols.
- * Fairly good administration skills of networking devices.

Programming languages

- * Very good knowledge of C/C++, Python and Assembly (IA-32).
- * Good knowledge of Java, shell scripting, PHP, HTML and XML.
- * Fairly good knowledge of Javascript and Perl.
- * Good knowledge of the UML modelling language.

Databases

- * Good knowledge of SQL and relational DBMSes.
- * Good analysis and design skills.
- * Basic knowledge of object-oriented DBMS.

Publications

ASE 2010

A. Fattori, R. Paleari, L. Martignoni, and M. Monga.
Dynamic and transparent analysis of commodity production systems.
In *Proceedings of the 25th IEEE/ACM International Conference on Automated Software Engineering (ASE)*, Antwerp, Belgium, Sept. 2010

RAID 2010

L. Martignoni, A. Fattori, R. Paleari, and L. Cavallaro.
Live and trustworthy forensic analysis of commodity production systems.
In *Proceedings of the 13th International Symposium on Recent Advances in Intrusion Detection (RAID)*, Ottawa, Canada, Sept. 2010

ISSTA 2010

L. Martignoni, R. Paleari, G. Fresi Roglia, and D. Bruschi.
Testing system virtual machines.
In *Proceedings of the 2010 International Symposium on Testing and Analysis (ISSTA)*, Trento, Italy, July 2010

- ISSTA 2010 R. Paleari, L. Martignoni, G. Fresi Roglia, and D. Bruschi.
N-version disassembly: differential testing of x86 disassemblers.
In *Proceedings of the 2010 International Symposium on Testing and Analysis (ISSTA)*, Trento, Italy, July 2010
- USENIX 2010 R. Paleari, L. Martignoni, E. Passerini, D. Davidson, M. Fredrikson, S. Jha, and J. Giffin.
Automatic generation of remediation procedures for malware infections.
In *Proceedings of the 2010 USENIX Security Symposium International Symposium*, Washington, USA, Aug. 2010
- DIMVA 2010 L. Martignoni, R. Paleari, and D. Bruschi.
Conqueror: tamper-proof code execution on legacy systems.
In *Proceedings of the 7th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, Lecture Notes in Computer Science, Bonn, Germany, July 2010. Springer
- ICISS 2009 L. Martignoni, R. Paleari, and D. Bruschi.
A framework for behavior-based malware analysis in the cloud.
In *Proceedings of the 5th International Conference on Information Systems Security (ICISS 2009)*. Springer, Dec. 2009
- ACSAC 2009 G. F. Roglia, L. Martignoni, R. Paleari, and D. Bruschi.
Surgically returning to randomized lib(c).
In *Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC 2009)*. IEEE, Dec. 2009
- WOOT 2009 R. Paleari, L. Martignoni, G. Fresi Roglia, and D. Bruschi.
A fistful of red-pills: How to automatically generate procedures to detect CPU emulators.
In *Proceedings of the 3rd USENIX Workshop on Offensive Technologies (WOOT)*, Montreal, Canada, Aug. 2009. ACM
- ISSTA 2009 L. Martignoni, R. Paleari, G. Fresi Roglia, and D. Bruschi.
Testing CPU emulators.
In *Proceedings of the 2009 International Symposium on Testing and Analysis (ISSTA)*, Chicago, IL, USA, July 2009
- DIMVA 2009 E. Passerini, R. Paleari, and L. Martignoni.
How good are malware detectors at remediating infected systems?
In *Proceedings of the 6th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*. Springer, July 2009
- SESS 2009 M. Monga, R. Paleari, and E. Passerini.
A hybrid analysis framework for detecting web application vulnerabilities.
In *Proceedings of the 5th International Workshop on Software Engineering for Secure Systems*, Vancouver, Canada, May 2009. ACM.
to appear
- DIMVA 2008 E. Passerini, R. Paleari, L. Martignoni, and D. Bruschi.
Fluxor: detecting and monitoring fast-flux service networks.
In *Proceedings of the 5th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, Lecture Notes in Computer Science, Paris, France, July 2008. Springer
- DIMVA 2008 R. Paleari, D. Marrone, D. Bruschi, and M. Monga.
On race vulnerabilities in web applications.
In *Proceedings of the 5th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*, Lecture Notes in Computer Science, Paris, France, July 2008. Springer

Teaching experience

Dates	June 2010
Occupation or position held	Teacher
Main activities and responsibilities	Teacher for the course “ <i>Information security</i> ”
Name and address of employer	Centro di Formazione Professionale Vigorelli, Milano
Dates	April 2010
Occupation or position held	Teacher
Main activities and responsibilities	Teacher for the course “ <i>Fundamentals of security</i> ”
Name and address of employer	Università degli Studi di Milano
Dates	2009-2010
Occupation or position held	Teaching assistant
Main activities and responsibilities	Teaching assistant for the course “ <i>Information security 2</i> ” (“ <i>Progetto della sicurezza di rete</i> ”)
Name and address of employer	Università degli Studi di Milano
Dates	June 2009
Occupation or position held	Teacher
Main activities and responsibilities	Teacher for the course “ <i>Security attacks</i> ”
Name and address of employer	Centro di Formazione Professionale Vigorelli, Milano
Dates	May 2009 – June 2009
Occupation or position held	Teaching assistant
Main activities and responsibilities	Teaching assistant “ <i>Abilità informatiche</i> ”
Name and address of employer	Università degli Studi di Milano, corso di laurea in Chimica e Tecnologie Farmaceutiche
Dates	March 2009
Occupation or position held	Lecturer
Main activities and responsibilities	Lecturer for the talk “ <i>Malware and underground economy</i> ”, held during CLUSIT Security Summit 2009
Name and address of employer	CLUSIT, Milano
Dates	January 2009 – February 2009
Occupation or position held	Teacher
Main activities and responsibilities	Teacher for the course “ <i>Information security</i> ”
Name and address of employer	Centro di Formazione Professionale Vigorelli, Milano
Dates	2008-2009
Occupation or position held	Teaching assistant
Main activities and responsibilities	Teaching assistant for the course “ <i>Information security 2</i> ” (“ <i>Progetto della sicurezza di rete</i> ”)
Name and address of employer	Università degli Studi di Milano
Dates	2008-2009
Occupation or position held	Teaching assistant
Main activities and responsibilities	Teaching assistant for the course “ <i>Information security</i> ” (“ <i>Sicurezza dei calcolatori e delle reti</i> ”)
Name and address of employer	Università degli Studi di Milano
Dates	September 2008
Occupation or position held	Teacher
Main activities and responsibilities	Teacher for the course “ <i>Hacker techniques and tools</i> ”
Name and address of employer	GFI Italia, Roma
Dates	June 2008

Occupation or position held	Teacher
Main activities and responsibilities	Teacher for the course " <i>Information security</i> "
Name and address of employer	SIAM, Milano
Dates	April 2008 – May 2008
Occupation or position held	Teacher
Main activities and responsibilities	Teacher for the course " <i>Security attacks</i> "
Name and address of employer	Centro di Formazione Professionale Vigorelli, Milano
Dates	January 2008 – February 2008
Occupation or position held	Teacher
Main activities and responsibilities	Teacher for the course " <i>Information security</i> "
Name and address of employer	Centro di Formazione Professionale Vigorelli, Milano
Dates	2007-2008
Occupation or position held	Teaching assistant
Main activities and responsibilities	Teaching assistant for the course " <i>Information security</i> " (" <i>Sicurezza dei calcolatori e delle reti</i> ")
Name and address of employer	Università degli Studi di Milano
Dates	January 2007 – February 2007
Occupation or position held	Teacher
Main activities and responsibilities	Teacher for the course " <i>Information security</i> "
Name and address of employer	Centro di Formazione Professionale Vigorelli, Milano
Dates	2006 – 2007
Occupation or position held	Teaching assistant
Main activities and responsibilities	Teaching assistant for the course " <i>Information security</i> " (" <i>Sicurezza dei calcolatori e delle reti</i> ")
Name and address of employer	Università degli Studi di Milano

Additional information

Driving licence(s) Driving licence of B category since October 2000.

Awards

- 13 March 2010** Together with my team, I qualified for the Capture the Flag finals of CodeGate 2010, a security convention held in Seoul, South Korea. The challenge involved about 600 different teams from all over the world, and only the first 8 teams qualified.
- 8 March 2009** Together with my team, I qualified for the Capture the Flag finals of CodeGate 2009, a security convention held in Seoul, South Korea.
- 1 June 2008** Together with my team, I qualified for the Capture the Flag finals of DEFCON 2008, the largest underground hacker convention. Only the first 7 teams (out of more than 370) qualified. We were the first Italian team that has ever been able to participate to DEFCON finals.
- 7 December 2007** My team won the International Capture the Flag contest, a distributed, wide-area security contest organized by the University of California, Santa Barbara. We classified 1st out of 35 teams from all around the world.