

josélopes

penetration testing & security consultancy

contact

+351 919 864 496

www.jmsalopes.com
sa@jmsalopes.com

 @b4stiel

languages

portuguese &
english fluency

programming

♥ Java,
C/C++/C#/Obj-C,
Python, PHP & JS

interests

professional: privacy,
anonymization, crypto,
appsec, social engineering,
red teaming, netsec,
vulnDev **personal:** music,
hardware, motorcycles,
gaming, reading

social skills

*Working in a wide range
of projects and teams, I
have hardened my
teamwork skills and
nurtured my leadership
traits. — Security Consultant*

*Independently researching
subjects unacquainted by
my colleagues, I developed
problem solving skills and
autonomy. — Junior Researcher*

experience

2014–...

MWR InfoSecurity

Security Consultant

Manchester, United Kingdom

- Delivered a multitude of security assessments covering application security, code reviewing and network security
- Worked closely with clients, establishing fruitful professional relationships that led to more projects and better value for the clients
- Led short-term projects, and delivered long-term on-site projects
- Developed internal training, namely for iOS application security assessments; and external training for iOS developers
- Supported internal processes such as recruiting, team building and office management

2012–2014

LASIGE Research Unit

Junior Researcher

Lisbon, Portugal

Researched privacy and anonymity solutions regarding:

- How to assure and protect the privacy and anonymity of the human genome
- How to assure and enforce infosec properties in smart-grids
- Anonymous and distributed communication over the Internet

Studied the design and use of forward error correction (FEC) codes in malicious environments:

- In-depth study of LT codes
 - Found an attack to break the code's resilience
- In-depth study of Raptor codes, in greater detail the RaptorQ code
 - First public implementation of IETF's RFC 6330 (the OpenRQ library)
 - Attacked the design of Raptor codes, breaking RaptorQ's resilience

projects

2013–...

OpenRQ Library

Lead developer/maintainer

<http://www.lasige.di.fc.ul.pt/openrq>

In the context of his Masters' thesis, José implemented a RaptorQ library in Java. Since then, it has evolved into an open source project. It offers a simple but powerful API, so any developer can use it on their applications. It is suitable for high-performance network applications, but its flexible API allows for an easy integration with common network communication software.

2009–...

XMakemol2 Project

Lead developer/maintainer

<https://github.com/zemasa/xmakemol2>

XMakemol is a mouse-based software for viewing atomic and other chemical systems. It reads XYZ input files and renders atoms bonds and hydrogen bonds. XMakemol2 was created from the original XMakemol software to fill in the need to manipulate/operate a XYZ file. Namely by adding/removing atoms and applying geometric transformations to atoms or molecules.

education

2011–2013	MSc in Information Security (avg. 18/20) <i>“Communication with RaptorQ Erasure Codes in Malicious Environments”</i> This thesis describes an attack to IETF’s RFC 6330 which specifies the RaptorQ erasure code. Additionally, from this work resulted the first public implementation of the RaptorQ FEC code — the <i>OpenRQ</i> library. (final grade: 19/20)	University of Lisbon, Faculty of Science
2008–2011	Licentiate in Informatics Engineering (avg. 14/20)	University of Minho

technical skills

IT skills

- Deep understanding of Windows, Linux and Mac OS X operating systems
- Strong programming skills in Windows & Unix systems
- .NET technologies
- Distributed systems technologies – namely Zookeeper, Cassandra and Hadoop
- SQL and NoSQL databases
- SOAP and RESTful web services
- Forward error correction techniques
- RPC and Java RMI
- Front-end development using AJAX
- System and network monitoring

InfoSec skills

- Web and mobile application security testing
- Network security testing
- Vast experience in code reviewing
- Deep understanding of common network protocols
- Strong knowledge of encryption algorithms and modes of operation
- Vast experience with vulnerability analysis and penetration testing tools
- IPsec and VPN technologies
- 802.1X, BT and RFID security
- Reverse engineering
- Computer forensics

certifications

2015	CRT - CREST Registered Tester http://www.crest-approved.org/professional-qualifications/registered-tester/index.html	CREST
2015	OSCP - Offensive Security Certified Professional https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/	Offensive Security

publications

Stopping Rapid Tornadoes with a Puff José Lopes, Nuno Neves <i>IEEE Security & Privacy</i> , 2014	Robustness of the RaptorQ FEC Code Under Malicious Attacks José Lopes, Nuno Neves <i>INForum</i> , 2013
---	---