

josélopes

information security specialist

contact

Somewhere in the UK

+44 nope :)

www.jmsalopes.com
sa@jmsalopes.com

 @b4stiel

languages

portuguese &
english fluency

programming

♥ Java, C/C++/C#
Python, PHP &
JavaScript

interests

professional: privacy,
anonymization, crypto,
vulnerability research,
exploit dev, netsec, social
engineering **personal:**
music, hardware,
motorcycles, gaming,
reading

social skills

*Dealing closely with clients
I've learned to understand
their requirements and
manage their expectations.*
— Junior Security Consultant

*Working in an
multi-purposed team I've
hardened my
teamwork skills and
nurtured my leadership
traits.* — Junior Researcher

*Researching a subject
unacquainted by my
colleagues, I enhanced my
problem solving skills and
autonomy.* — Masters student

experience

- 2014–... **MWR InfoSecurity** Manchester, United Kingdom
Junior Security Consultant
Mobile and web application penetration testing:
 - iOS and Android application pentesting
 - Device/build reviews
 - Source code auditing
- 2012–2014 **LASIGE Research Unit** Lisbon, Portugal
Junior Researcher
Researching privacy and anonymity in general, but namely:
 - How to assure and enforce infosec properties in a smart-grid
 - Anonymous and distributed communication over the Internet
- 2012–2013 **LASIGE Research Unit** Lisbon, Portugal
Masters student
Studied the design and use of forward error correction (FEC) codes, namely fountain codes, in malicious environments.
Detailed achievements:
 - 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)
 - Found an attack to break RaptorQ's resilience

projects

- 2015–... **Gobby** <https://gitorious.org/gobby>
Developer/maintainer
Co-developed an iOS chat application with different levels of vulnerabilities/protectations. The aim of the application is to provide training in iOS application security assessment.
- 2014–... **OpenRQ Library** <http://www.lasige.di.fc.ul.pt/openrq>
Lead developer/maintainer
In the context of my Masters' thesis I 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 his 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** <https://github.com/zemasa/xmakemol2>
Lead developer/maintainer
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.

technical skills

IT skills

- Deep understanding of Linux
- Strong programming skills in Unix systems
- Familiarity with .NET technologies
- Experience with distributed systems technologies
- Experience with SOAP and RESTful web services
- Wealth of knowledge in forward error correction techniques and erasure coding
- Experience with RPC and Java RMI
- Experience with AJAX technologies
- Experience with Nagios and systems monitoring

InfoSec skills

- Deep understanding of popular network protocols, namely TCP, UDP, IP, SNMP and HTTP
- Strong knowledge of encryption algorithms and modes of operation
- Experience with IPsec and VPN technologies
- Basic reverse engineering skills
- Basic computer forensics skills
- Familiarity with 802.1X, BT and RFID security
- Experience with scanning, vulnerability analysis and penetration testing tools.
- iOS and Android OS and application security
- Source code review and auditing

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 RatorQ 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

certifications & awards

2013	Best Paper in Security of Computer Systems and Communications Best paper in the SCSC track.	INForum Conference
2015	Offensive Security Certified Professional <i>“OSCP challenges the students to prove they have a clear practical understanding of the penetration testing process and lifecycle through an arduous 24h certification exam.”</i>	Offensive Security

publications

Stopping Rapid Tornadoes with a Puff
José Lopes, Nuno Neves
IEEE Security & Privacy, 2014

Robustness of the RaptorQ FEC Code Under Malicious Attacks
José Lopes, Nuno Neves
INForum, 2013