josélopes

information security specialist

contact

R. António Albino Machado, nº13 5ºB
Lisbon 1600-831
Portugal

+351 919 864 496

www.jmsalopes.com
sa@jmsalopes.com
@zemanelsa

languages

portuguese & english fluency

programming

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

social skills

Working in an multi-purpose and multi-cultural team, I hardened my teamwork skills and nurtured my leadership traits.

Independently researching a subject unacquainted by all my colleagues, I developed problem solving skills and autonomy.

education

2011–2012 **MSc** in Information Security (avg. 18/20) — University of Lisbon, Faculty of Science

"Communication with RaptorQ Erasure Codes in Malicious Environments"
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 *OpenRQ* library. (final grade: 19/20)

2008–2011 **Licentiate** in Informatics Engineering (avg. 14/20) — University of Minho

projects

2014–present **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 that any developer can use in his applications.

2009–present **XMakemol2 Project** — `https://github.com/zemasa/xmakemol2`

Lead developer/maintainer
In the context of an academic research project made for the Physics department of Minho University, was born an open source project/software named 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.

experience

2012–present **LASIGE Research Unit** — Lisbon, Portugal

Junior Researcher
Researching privacy and anonymity in general.
Specifically researching:

- 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

Master 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

technical skills

IT skills

- Deep understanding of Linux and Mac OS X operating systems
- Strong programming skills in Unix systems (incl. Android)
- Familiarity with .NET technologies
- Experience with distributed systems technologies such as Zookeeper, Cassandra and Hadoop
- Experience with SQL and NoSQL databases
- Experience with SOAP and RESTful web services
- Solid comprehension of forward error correction techniques and erasure coding
- Experience with RPC and Java RMI
- Experience with AJAX
- Experience with Nagios and systems monitoring
- Experience with the Apache web server and Tomcat

InfoSec skills

- Deep understanding of popular network protocols, specially TCP, UDP, IP and HTTP
- Strong knowledge of encryption algorithms and modes of operation
- Experience with IPsec and VPN technologies
- Basic reverse engineering skills
- Experience with 802.1X, Bluetooth and RFID security
- Familiarity with vulnerability analysis and penetration testing tools, namely:
  - sqlmap
  - Metasploit
  - THC-Hydra
  - Nessus
  - Nmap
  - Wireshark
  - Burp Suite
  - WebScarab
- Risk management skills
- Security incident response skills

communication skills

2013 **Oral Presentation** INForum Conference
Presented a paper I co-authored on the robustness of the RaptorQ FEC code when communication is done in a malicious environment.

2014 **Oral Presentation** Anubis Netoworks
Gave a talk on Raptor codes: their properties and why they are awesome!

interests

professional: privacy, anonymization, cryptography, incident response, vulnerability research, network security, distributed systems, forward error correction **personal:** music, computer hardware, motorcycles, gaming, reading

publications

international peer-reviewed conferences/proceedings

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

local peer-reviewed conferences/proceedings

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