Michele **Spagnuolo**

Senior Information Security Engineer @ Google Switzerland · Block chain expert

Currently in Zürich, Switzerland

(+1) 765 314 3141 | mikispag@gmail.com | miki.it | mikispag | michelespagnuolo | mikispag

Experience

Google

Zürich, Switzerland

Senior Information Security Engineer — *Jan. 2014 - ongoing*

- Co-designed parts of the W3C Content Security Policy (CSP) specification, in order to make it possible for real-world, complex web applications to mitigate XSS vulnerabilities. Implemented supporting tools and drove adoption at Google.
- Performed security code audits and design reviews for Google/Alphabet products.
- Developed technical solutions to help mitigate whole classes of security vulnerabilities.
- Fuzzed at scale, both internal products and open-source software and libraries.
- Conducted research to identify new web attack vectors.

Spreaker

(remote)

Security Consultant and System Administrator — *Jan. 2011 - Dec. 2011*

- Carried out security audits, performed penetration tests and white/black-box analysis of frontend and backend systems.
- Deployed a growing architecture on AWS, designed PostgreSQL database replication with continuous archiving.

Education

M.Sc. in Engineering of Computing Systems

Milan, Italy

Politecnico di Milano — *2011 - 2013*

- 110/110 with honors

M.Sc. in Computer Science

Chicago, IL, USA

University of Illinois at Chicago — *2011 - 2013*

- GPA 4.0

Alta Scuola Politecnica diploma with honors

Milan & Turin, Italy

Alta Scuola Politecnica — *2011 - 2013*

Projects

Rosetta Flash

Beat Same Origin Policy playing with bytes — *Jul. 2014*

- Combine DEFLATE, Flash, and JSONP in a creative way and break the web! Working with Adobe and popular web frameworks, I prevented sensitive data exfiltration and forged authenticated requests in most of the modern web.
- Presented at major international conferences, nominated for a Pwnie Award and voted in the Whitesec Top 5 vulnerabilities.

BitIodine

Extract knowledge from the Bitcoin block chain — *2013 - 2015*

- Perform complex queries on Bitcoin transactions, group addresses together by controlling entity, and much more.
- Used by malware analysts and law enforcement to investigate cases such as the Silk Road, CryptoLocker and the Mt. Gox scandal.
- Served as a base for professional frameworks such as CipherTrace, Coinalytics/Skry, and others. A rewritten version of the Clusterizer is currently in use for abuse detection by several Bitcoin businesses.

Publications

CSP is Dead, Long Live CSP: On the Insecurity of Whitelists and the Future of the Content Security Policy

2016

Proceedings of the 23rd ACM Conference on Computer and Communications Security, ACM

*L. Weichselbaum, **M. Spagnuolo**, S. Lekies, A. Janc*

BitIodine: Extracting intelligence from the Bitcoin network

2014

International Conference on Financial Cryptography and Data Security

***M. Spagnuolo**, F. Maggi, S. Zanero*

Certifications & Awards

2018 **Oxford Fintech Programme**, Saïd Business School - University of Oxford
2014 **Internet Bug Bounty**, for Rosetta Flash
2014 **Whitesec Top 5 Vulnerabilities**, for Rosetta Flash
2014 **Pwnie Awards - Nomination**, for Rosetta Flash
2011 - … **Google, Twitter, Opera, eBay, Tumblr, Nokia, Shopify, Mailchimp, Starbucks**, …security HoFs

Conferences (speaker)

Hack In The Box & ScaleUp Porto & CONFidence — *Amsterdam & Porto & Krakow*
Defense-in-depth techniques for modern web applications — *May - June 2018*

TEDx Lake Como — *Como*
What is block chain technology and how it can change the world — *November 2017*

Hack In The Box & OWASP AppSecEU & OWASP AppSec NZ — *Amsterdam & Auckland & Belfast*
So we broke all CSPs... You won't guess what happened next! — *April - May 2017*

Global Conference on Money Laundering and Digital Currencies — *Doha*
Extracting knowledge from cryptocurrencies — *January 2017*

IEEE SecDev — *Boston*
Adopting Strict Content Security Policy for XSS Protection — *November 2016*

ACM CCS — *Vienna*
CSP is Dead, Long Live CSP: On the Insecurity of Whitelists and the Future of the Content Security Policy — *October 2016*

OWASP AppSecEU & Area41 & VOXXED Days — *Rome & Zürich*
Making CSP great again! — *April - June 2016*

Hack In The Box — *Amsterdam*
CSP Oddities — *May 2016*

Hack In The Box & Tetcon & OWASP AppSecEU — *Kuala Lumpur & Saigon & Amsterdam*
Rosetta Flash — *October 2014 - May 2015*

IFCA Financial Cryptography and Data Security — *Christ Church*
BitIodine: extracting intelligence from the Bitcoin network — *March 2014*

CVEs

2016 CVE-2016-4167 (Adobe DNG SDK)

2014 CVE-2014-4671, CVE-2014-5333, CVE-2015-3042 (Adobe Flash), CVE-2014-4500 (libicu), CVE-2014-8962, CVE-2014-9028 (libFLAC), CVE-2014-8964 (PCRE), CVE-2014-8145 (sox), CVE-2014-8139, CVE-2014-8140, CVE-2015-8141 (unzip)

Skills

Information Security Deep understanding of web security, mitigations, and the Open Web Platform (OWP). Good *nix knowledge.
Coding Fluent in Java, C(++), Go, Rust, Python, JS (Closure), PHP, and scripting languages.
Languages Perfect English and Italian, basic German and Swiss German.