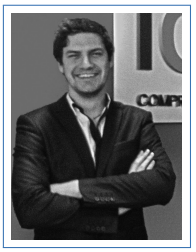
Pascal Clement

Mobile Security SME | DevSecOps
Security Researcher & Project Lead
Qualified Engineer

thireus.com
thireus
thireus
PGP DBC0BB36



Pascal Clement serves as Qualified Engineer and Mobile Security SME Consultant.

Pascal started being involved in IT Security more than 16 years ago, and has built 8 years of professional experience.

He is known for his creation of the ironha1l Tool Suite, an open-source iOS ramdisk injector tool that used a bootrom exploit (ironha1l.thireus.com) and for his publications in password cracking research (blog.thireus.com). He has a Master's Degree in Cryptography and Computer Security, as well as an Engineering Degree in Network and Telecommunications.

He began his professional career as a penetration tester and was responsible for carrying out penetration tests on mobile and network-based applications, network vulnerability assessments, infrastructure audits, security research, and more. Then he became a team leader and was responsible for a small team of security researchers and pentesters - in the context of Mobile Security research for iOS and Android applications and operating systems.

Pascal is now a DevSecOps consultant and carries on his profession as a Mobile Security SME and project lead.

Experience – 8 years of work experience in the IT Security industry

Jobs

Feb 2019 (1yr 7mos) **DevSecOps Consultant**, *HSBC*, London, `https://hsbc.co.uk/`.
Mobile Security SME & Project Lead

Responsibilities and tasks:

- Project lead for Mobile Security Tooling - DevSecOps & pipeline integration at a global scale (self-service automated and scalable mobile security tools).
- Performed MAST market analysis, engaged with vendors, trial evaluation and vendor selection, presented project to various committees of the company, organised training, established product evaluation methodology and conducted weekly follow-ups with vendors.
- Helped structure and document a process to acquire new products/services in compliance with company's internal policies and strategy. Established business requirements, project roadmap, vendor selection methodology and product scoring.
- Wrote implementation guidelines for MAST (SaaS) integration with cloud-based and on-prem tools & services (Jenkins, Kenna Security, Jira, Self-Service Portal, SSO, AD, etc.)
- Suggested internal process improvements and helped other departments with evaluating and improving their activities.
- In charge of MAST onboarding (team selection, presentation, follow-up with evaluation, feature requests and feedback), configuration & deployment, CI/CD integration, MAST training & knowledge transfer and operational support.
- Wrote documentation and detailed (in an auditable fashion) each step of the process followed, leading to a successful project. Aim: bring new joiners up to speed on similar projects, project handover and internal audit.
- Other tasks: Tool adoption strategy for mobile developers, pentesters and ITSOs; Standardisation of MAST within SDLC process; Performance Monitoring & Metrics; Compliance (HRCs, Access Control, Architecture, Solution Design Document).

May 2016 (2yrs 7mos) **Lead Security Researcher**, [redacted] , [redacted] , [redacted] .

Worked as a full-time consultant. Primary objectives: to develop and lead a team of security researchers and security testers that would constitute the elite security workforce of the company. This led to work on the most advanced cyber-security technologies and delivering cutting-edge capabilities. My role was also to build a strong relationship with clients and deliver on highly sensitive projects. I have performed both management related work and technical work. I have utilised my experience and knowledge to establish security testing processes which led to enhancing the team performances and gained the praise of upper management and clients alike on many occasions. I have discovered several hundreds of security vulnerabilities and flaws in mobile applications and have helped design secure and innovative solutions.

Worked for the following industries: Mobile Software [redacted] .

Responsibilities and tasks:

- Full-time project manager on company's key services (6 different major projects)
- Helped build the software security testing lab of the company: was the first technical employee conducting security evaluations, helped recruit a team of experts, got hardware and software for the lab, helped set up the logistics, set up security testing processes with vendors, clients and internal company departments.
- Managed a team of 6 to 8 security researchers and consultants
- Performed, managed and delivered more than 100 security assessments (iOS applications and Android applications), pentesting, code review, design review and proposal, threat modeling
- Performed iOS security research
- Attended and presented the company's products and services at various conferences
- Recruited and conducted technical interviews
- Trained security researchers on mobile security and application penetration testing techniques
- Won the company's award of Best Team of the Year 2017

Nov. 2012 (3yrs 6mos)

Started Associate

Promoted in Apr. 2013

Senior Security Consultant, *IOActive*, London, `https://ioactive.com/`.
Worked for Fortune Global 500 companies which has involved traveling up to a dozen countries. Responsible for carrying out penetration tests on mobile and network-based applications, network vulnerability assessments, infrastructure audits, ongoing security research, and more. Actively contributed to IOActive's expansion in the EMEA region by delivering high quality security services and maintaining lasting business relationships. Performed a variety of management related work such as holding job interviews, writing reports and statements of work, scoping projects and actively contributing to project meetings. Representing the elite IOActive image was also an important aspect of my job.

Promoted Senior in Sep. 2015

Worked for the following industries: Banking, Mobile Software, Enterprise Software, Business Services, Retail Sales, Electronics Manufacturing & Equipment, Finance, Insurance, Health, Government.

Responsibilities and tasks:

- Technical lead responsibilities
- Wrote security assessment proposals for potential clients
- Project scoping and client report writing
- Penetration testing of corporate software and back-end solutions such as payment processing or corporate data processing
- Infrastructure penetration testing and security audit in sensitive environments such as datacentres or corporate premises
- Cloud-based applications penetration testing
- Corporate wireless penetration testing
- Penetration testing and code review on mobile applications (iOS and Android), most of which were banking applications
- Penetration testing on Web applications of various kinds
- Security research on password cracking and wireless security
- Recruiting and conducting technical interviews
- Attending and presenting the company's products and services at various conferences

Business

April 2016 (2yrs 8mos)

Entrepreneur, [redacted] , [redacted] .

Internships

2012 (5 months)

Security Consultant, *Thales Communications & Security*, Vélizy-Villacoublay (France), `https://www.thalesgroup.com/en`.

- R&D iOS and Android Security
- Penetration Testing (Web/Network/Apps)
- Reverse engineering

2011 (3 months)

Technology Scouting, *Oberthur Technologies' Card Systems (now IDEMIA)*, Pessac (France), `https://www.idemia.com/`.

- TrustZone (ARM) Research
- Android KeyLogger

Education – 6 years postgraduate, Engineering & Master degrees

2011–2012 Graduated
Master's Degree with distinctions, Cryptology & Computer Security, *University of Bordeaux 1*, `https://www.u-bordeaux.com`, Double Degree.
Software Security, Network Security, Smart Card, Operating System, Cryptanalysis.

2009–2012 Graduated
Engineer's Degree with distinctions, Network & Telecommunications, *ENSEIRB-MATMECA*, `https://www.bordeaux-inp.fr/en`.
Telecommunications Engineering Degree – Telecommunications, engineering science, computer science, electronics, digital simulation, embedded systems, networks, network security. Obtained English Level B2 certificate. TOEIC (Score 820) + IELTS (Score 6.5)

2006–2009 CCP
Classe Préparatoire aux Grandes Écoles, *Lycée Thiers and Lycée Frédéric Mistral*, `https://ccp.scei-concours.fr/`.
Successful candidate to integrate the ENSEIRB-MATMECA engineering school following the CCP (Concours Communs Polytechniques) competition.

2006 Graduated
High School Degree with distinctions, *Major in Science*.
Mathematics and Physics major.

Skills

Computing

Tools	Wireshark, Nmap, Nessus, Burp Suite Pro, Metasploit, Aircrack-NG, Scapy, GDB. BackTrack, Kali. Matlab, Maple, Sage-Math. IDA, Hopper Disassembler, Frida, Cycript.
OOP	C++, Java, JavaCard, Objective C, Swift.
Imperative languages	C, Rust, Pascal, Basic, Perl, Python.
Network	TCP/IP, Ethernet, WiFi, 3G, IpTables, IPsec, SSL/TLS, Sniffing, Scanning, (D)DoS, MITM.
Web	XHTML/CSS, PHP, Javascript, MySQL.
Other	Good knowledge of system architecture & network security. GNU/Linux OS Master. Familiar with JIRA, Confluence, GitLab, Word, Excel, etc.

Achievements

2014-2015 **PeerParser**, *Private Research*.

Wrote a Bitcoin/Peercoin blockchain parser in C from scratch (which led to understanding the Bitcoin block scheme and Bitcoin script language). This tool served a private purpose to deanonymise and map all blockchain public addresses and to have a money flow map (with the use of blockchain data files only). Using Gephi to map all nodes and group nodes. Using web crawlers to find user's public keys on various Forums and Websites as well as other investigation techniques to deanonymise coin exchanges and coin miners. A partial screenshot of the results can be found at: [redacted]. Note that since, several Bitcoin and Peercoin protocol upgrades broke the tool. The source code is unmaintained and currently private.

2014-2015 [redacted], *Private Research*.

[redacted]

ECDSA bruteforcer in C. Source code and results are private. [redacted]

2012 **ironha1l**, `https://ironha1l.thireus.com/`.

iOS forensics ramdisk injector tool in C, using libusb. Compatible with MacOS, Linux, FreeBSD, Android. GUI Java Android.

Since 2012 **Thireus Cydia Repository**, `https://repo.thireus.com/`.

A Cydia repository that I maintain which contains various jailbreak-related tools, some of which help security penetration testers for iOS security assessments.

2011 **1st Prize Thales**, *Contest ENSEIRB-MATMECA*, Telecommunication Section.

Project manager and iOS developer. Development of a VoIP application with mobility management over 3G/WiFi for iPhone and Android OS.

2011 **Network and Web Security Lecture**, *ENSEIRB-MATMECA*.

Three hours training at ENSEIRB-MATMECA, with 60 future engineer students to heighten awareness about network and Web security.

Since 2011 **Blog**, `https://blog.thireus.com/`.

IT Security related articles.

2009–2011 **Blog**.

Applications, hacks, drivers. Research and study notes.

2005–2011 **DareYourMind**.

CTF website with various security challenges.

Languages

French	Mother tongue
English	Fluent — *Level B2 certificate. TOEIC (Score 820) + IELTS (Score 6.5)*

Hobbies and Interests

Conferences

2012 **Hack in Paris**, Paris, Listener.

2012, 2013, 2016 **Hack In The Box**, Amsterdam, Listener.

2013 **BlackHat**, Las Vegas, Listener.

2013 **DEFCON**, Las Vegas, Listener.

2016 **BlackHat Europe**, London, Listener.

2017 **REcon**, Brussels, Listener.

2017 **MWC17**, Barcelona, Presenter.

2018 **44Con**, London, Listener.

2019 **DevSecOps - London Gathering**, London, Listener.

Trainings

2010 **IT Security courses at Copenhagen University College of Engineering**, Denmark, by Ihk Copenhagen University College Of Engineering.
Summer school. 20 days of IT Security courses.

2016 **Mobile Application Hackers Handbook Training**, Amsterdam, by Dominic Chell.
Learned new tricks and techniques to hack and secure mobile applications on the iOS and Android platforms.

2016 **iOS Kernel Exploitation Training**, Berlin, by Stefan Esser.
Covered the techniques and vulnerabilities to create an iOS jailbreak.

2016 **Software Defined Radio**, London, Michael Ossmann.
Introduction to digital signal processing, software radio, and tools.

2017 **MacOS Sierra and iOS 10 Kernel Internals for Security Researchers**, Brussels, By Stefan Esser.
Covered the Kernel securities in both iOS and MacOS and how to bypass or utilise these features.

2017 **RIVIYERA FPGA and VHDL**, by SciEngines.
Trained to use and program a RIVIYERA FPGA for password cracking.

2018 **The ARM IoT Exploit Laboratory**, London, by Saumil Shah.
The class covered everything from an introduction to ARM assembly all the way to Return Oriented Programming (ROP) on ARM architectures.

I enjoy...

Keywords: Hackintosh, Jailbreak, Password Cracking, Bitcoin