Matthieu Daumas | Junior Engineer

+33 (623) 316 264 • matthieu@daumas.me • plcp

Looking for a full-time job in Paris within IT Security & friends

Work Experience

Researcher – master thesis on The Onion Router — **April - (Sep. 2018)**
Security & Privacy Engineering Team, EPFL, tech. used: python, C, chutney — *Lausanne – Switzerland*
Build a lightweight client to connect even more things to TOR, enjoying cryptography & security.

Developer within IT Security Testing — **March - Sep. 2017**
Airbus, Operational IT Security Team (EVYYS), tech. used: python, fuzz testing methodology — *Toulouse – France*
Develop on the internal fuzzing framework & participate in various other activities of the team.

SysAdmin within a small startup — **June - Sep. 2016**
Almena France, tech. used: bash & zsh, c++17, Let's Encrypt, SQL, apache2 — *Muret – France*
Setup the startup infrastructure, various cloud-like self-hosted tools and work on a homebrewed crawler.

Intern, BEAMS Laboratory — **June - Aug. 2015**
ULB University, tech. used: python, c++14, logic analyzers, sigrok-cli — *Brussels – Belgium*
Create a set of tools to instrument analysis of discrete datagrams for practical courses.

Intern, IRIT Laboratory — **April - June 2014**
Paul Sabatier University, tech. used: java, HTML5, CSS3, javascript — *Toulouse – France*
Assist in the organisation of the GDN2014 conference and develop a group-decision support system.

Independent Activities

Attending various conferences & symposiums, IT Security Community — **2014 -**
Such as CCC (Germany), SSTIC, NdH, St'Hack, THSF, THC (France) & others
Keeping myself active within communities, mostly attending and occasionally giving talks & rumps.

Chairman, Toulouse Hacking Convention, Volunteering — **2016 - 2018**
TISA is an IT Security Association, main organizer, tech. used: mailman2 & lot of logistics
The THC brings together IT security researchers and enthusiasts around 24h of talks & CTF.

Member of the CTF team "Pony7", Competitions — **2014 - 2017**
Capture the Flag, pony7 on CTFTime, tech. used: various (google-fu, hands-on tools, one-liners…)
Most active during 2014 & 2015, at best top 50 on international & top 5 on national events.

Treasurer, net7 – "Hackerspace", Volunteering — **2015 - 2016**
Local computer club, learning & teaching, tech. used: various (F/LOSS, GnuPG, git, LDAP…)
Learning everything from scratch, starting with archlinux & maintaining a dozen of servers.

Education

Master, Security of Information Systems and Networks — **2016 - 2017**
RT-SSIR (within TLS-SEC), incl. x86 protected mode, cryptography, kernels & hypervisors — *Toulouse – France*

Engineering degree, studying computers – TLS-SEC, IT Security specialization — **2014 - 2017**
INP-ENSEEIHT, incl. hardware architectures, compilation, parallel & real time programming — *Toulouse – France*

Preparatory course, polytechnic curriculum — **2012 - 2014**
CPPT, including linear algebra, organic chemistry, electronics and biology — *Toulouse – France*

Master, Performance in Software, Media and Scientific computing – will graduate in 2018 — **2017 - (2018)**
PSMSC (Univ. Toulouse & n7), incl. theory of distributed systems, thesis on The Onion Router — *Toulouse – France*
Taking some time to explore & contribute to nice things, doing bits of research before going to industry.

Foreign Languages

English: **C1 Level, TOEIC 980** - Proficient speaker
French: **Native** - Fluent speaker
German: Learning
Japanese, Polish: Elementary

Good writing skills: proficient in French and English – good experience writing clean documentation, reports and mails.

Skills

Main Areas: IT Security, cryptography, development, code audit, F/LOSS, vulnerability research,, distributed systems...
Daily Tools: man, tmux, vim, git, ssh, zsh, mlterm, make, clang, gcc, mpv, various others (find, pgrep, ss, xxd, tput)...
Fluent Skills: python, c++17, bash, c, GNU/Linux (archlinux, debian & systemd), searching the internet (google-fu)...
Working Skills: sysadmin, x86 inner workings, gdb-peda, z3, "machine learning", qemu, sql, php, django, docker, dhcp...
Auxiliary Skills: reverse & IDA, wireshark, js/html5/css3, arduino/teensy, "blockchains", LISP Scheme, android, java...
Office Skills: lualatex, libreoffice, crafting nice slides & various documents, reading & writing mails, basic human skills...

Miscellaneous

Full clean driver's license.

Enjoy having a beer with coworkers, idling on IRC together and actively participating into shared activities, especially if there is some form of IT Security-related fluff around – note that I also enjoy more "common" activities as well.

Recreative Programming

One of my main hobbies is to hack & program enjoyable pieces of code. Here are several excerpts, cherry-picked for their diversity in order to give a good overview of what I am doing when I get home – i.e. outside of my "day job".

qbinstr – play with *Dynamorio*'s binary instrumentation capabilities
https://github.com/plcp/.relics/blob/master/16/qbinstr
As an exercise, start with clean calls, then build a probe using local thread storage, spilled registers & proper instrumentation.

binfmt_misc – some trivia involving miscellaneous binary formats
https://github.com/plcp/.relics/blob/master/17/binfmt_misc
The poor man's rootkit, turn any suid binary into privilege escalation if $/proc/sys/fs/binfmt\_misc/register$ is writeable.

clenche – a meta-template library to build flat control flows
https://github.com/plcp/clenche
Flatten callgraphs using *std* :: *variant* and dirty templates, build fast traits-oriented discrete simulations, mostly for fun & profit.

bashful – fiddle with *bash* internals and its loadable built-ins
https://github.com/plcp/bashful
Expose internal *bash* variable properties using *ptrace* (via *gdb*), then abuse loadable build-ins to craft $\$RANDOM$-like variables.

tim – randomly search for a worst-case of *Timsort*, aka python's sort
https://github.com/plcp/.relics/blob/master/18/tim
Given a list, search for a worst-case permutation against *Timsort*, use confidence intervals to spot noisy time deltas below $1ms$.

hayfield – challenge where one must break an exotic cipher (build for thc18 CTF)
https://github.com/plcp/.relics/tree/master/ctf/thc18/crypto-hayfield
Given an exotic cipher that hides a twist, study its properties, exploit its flaws and decrypts few ciphers without any key.

moche – challenge where one must hijack a mosh-like secure shell (build for thc17 CTF)
https://github.com/plcp/.relics/tree/master/ctf/thc17/crypto-moche
Given a mosh-like client and server, exploit a MAC-then-encrypt flaw to build an oracle, fully decrypt and replay keystrokes.

sandkox – a sandboxing library inspired by good ol' suid sandboxes (build for thc18 CTF)
https://github.com/plcp/sandkox
Challenge where a website runs any binary as root, but first checks linkage via *ldd* and overrides *.init* to "sandbox" the execution.

Whenever I have the occasion – at work or during my daily life – I also like solving and writing exercises & CTF challenges, teaching what I can and learning from others, just as other forms of shared activities that promotes knowledge transmission.

Leisures

Have played the Alto Saxophone for 10 years, enjoy cooking, running around with sandbags, occasional woodworking, urban exploration & various locksmitheries. Have also most of my friends in Paris, thus room to be happy & productive.