

# 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

<b>Researcher – master thesis on The Onion Router</b> <i>Security &amp; Privacy Engineering Team, EPFL, tech. used: python, C, C++17, chutney</i> Build a lightweight client to connect even more things to TOR, enjoying cryptography & security.	<b>April - (Sep. 2018)</b> <i>Lausanne – Switzerland</i>
<b>Developer within IT Security Testing</b> <i>Airbus, Operational IT Security Team (EVYYS), tech. used: python, fuzz testing methodology</i> Develop on the internal fuzzing framework & participate in various other activities of the team.	<b>March - Sep. 2017</b> <i>Toulouse – France</i>
<b>SysAdmin within a small startup</b> <i>Almena France, tech. used: bash &amp; zsh, c++17, Let's Encrypt, SQL, apache2</i> Setup the startup infrastructure, various cloud-like self-hosted tools and work on a homebrewed crawler.	<b>June - Sep. 2016</b> <i>Muret – France</i>
<b>Intern, BEAMS Laboratory</b> <i>ULB University, tech. used: python, c++14, logic analyzers, sigrok-cli</i> Create a set of tools to instrument analysis of discrete datagrams for practical courses.	<b>June - Aug. 2015</b> <i>Brussels – Belgium</i>
<b>Intern, IRIT Laboratory</b> <i>Paul Sabatier University, tech. used: java, HTML5, CSS3, javascript</i> Assist in the organisation of the GDN2014 conference and develop a group-decision support system.	<b>April - June 2014</b> <i>Toulouse – France</i>

## Independent Activities

<b>Attending various conferences &amp; symposiums, IT Security Community</b> <i>Such as CCC (Germany), SSTIC, NdH, St'Hack, THSF, THC (France) &amp; others</i> Keeping myself active within communities, mostly attending and occasionally giving talks & rumps.	<b>2014 -</b>
<b>Chairman, Toulouse Hacking Convention, Volunteering</b> <i>TISA is an IT Security Association, main organizer, tech. used: mailman2 &amp; lot of logistics</i> The THC brings together IT security researchers and enthusiasts around 24h of talks & CTF.	<b>2016 - 2018</b>
<b>Member of the CTF team "Pony7", Competitions</b> <i>Capture the Flag, pony7 on CTFTime, tech. used: various (google-fu, hands-on tools, one-liners...)</i> Most active during 2014 & 2015, at best top 50 on international & top 5 on national events.	<b>2014 - 2017</b>
<b>Treasurer, net7 – "Hackerspace", Volunteering</b> <i>Local computer club, learning &amp; teaching, tech. used: various (F/LOSS, GnuPG, git, LDAP...)</i> Learning everything from scratch, starting with archlinux & maintaining a dozen of servers.	<b>2015 - 2016</b>

## Education

<b>Master, Security of Information Systems and Networks</b> <i>RT-SSIR (within TLS-SEC), incl. x86 protected mode, cryptography, kernels &amp; hypervisors</i>	<b>2016 - 2017</b> <i>Toulouse – France</i>
<b>Engineering degree, studying computers – TLS-SEC, IT Security specialization</b> <i>INP-ENSEEIH, incl. hardware architectures, compilation, parallel &amp; real time programming</i>	<b>2014 - 2017</b> <i>Toulouse – France</i>
<b>Preparatory course, polytechnic curriculum</b> <i>CPPT, including linear algebra, organic chemistry, electronics and biology</i>	<b>2012 - 2014</b> <i>Toulouse – France</i>
<b>Master, Performance in Software, Media and Scientific computing – will graduate in 2018</b> <i>PSMSC (Univ. Toulouse &amp; n7), incl. theory of distributed systems, thesis on The Onion Router</i> Taking some time to explore & contribute to nice things, doing bits of research before going to industry.	<b>2017 - (2018)</b> <i>Toulouse – France</i>

## Foreign Languages

<b>English:</b> C1 Level, TOIEC 980 - Proficient speaker	<b>German:</b> Learning
<b>French:</b> Native - Fluent speaker	<b>Japanese, Polish:</b> 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 assembly, gdb-peda, z3, IDA, qemu, sql, php, django, docker, nginx, wireshark, dhcp, dns...  
**Auxiliary Skills:** (some) LISP scheme, arduino/teensy, js/html5/css3, android, java, "blockchains", "machine learning"...  
**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.

**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.

**profile.sh – a bourne-again shell profiler**

<https://github.com/plcp/.relics/tree/master/18/profile.sh>

Use trickery and *PS4* expansion to profile bourne-again shell scripts, display a colorful summary – helping you identifying bottlenecks.

**binfmt\_misc – some trivia involving miscellaneous binary formats**

[https://github.com/plcp/.relics/blob/master/17/binfmt\\_misc](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.

**subcut.py – slicing conference audio with *librosa* for further processing**

<https://github.com/plcp/.relics/blob/master/17/subcut.py>

Handle sound as floating point series, detect silence as off-variance series, then cut conference audio into slices for further processing.

**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.

**sandbox – a sandboxing library inspired by good ol' suid sandboxes (build for thc18 CTF)**

<https://github.com/plcp/sandbox>

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.