Programming cryptoparties in Libraries

Damien Belveze

Programming cryptoparties in Libraries : How Librarians can contribute to Students and Citizens empowerment against tracking and mass-surveillance

« Librarians are badass » (Edward Snowden)

IFLA statement on privacy and its role to librarians commitment

For french students, privacy is usually not included in the curriculum excepts in the margins, as a part of an optional course that some student attend to make their digital skills certified (C2i)[1]. A few years ago, I noticed among students of my former engineering school a real lack of knowledge on privacy and an insufficient perception of its importance, particularly in the building of mobile application, though these students are often asked to design apps that are supposed to collect users data.

At the university of Rennes1, I am in charge of training sessions for students from undergraduate level to PhD. I usually teach them how to find valid and relevant scientific information, how to manage bibliographic references, how to become an open scientist in the sense of Open Access. My colleagues also show them how to manage, store and share research data.

Encrytion can sometimes be related to some of these topics. PhD students, for instance, who collect data on sensitive matters like drug side effects should sometimes consider encrypting these data in order to avoid theft or espionage attempts as they sometimes occur inside or outside the lab[2].

Apart from my duty at the university, I am also member of a local association who promotes the use of Open Source software and supports the cause of privacy. As much as possible, I try to make both activities meet in a professional context : cryptoparty is a way of making this possible. Chloe Lailic, my former colleague of INSA Rennes library and I share the same goal: spread cryptoparties in as many french libraries as possible including public libraries as well as academic ones. We decided to start from our own institution and have organized each year since 2015 an annual event about privacy. We have been feeling more legitimate doing this since IFLA released its statement on privacy on August 2015[3]. This declaration brought us attention from our colleagues and support from our library administration boards.

Definition of cryptoparties

I will not try to define again what a cryptoparty can be or can not be. I will only refer to Asher Wolf's definition of it in her very inspiring book[4] published online and anonymously accessible via Tor. A cryptoparty in an event designed to let every citizen learn basic encryption tools and understand how they operate. This event must be commercially non aligned. Organizers should not get support from any for-profit corporation. A cryptoparty must also be politically neutral, even if policy making in the field of privacy can be questioned. Cryptoparties are open to everybody. Security experts are welcome as trainers, or as attendees provided they do not take precedence over invited speakers and trainers. We would like this event to be as inclusive as possible. Since 2015, we have been trying to escape two major difficulties: on one hand, we do not want to fuel paranoia among our attendees, on the other side, we try to raise the level of awareness of the younger who often do not pay enough attention to their use of social media. Moreover, when it comes to our ears, we do not let the "nothing to hide" argument uninterrogated. After having attended one of our cryptoparties, people should consider privacy and digital rights as a part of their fundamental rights, if this was not the case before.

Cryptoparties in libraries : New opportunities

In the first place, cryptoparties were designed for hackerspaces. But recent studies[5] have confirmed the general observation that women usually will hardly engage in hackerspaces or makerspaces. Such barriers also seem to exist to seniors involvement in those places. On the contrary, libraries are supposed to give an opportunity to widen the audience. They provide new chances to reach people who are not yet convinced, and to mainstream the use of the most basic (which does not mean the less protecting) encryption tools in order to empower civil society. This is our intention, but the task remains quite difficult to achieve. I will discuss it later.

Cryptoparties in libraries : Auditing the library system on the privacy aspect

In France, patrons privacy benefits from a rather protecting legal framework. As any set of personal data, loan records must be treated in compliance with the Commission for Digital Rights (CNIL) provisions and have to be deleted after a short period of time.
Since this task has always been automated because it is easier to fulfill the law that way, in case of election of a far-right wing extremist at the presidency, French librarians would not be suddenly confronted to the vast and sensitive task of a complete patrons records deletion, as were American Librarians between the Trump election and his inauguration[6].

This, added maybe to the lack of interest of french Intel Agencies for these records (in comparison to the Patriot Act) can explain why French librarians have only showed recent concerns on this issue and why the professional literature on this topic is quite rare in this country.

Nevertheless, a brief survey of the question makes it clear that the privacy of french users is not less targeted than the privacy of Americans, if not as much by governemental activities, then by commercial ones.
As a consequence, colleagues might be too confident with their protocols on that regard. They sometimes fail for lack of scrutiny on the choice of their password policies (especially for passwords that give limited access to wifi) : the user, for instance, is too often given a weak password that contains his name. The other issue, the amount of user data that will be stored or sent to third-parties is seldom adressed, whereas these last years some very interesting surveys have been published on that topic[7] and important leakage of users data by retailers or digital rights managers have been disclosed[8]. Indeed, when a user borrows an e-book, his login may be sent up to four agents : the provider of the discovery tool on which he typed the request terms, Amazon (even if Amazon does not retail the borrowed book, as soon as the discovery tool uses Amazon API to link with the retailer's book covers, the request is sent to the curved arrow company servers). The library IT provider will also keep it as a GET request log, and finally as we mentioned it, the provider of the Digital Rights Manager that makes the loan possible for the period defined by the publisher will get its own copy of the accessed book title linked to its borrower profile. This is of great concern for librarians who feel involved as well for the development of digital reading among the public as for the protection of people privacy.

We could also mention library websites that are not yet accessible in a secure mode (SSL) or track visitors with tools hosted by third-parties like Google Analytics.

To a certain extent, a crytoparty also gives the opportunity to audit the library system on a privacy perspective.

Cryptoparties in french libraries : challenges and constraints

Cryptoparties, as we said, were designed by and for communities who share at least a sharp interest to DIY[1] meetings as well as a sense of self-organization. On the contrary a library works on

1Do It Yourself

a rather hierarchical basis and often do not even controls the IT network it uses to fulfill its missions. The library usually depends on an IT staff who does not work on the premises. This staff is accountable for the whole network security wether it be the network of an university or of the whole City administration). To this regard, a librarian who wants to organize a cryptoparty within the library walls will have to spend some time to convince not only the library administration board but also the administrator of the public or academic network.
Bringing a Tor exit relay in a library for example seems far beyond what can be done in a french library today while some libraries in the United States -and first of them Kilton Library (New Hampshire)[9] managed to do so in 2015. At the INSA Rennes Library, we persuaded our system administrator to install Tor browsers on library public computers, at least for 8 eight months, before this software had to be removed from those computers to comply an ANSSI (national agency for informatic systems security) recommandation[10]. This recommandation did not refer to the state of emergency but on the alleged harm Tor Traffic would possibly cause to servers.

Nevertheless, good compromises have been found with other system administrators, especially in academic environment, allowing librarians and cryptoparty organizers temporarily use the local network to run Tor browsers wether in its standalone version or via a Tails[2] distribution key in both cases from attendees devices, so that they could learn by doing about these softwares.

These compromises are sometimes harder to find in public libraries, where everything that looks like an anonymous connection, even for a short period of time, is made impossible.
Some cryptoparties in french public libraries had to be canceled after having been announced for lack of access to the library network. In order to help cryptoparty organizers and librarians to deal with this issue, we launched in 2015 a public mailing list[11] hosted by Renater, which provides Internet to all universities and high schools. There, arguments, cases, technical and pedagogical information are shared and discussed. This list aims to spread cryptoparties in libraries across the country and works as a digital agora where hackers, advocates for privacy, teachers and librarians meet and contribute together to a better understanding of the benefit of encryption tools for the society. Journalists also play a major role in that matter. This is why, in a city like Rennes, along with developers and engineers, we have made several cryptoparties in the office of a local journalists association. Focusing on journalist practices can be rewarding for the cause of encryption. Once they were trained to these tools, Journalists will not only give better protection to their sources, but they will be more likely to feed a counter-speech to inaccurate and sometimes fancied articles on darknet and other web Mariana trenches as related to terrorist threats published quite every day in the press[12].

Cryptoparties in Libraries : How does it work ? What does it look like ?

A cryptoparty may be designed in many ways. A single meeting between two persons, one learning from the other, can already be considered as a cryptoparty according to Asher Wolf. As we, Chloé Lailic and I, tried first to adapt cryptoparty to Academia, we designed our two first events with an introductory speech. In the first edition of our cryptoparty, this speech was held by a security expert and former PhD student of a neighbour engineering school. The second edition introductory conference was much more relevant to the values and concerns we wanted to share : Okhin, hacker and employee from the NGO “La Quadrature du Net” gave a very engaging speech, and highlighted how encryption protects minorities, and by doing so, safeguards democracy. For the third edition, a hybrid speech between conference and performance, much used in France by community educators and known as “conférence gesticulée” was given by the hacker Lunar. This performance usually includes biographic details about the speaker. Lunar, who has been active on the internet since his childhood, embodied perfectly this kind of talentuous activist who first saw the

---

2 The Amnesic Incognito Live System : Linux distribution loaded in a USB stick and designed by Guardian Project to preserve anonimity of its user on every computer he uses

internet as a great opportunity for social cooperation, and then, as it grew year after year to be the internet we know today, as well as a threat for our fundamental rights.

Right after the conference or within the same week, libraries may host simultaneous workshops for half a day or a day long. The programme can include an install party with the help of the local association who supports GNU and Open Source software. Linked to a cryptoparty, an Install Party aims at helping people to better understand the important role played by Open Source operating systems, especially Linux distributions, which minimize the leakage of personal data and improve personal digital security.

In our last edition of this event, two Libraries (Rennes 1 and INSA Rennes) hosted up to 9 workshops at the same time. This encompassed presentations and demos of Privacy apps for mobile phones, free and open source designed to replace Google or Microsoft Office tools, PGP messaging, introduction to Tor and Tails, Breaking and strenghening passwords methods, Radio-Frequency attacks, privacy chatroom, philosophical and political workshop on digital intimacy, self-censorship and civil rights.

How to reach more people from more various backgrounds

Even if more students have attended our cryptoparties than we one could have expected if they had taken place in hackerspaces, we have not yet achieved our goal to reach the widest range of citizens, to begin with ones who were targeted in our communication plan e.g non techy people, librarians, seniors and women. Data collection for registration is usually reduced to a minimum for obvious reasons, but the under-representation of these categories have been several times observed, while young (from 30 to 40 years old) white male people with already strong digital skills were obviously over-represented. We are not sure either that militants and activists consider our cryptoparties as relevant to their situation although their need for protection against intel or police's scrutiny is beyond any doubt under the emergency state. The same bias could be assumed here as the one which Anne-Marie Oostveen noticed about PGP (Pretty Good Privacy) protocol[13] : such encryption protocol will be more often used by people who are interested in technologies than by people whose privacy disclosure have more negative effects.

It is also difficult to make people come who claim they have nothing to hide. Most of the time we deal with people who know the price of privacy and feel the urgency to stand for the right of privacy in a post-Snowden era. A parallel could be drawn with tools designed to hunt fake news : only people who have already developped a keen interest in assessing the reliability of information shared by social media will consent to use them while these tools would a have a far greater impact on users who underestimate the spreading of fabricated information.

What can be next ?

A cryptoparty is open to everybody, but unfortunately not anybody goes there. Organize a cryptoparty in a library, you will see people trying to find their way to sessions venue or conference room and asking for help, because it is the fist time they enter your library. Will you find other librarians or some of your patrons heading to the same rooms? Nobody can garantee it. Programming seven or eight training sessions in the course of a year would have maybe a greater impact than organizing one single annual event. This programme could raise the library’s concern for patrons privacy to the level of its day-to-day and long terms actions. We could also focus more on certain categories of population, by including in the list of workshops for instance training for women on how to escape and block digital harassment. We could also meet activists on public spaces next to these street libraries some librarians installed during the so-called “Nuit Debout” social movement that took place in France last spring.

Involve people, let them know that librarians can do something for their privacy is a long labour and even within our walls, in the very heart of our devices, there still is a great deal of work in the

pipeline.

Damien Belvèze, Rightscon proceeding, 2016/03/31

References :

[1] Ministère de l'Enseignement Supérieur et de la Recherche, « Guide sur la sécurité des données personnelles (ed. 2010) | C2i », *Ressources pour le C2i*, 2010. [En ligne]. Disponible sur: https://c2i.enseignementsup-recherche.gouv.fr/ressource/guide-sur-la-securite-des-donnees-personnelles-ed-2010. [Consulté le: 06-avr-2017].

[2] « Recommandations pour la protection des données et le chiffrement ». CNRS/FSD, 2008.

[3] International Federaction of Library Associations, « IFLA Publishes a Statement on Privacy in the Library Environment », *IFLA*, 20-août-2015. [En ligne]. Disponible sur: https://www.ifla.org/node/9803. [Consulté le: 06-avr-2017].

[4] A. Wolf, « Cryptoparty Handbook », 2012. [En ligne]. Disponible sur: https://www.cryptoparty.in/learn/handbook. [Consulté le: 06-avr-2017].

[5] J. Lewis, « Barriers to women's involvement in hackspaces and makerspaces | », sept-2015. [En ligne]. Disponible sur: http://access-space.org/klick-2-barriers-to-womens-involvement-in-hackspaces-and-makerspaces/. [Consulté le: 06-avr-2017].

[6] S. Thielman, « Libraries promise to destroy user data to avoid threat of government surveillance », *The Guardian*, 30-nov-2016.

[7] C. Lynch, « The rise of reading analytics and the emerging calculus of reader privacy in the digital world », *First Monday*, vol. 22, nº 4, avr. 2017.

[8] N. Gary, « Adobe avoue espionner ses utilisateurs : une affaire rootkit en vue », *Actualitté*, 08-oct-2014.

[9] Y. Eudes, « Libertés numériques : aux Etats-Unis, les bibliothécaires font de la résistance », *Le Monde.fr*, 07-mars-2016.

[10] « Bulletin d'actualité CERTFR-2016-ACT-009 ». 29-févr-2016.

[11] « cryptobib - Sensibiliser les usagers des bibliothèques à la protection de leur vie privée et veiller à la confidentialité des données personnelles dans les systèmes d'information documentaires - arc ». [En ligne]. Disponible sur: https://groupes.renater.fr/sympa/arc/cryptobib. [Consulté le: 06-avr-2017].

[12] Bluetouff, « @Marianne2fr, Tor, le poids des mots, le choc des pixels : plongée dans le journalisme à la con | », *Reflets.info*, 11-mai-2013.

[13] A. Oostveen, « PGP/GPG Survey Results », *Anne-Marie Oostveen*, 29-sept-2016. [En ligne]. Disponible sur: https://blogs.oii.ox.ac.uk/oostveen/2016/09/29/pgpgpg-survey-results/. [Consulté le: 21-janv-2017].