Journée de la Sécurité Informatique en Normandie ; sécurité(s) et liberté(s)

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 30 novembre 2018. Dernière mise à jour le 27 décembre 2018

https://www.bortzmeyer.org/jsecin-2018.html

Des conférences sur la sécurité informatique, il y en a trois par jour en France, parfois dans la même ville. On peut passer sa vie professionnelle à aller à de telles conférences. Mais elles sont plus ou moins intéressantes. La Journée de la Sécurité Informatique en Normandie <http://jsecin.insa-rouen.fr/> fait partie de celles qui sont intéressantes. J'y ai présenté une réflexion en cours sur le débat « sécurité et liberté » dans le contexte de la sécurité informatique.

La JSecIN <http://jsecin.insa-rouen.fr/> s'est tenue à Rouen le 29 novembre 2018, dans les locaux banlieusards de l'Université Rouen-Normandie (et co-organisée avec l'INSA). Le public était donc très majoritairement composé d'étudiants en informatique (dont une très faible proportion de femmes), avec quelques professionnels. Les exposés étaient tous intéressants. On a commencé avec Renaud Echard (ANSSI). Il a rappelé des bases en sécurité informatique, comme le fait qu'il faut utiliser le chiffrement systématiquement. Des bases vraiment basiques, certes, mais pas encore appliquées partout. L'orateur estime d'ailleurs que « 80 % des attaques seraient évitées avec l'application de quelques mesures simples d'hygiène numérique ». (La formation est donc un point-clé.)

On a vu bien sûr la classique (mais toujours vraie et utile) photo « le triptyque de la sécurité » : une porte blindée, avec un vérin de fermeture (la technique), un mot « cette porte doit rester fermée » (l'organisation) et une canette de Coca écrasée qui la tient ouverte (l'humain). Autre remarque pertinente : « Il vaut mieux une procédure simple qu'une procédure de 40 pages que personne ne lit. » L'orateur a également insisté sur l'importance de techniques simples : si le type qui fait la promotion d'une solution de sécurité ne peut pas vous l'expliquer simplement, c'est que le système est trop compliqué pour être auditable, et est donc peu sûr.

On a eu droit aussi à un peu de bureaucratie de la sécurité comme ce bon résumé de la différence entre OIV (Opérateur d'Importance Vitale, par exemple en Normandie, celui de l'énergie qui est au bord de la mer) et OSE (Opérateur de Service Essentiel) : « Un OSE est un OIV-light ». Et à la difficulté de l'attribution des cyberattaques : « Si vous me demandez d'où vient l'attaque, je vous dirais de me poser la question en privé. Et, là, je vous répondrais que je ne peux pas le dire. » Et une anecdote pour

finir : dans les aéroports et gares français, de nombreux engins portables sont volés chaque jour. L'ANSSI recommande officiellement les autocollants sur le portable (pour rendre plus difficile les substitutions discrètes.)

Puis Solenn Brunet (CNIL) a présenté le paysage de la protection des données personnelles à l'heure du RGPD. Un exposé très riche (peut-être trop) car le sujet est complexe et nécessite de nombreuses explications. L'oratrice rappelle que le RGPD reprend l'essentiel de la loi Informatique & Libertés de 1978. Les gens qui se sont angoissés de certaines obligations du RGPD (minimisation des données, par exemple) ont donc 40 ans de retard. Principaux changements du RGPD : sanctions accrues, partage des responsabilités (donneur d'ordres et sous-traitants), recours collectifs...Depuis le RGPD, 6000 plaintes ont été déposées à la CNIL dont trois plaintes collectives, par La Quadrature, NOYB et Privacy International. Conclusion : la CNIL est là pour vous aider (pas seulement pour sanctionner), allez la voir `<https://www.cnil.fr/>` pour conseil/accompagnement/etc.

Ensuite, les gens d'Exodus Privacy `<https://exodus-privacy.eu.org/>` (tellement privé que leurs noms de l'état civil n'ont pas été donné) ont présenté leur travail d'analyse des applications sur Android, et notamment des innombrables pisteurs dont elles sont truffées. (Voir par exemple celle de l'Obs `<https://reports.exodus-privacy.eu.org/en/reports/3032/>` alors que ce journal explique régulièrement que les GAFA sont méchants.) Les développeurs ne mettent pas toujours les pisteurs délibérement. Ils utilisent des bibliothèques, et beaucoup incluent les pisteurs [disons franchement : les mouchards]. Vous utilisez le SDK Facebook, il y a un pisteur Facebook dedans. Programmeu[Caractère Unicode non montré [1]]r[Caractère Unicode non montré]se[Caractère Unicode non montré]s : attention donc à ce que vous embarquez dans votre application.

Un excellent mais terrible exemple était celui de l'application « Baby + » (application de suivi de grossesse) qui transmettait des données personnelles à Facebook : le fœtus avait un compte Facebook avant même sa naissance. (Alors que personne n'avait utilisé Facebook sur cet ordiphone.) Pour aider l'excellent travail d'analyse d'Exodus Privacy, c'est par ici `<https://exodus-privacy.eu.org/page/contribute/>`.

Puis Gaetan Ferry (Synacktiv) a parlé d'obscurcissement des programmes. Il s'agit de transformer un programme en quelque chose d'illisible (pas mal de développeurs PHP y arrivent très bien sans disposer de ces outils...) Cette technique ne sert qu'au logiciel privateur et aux attaquants qui veulent faire passer un logiciel malveillant à travers les protections du réseau (ce ne sont pas forcément des malhonnêtes, cela peut être des pentesteurs). Ce n'est donc pas forcément utile, mais c'est rigolo techniquement.

Les analyses théoriques de l'obscurcissement de programmes montrent que ça ne marche pas. Mais en pratique, ça marche suffisamment pour les buts souhaités (rendre l'analyse plus difficile, voire impossible en pratique). On obscurcit les noms en remplaçant les noms des classes/variables/fonctions. Cette perte d'informations est irrémédiable. Évidemment, ça ne suffit pas, il faut aussi brouiller la structure du code. (Mais ça peut casser le programme s'il fait de l'introspection.) On utilise par exemple la « chenxification » : remplacer tout le programme par un énorme "*switch*". Et pour obscurcir les données, on les remplace par des résultats de fonctions (par exemple on remplace `false` par `n > n`, bon évidemment, en vrai, c'est plus compliqué). À noter que déboguer une bogue dans l'obscurcisseur est difficile puisque le programme produit est obscur...

Enfin, Pierre Blondeau (Université de Caen) a présenté un système de "*boot*" sécurisé mais automatique d'une machine Linux dont le disque est chiffré. Le cahier des charges imposait qu'on puisse

1. Car trop difficile à faire afficher par LaTeX

démarrer la machine même en l'absence de son utilisateur (et donc sans connaitre la phrase de passe). Donc, dans initramfs, il a ajouté un client qui s'authentifie (cryptographie asymétrique) auprès d'un serveur local qui lui donne la clé de déchiffrement du disque. Un méchant qui volerait une des machines ne pourrait pas la démarrer. Le logiciel est disponible en ligne <https://forge.greyc.fr/projects/network-trusted-boot>.

Mon exposé à cette conférence portait sur « La sécurité est-elle l'amie ou l'ennemie des droits humains ? ». Les supports de l'exposé sont disponibles ici en PDF (en ligne sur https://www.bortzmeyer.org/files/jsecin-securite-dh-pour-ecran.pdf), il y a aussi une version pour l'impression sur papier (en ligne sur https://www.bortzmeyer.org/files/jsecin-securite-dh-pour-impression.pdf), et, si vous lisez le LaTeX, le source (en ligne sur https://www.bortzmeyer.org/files/jsecin-securite-dh.tex). Une transcription de l'exposé a été faite par l'APRIL (merci à eux pour cet énorme travail, fait avec soin !) et est désormais en ligne <https://www.april.org/la-securite-est-elle-l-a
(Pendant cet exposé, j'ai cité Zittrain donc c'est l'occasion de dire que j'avais parlé de son livre <https://www.bortzmeyer.org/future-internet.html>.)

Tout (sauf l'exposé du représentant de l'ANSSI) a été filmé et les vidéos se trouvent sur la plateforme de l'Université <https://webtv.univ-rouen.fr>. La mienne est .

Merci à Magali Bardet, Romain Hérault, et tous les autres organisateurs (et aux spectacteurs).