Les données que récolte Google – Ch.3

Voici déjà la traduction du troisième chapitre de Google Data Collection, l'étude élaborée par l'équipe du professeur Douglas C. Schmidt, spécialiste des systèmes logiciels, chercheur et enseignant à l'Université Vanderbilt. Si vous les avez manqués, retrouvez les chapitres précédents déjà publiés.

Il s'agit aujourd'hui de mesurer ce que les plateformes les plus populaires recueillent de nos smartphones

Traduction Framalang : Côme, goofy, Khrys, Mika, Piup. Remerciements particuliers à badumtss qui a contribué à la traduction de l'infographie.

La collecte des données par les plateformes Android et Chrome

11. Android et Chrome sont les plateformes clés de Google qui facilitent la collecte massive de données des utilisateurs en raison de leur grande portée et fréquence d'utilisation. En janvier 2018, Android détenait 53 % du marché américain des systèmes d'exploitation mobiles (iOS d'Apple en détenait 45 %)[1] et, en mai 2017, il y avait plus de 2 milliards d'appareils Android actifs par mois dans le monde.[2]

12. Le navigateur Chrome de Google représentait plus de 60 % de l'utilisation mondiale de navigateurs Internet avec plus d'un milliard d'utilisateurs actifs par mois, comme l'indiquait le rapport Q4 10K de 2017[3]. Les deux plateformes facilitent l'usage de contenus de Google et de tiers (p.ex. applications et sites tiers) et fournissent donc à Google un accès à un large éventail d'informations personnelles,

d’activité web, et de localisation.

A. Collecte d’informations personnelles et de données d’activité

13. Pour télécharger et utiliser des applications depuis le Google Play Store sur un appareil Android, un utilisateur doit posséder (ou créer) un compte Google, qui devient une passerelle clé par laquelle Google collecte ses informations personnelles, ce qui comporte son nom d’utilisateur, son adresse de messagerie et son numéro de téléphone. Si un utilisateur s’inscrit à des services comme Google Pay[4], Android collecte également les données de la carte bancaire, le code postal et la date de naissance de l’utilisateur. Toutes ces données font alors partie des informations personnelles de l’utilisateur associées à son compte Google.

14. Alors que Chrome n’oblige pas le partage d’informations personnelles supplémentaires recueillies auprès des utilisateurs, il a la possibilité de récupérer de telles informations. Par exemple, Chrome collecte toute une gamme d’informations personnelles avec la fonctionnalité de remplissage automatique des formulaires, qui incluent typiquement le nom d’utilisateur, l’adresse, le numéro de téléphone, l’identifiant de connexion et les mots de passe.[5] Chrome stocke les informations saisies dans les formulaires sur le disque dur de l’utilisateur. Cependant, si l’utilisateur se connecte à Chrome avec un compte Google et active la fonctionnalité de synchronisation, ces informations sont envoyées et stockées sur les serveurs de Google. Chrome pourrait également apprendre la ou les langues que parle la personne avec sa fonctionnalité de traduction, activée par défaut.[6]

15. En plus des données personnelles, Chrome et Android envoient tous deux à Google des informations concernant les

activités de navigation et l'emploi d'applications mobiles, respectivement. Chaque visite de page internet est automatiquement traquée et collectée par Google si l'utilisateur a un compte Chrome. Chrome collecte également son historique de navigation, ses mots de passe, les permissions particulières selon les sites web, les cookies, l'historique de téléchargement et les données relatives aux extensions.[7]

16. Android envoie des mises à jour régulières aux serveurs de Google, ce qui comprend le type d'appareil, le nom de l'opérateur, les rapports de bug et des informations sur les applications installées[8]. Il avertit également Google chaque fois qu'une application est ouverte sur le téléphone (ex. Google sait quand un utilisateur d'Android ouvre son application Uber).

B. Collecte des données de localisation de l'utilisateur

17. Android et Chrome collectent méticuleusement la localisation et les mouvements de l'utilisateur en utilisant une variété de sources, représentées sur la figure 3. Par exemple, un accès à la « localisation approximative » peut être réalisé en utilisant les coordonnées GPS sur un téléphone Android ou avec l'adresse IP sur un ordinateur. La précision de la localisation peut être améliorée (« localisation précise ») avec l'usage des identifiants des antennes cellulaires environnantes ou en scannant les BSSID (''*Basic Service Set IDentifiers*''), identifiants assignés de manière unique aux puces radio des points d'accès Wi-Fi présents aux alentours[9]. Les téléphones Android peuvent aussi utiliser les informations des balises Bluetooth enregistrées dans l'API Proximity Beacon de Google[10]. Ces balises non seulement fournissent les coordonnées de géolocalisation de l'utilisateur, mais pourraient aussi indiquer à quel étage

exact il se trouve dans un immeuble.[11]

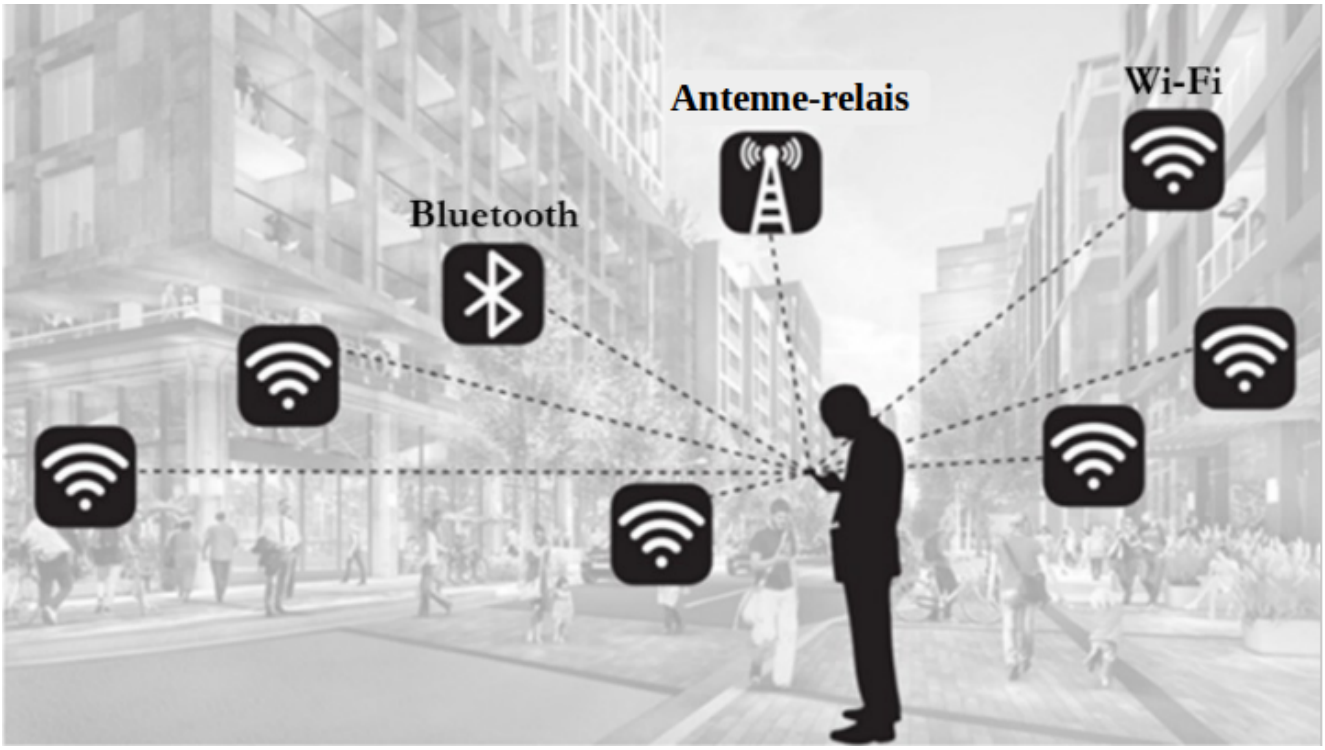


Figure 3 : Android et Chrome utilisent diverses manières de localiser l’utilisateur d’un téléphone.

18. Il est difficile pour un utilisateur de téléphone Android de refuser le traçage de sa localisation. Par exemple, sur un appareil Android, même si un utilisateur désactive le Wi-Fi, la localisation est toujours suivie par son signal Wi-Fi. Pour éviter un tel traçage, le scan Wi-Fi doit être explicitement désactivé par une autre action de l’utilisateur, comme montré sur la figure 4.

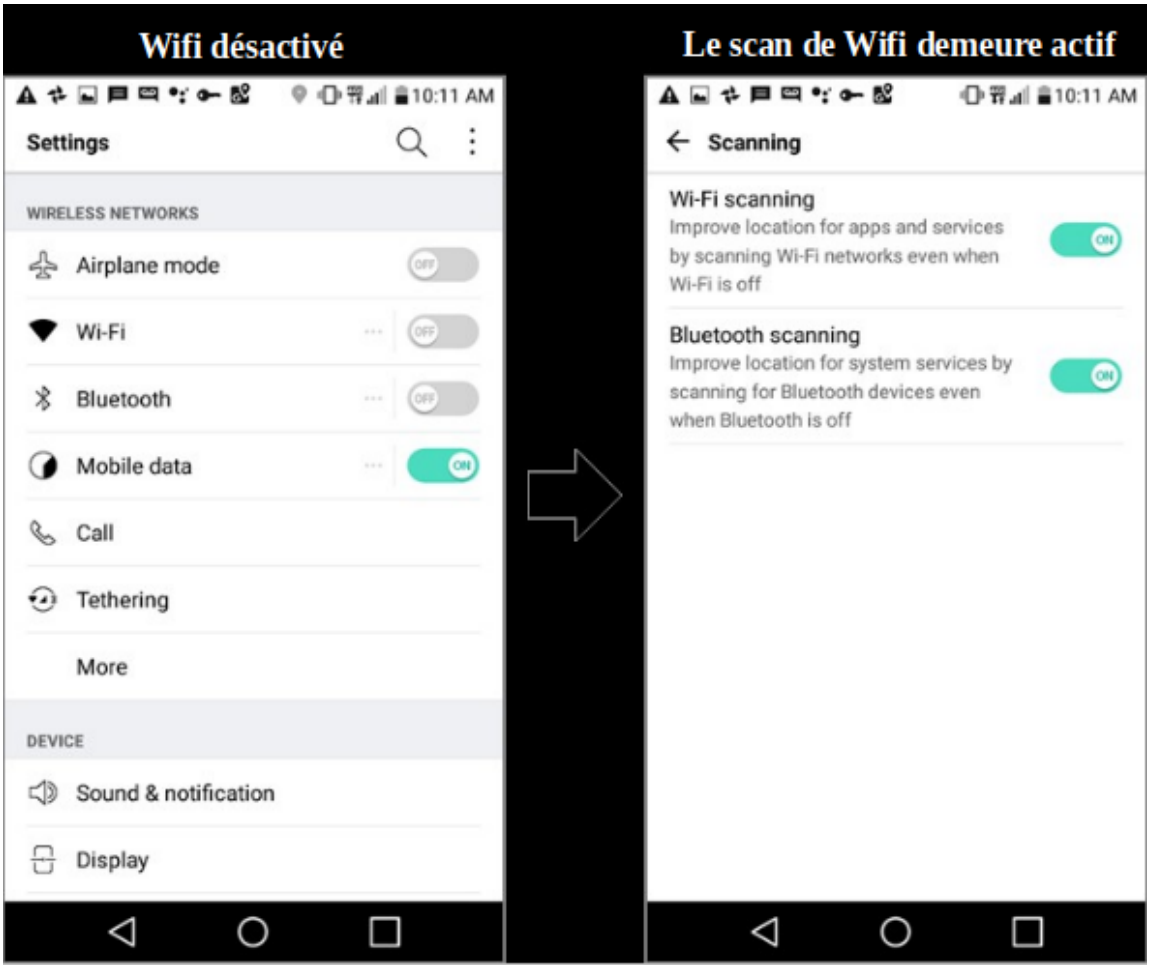


Figure 4 : Android collecte des données même si le Wi-Fi est éteint par l'utilisateur

19. L'omniprésence de points d'accès Wi-Fi a rendu le traçage de localisation assez fréquent. Par exemple, durant une courte promenade de 15 minutes autour d'une résidence, un appareil Android a envoyé neuf requêtes de localisation à Google. Les requêtes contenaient au total environ 100 BSSID de points d'accès Wi-Fi publics et privés.

20. Google peut vérifier avec un haut degré de confiance si un utilisateur est immobile, s'il marche, court, fait du vélo, ou voyage en train ou en car. Il y parvient grâce au traçage à intervalles de temps réguliers de la localisation d'un utilisateur Android, combiné avec les données des capteurs embarqués (comme l'accéléromètre) sur les téléphones mobiles. La figure 5 montre un exemple de telles données communiquées

aux serveurs de Google pendant que l'utilisateur marchait.

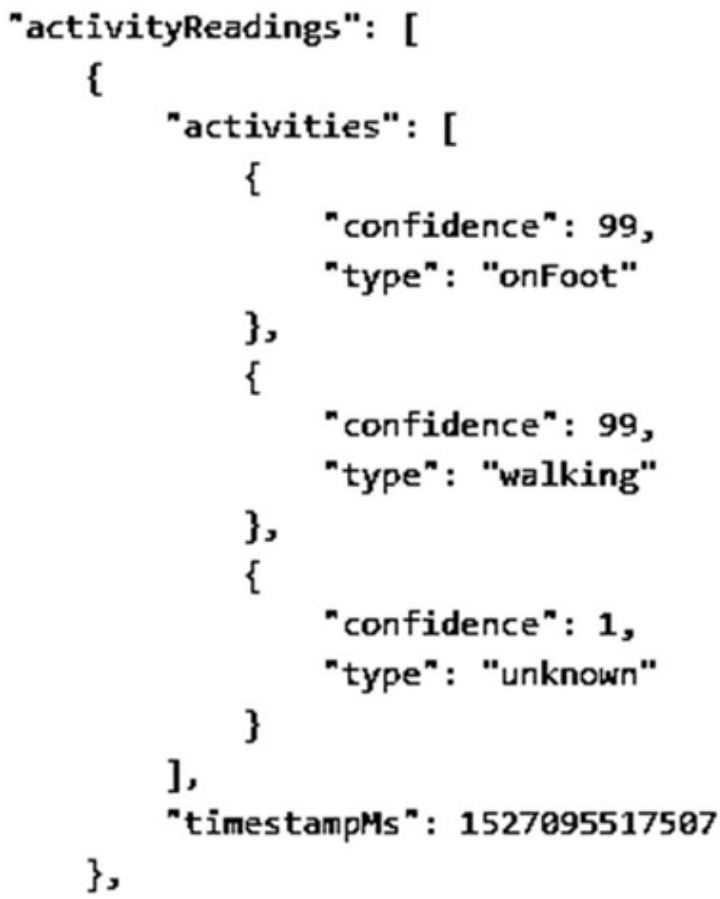


Figure 5 : capture d'écran d'un envoi de localisation d'utilisateur à Google.

C. Une évaluation de la collecte passive de données par Google via Android et Chrome

21. Les données actives que les plateformes Android ou Chrome collectent et envoient à Google à la suite des activités des utilisateurs sur ces plateformes peuvent être évaluées à l'aide des outils *MyActivity* et *Takeout*. Les données passives recueillies par ces plateformes, qui vont au-delà des données de localisation et qui restent relativement méconnues des utilisateurs, présentent cependant un intérêt potentiellement plus grand. Afin d'évaluer plus en détail le type et la

fréquence de cette collecte, une expérience a été menée pour surveiller les données relatives au trafic envoyées à Google par les téléphones mobiles (Android et iPhone) en utilisant la méthode décrite dans la section IX.D de l'annexe. À titre de comparaison, cette expérience comprenait également l'analyse des données envoyées à Apple via un appareil iPhone.

22. Pour des raisons de simplicité, les téléphones sont restés stationnaires, sans aucune interaction avec l'utilisateur. Sur le téléphone Android, une seule session de navigateur Chrome restait active en arrière-plan, tandis que sur l'iPhone, le navigateur Safari était utilisé. Cette configuration a permis une analyse systématique de la collecte de fond que Google effectue uniquement via Android et Chrome, ainsi que de la collecte qui se produit en l'absence de ceux-ci (c'est-à-dire à partir d'un appareil iPhone), sans aucune demande de collecte supplémentaire générée par d'autres produits et applications (par exemple YouTube, Gmail ou utilisation d'applications).

23. La figure 6 présente un résumé des résultats obtenus dans le cadre de cette expérience. L'axe des abscisses indique le nombre de fois où les téléphones ont communiqué avec les serveurs Google (ou Apple), tandis que l'axe des ordonnées indique le type de téléphone (Android ou iPhone) et le type de domaine de serveur (Google ou Apple) avec lequel les paquets de données ont été échangés par les téléphones. La légende en couleur décrit la catégorisation générale du type de demandes de données identifiées par l'adresse de domaine du serveur. Une liste complète des adresses de domaine appartenant à chaque catégorie figure dans le tableau 5 de la section IX.D de l'annexe.

24. Au cours d'une période de 24 heures, l'appareil Android a communiqué environ 900 échantillons de données à une série de terminaux de serveur Google. Parmi ceux-ci, environ 35 % (soit environ 14 par heure) étaient liés à la localisation. Les domaines publicitaires de Google n'ont reçu que 3 % du trafic,

ce qui est principalement dû au fait que le navigateur mobile n'a pas été utilisé activement pendant la période de collecte. Le reste (62 %) des communications avec les domaines de serveurs Google se répartissaient grosso modo entre les demandes adressées au magasin d'applications Google Play, les téléchargements par Android de données relatives aux périphériques (tels que les rapports de crash et les autorisations de périphériques), et d'autres données – principalement de la catégorie des appels et actualisations de fond des services Google.

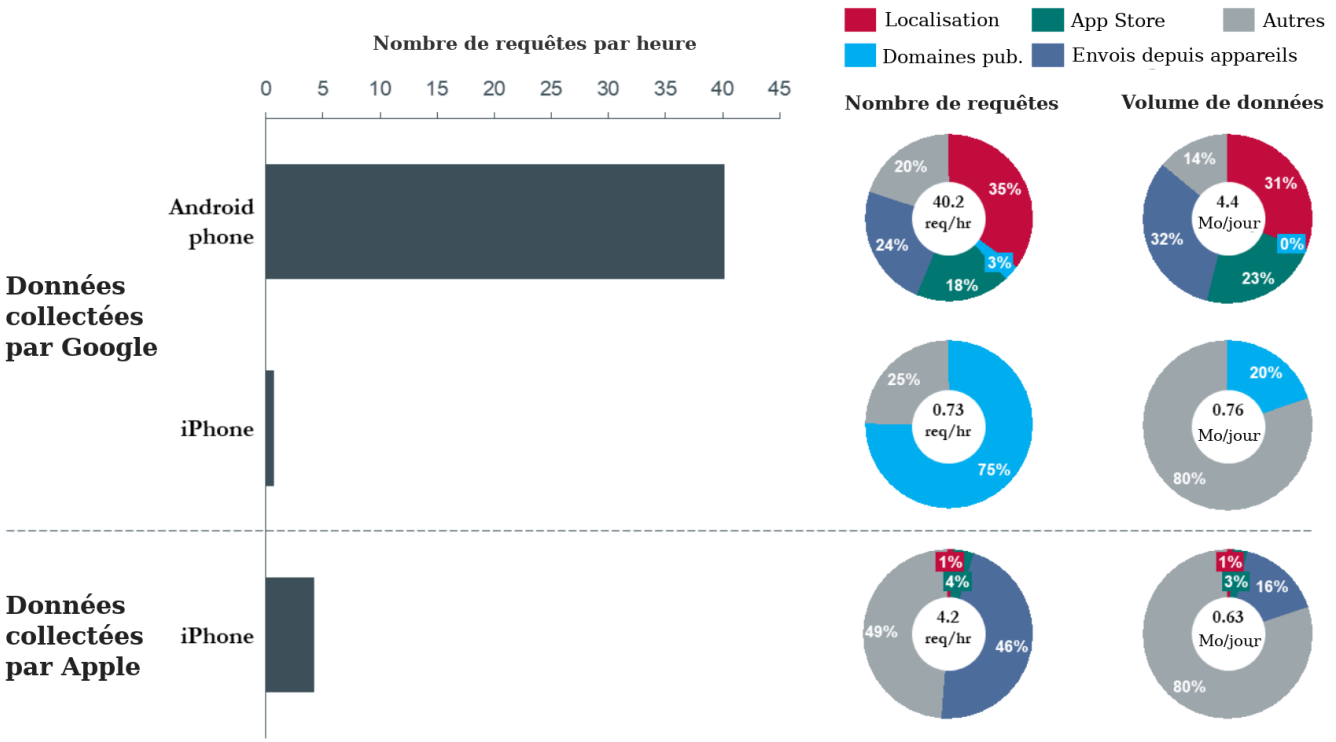


Figure 6 : Données sur le trafic envoyées par les appareils Andoid et les iPhones en veille.

25. La figure 6 montre que l'appareil iPhone communiquait avec les domaines Google à une fréquence inférieure de plus d'un ordre de grandeur (50 fois) à celle de l'appareil Android, et que Google n'a recueilli aucun donnée de localisation utilisateur pendant la période d'expérience de 24 heures via iPhone. Ce résultat souligne le fait que les plateformes Android et Chrome jouent un rôle important dans la collecte de

données de Google.

26. De plus, les communications de l’appareil iPhone avec les serveurs d’Apple étaient 10 fois moins fréquentes que les communications de l’appareil Android avec Google. Les données de localisation ne représentaient qu’une très faible fraction (1 %) des données nettes envoyées aux serveurs Apple à partir de l’iPhone, Apple recevant en moyenne une fois par jour des communications liées à la localisation.

27. En termes d’amplitude, les téléphones Android communiquaient 4,4 Mo de données par jour (130 Mo par mois) avec les serveurs Google, soit 6 fois plus que ce que les serveurs Google communiquaient à travers l’appareil iPhone.

28. Pour rappel, cette expérience a été réalisée à l’aide d’un téléphone stationnaire, sans interaction avec l’utilisateur. Lorsqu’un utilisateur commence à bouger et à interagir avec son téléphone, la fréquence des communications avec les serveurs de Google augmente considérablement. La section V du présent rapport résume les résultats d’une telle expérience.

La promiscuité sans fil des réseaux WiFi publics

Se connecter à un Wifi public dans un parc, une gare ou un café [1] pour accéder à Internet, c'est un peu comme passer par la salle d'attente du médecin avant une consultation. Dans les deux cas, vous avez confiance en votre destination [2], mais vous êtes au préalable enfermé dans un espace avec des étrangers, tous plus ou moins malades.

En effet, le WiFi d'un café vous connecte, comme la salle d'attente, avec votre entourage direct, sans que vous ayez rien demandé. Or, si votre dossier médical est confidentiel, il suffit de faire tomber ses papiers dans une salle d'attente pour que toutes les personnes présentes puissent les lire, et il suffit de se connecter (via un WiFi public) à un service qui n'utilise pas le protocole HTTPS pour que votre entourage connecté puisse s'immiscer dans votre session et votre intimité.

Les coupables ? Les sites conservant à votre place des éléments de votre vie privée d'une part, et proposant d'autre part et sans la protection du petit cadenas qui dénote de l'utilisation du protocole HTTPS, de « garder votre session ouverte » grâce à un cookie. Si vous y prenez garde, ce n'est pas le cas des services en ligne de votre banque.

Toutefois, si l'auteur est assez pessimiste dans son petit billet complémentaire (reproduit ici à la suite du premier) face aux moyens de protection à notre disposition, il existe plusieurs extensions Firefox pour limiter les risques sans trop se compliquer la vie, citons (sur les bons conseils de Goofy) HTTPS Everywhere, et Force-TSL. De plus, il me semble également assez simple de se connecter, où qu'on soit, d'abord à un VPN personnel, ou directement en SSH sur son serveur à soit (voir l'extension Foxyproxy de Firefox), pour surfer ensuite l'esprit tranquille et sans laisser de traces locales,

comme si on était à la maison. D'ailleurs, votre WiFi chez vous, il est protégé comment ?

Quand le berger prévient les moutons à New York City

Herding Firesheep in New York City

Gary LosHuertos – 27 octobre 2010 – TechnologySufficientlyAdvanced.blogspot.com
Traduction Framalang : Goofy, Pablo, cheval_boiteux

On a beaucoup parlé de Firesheep ces derniers jours. Cette extension gratuite pour Firefox récolte pour vous les cookies qui sont envoyés depuis un réseau WiFi non protégé n'utilisant pas le protocole SSL. Vous la mettez en route, elle collecte les cookies de Facebook, Twitter et de 24 autres sites (par défaut). Ensuite, vous pouvez voler l'identité d'un compte et obtenir l'accès sous cette identité.

L'extension n'a rien de scandaleux en elle-même. Si vous êtes un développeur un peu compétent, vous savez depuis longtemps que cette faille existait, n'est-ce pas ? Mais quid du reste du monde ? Tous ces gens qui n'ont jamais entendu parler de cette nouvelle menace si facile d'accès, qui n'ont pas été alertés par leurs amis, qui ne regardent pas Engadget, ni Slashdot, ni ABC Pronews7 à Amarillo ?

Je me suis dit que j'allais faire passer le message et aider les béotiens après leur travail, puisqu'il y a un grand Starbucks tout près de chez moi. J'y suis allé, j'ai acheté un peu de nourriture malsaine, j'ai ouvert mon portable et lancé Firesheep. Moins d'une minute plus tard, j'avais cinq ou six identités disponibles dans le panneau latéral. Trois d'entre elles étaient sur Facebook.

Absolument rien de surprenant ; Firesheep n'est pas magique, et tous ceux qui vont au Starbucks savent qu'un tas de gens y

mettent à jour leur statut Facebook sans faire attention, tout en sirotant leur café au lait. J'ai pensé que j'allais y passer un peu plus de temps, j'ai donc écouté un peu de musique, parlé à quelques amis, et le plus important (mais pas le plus simple) je n'ai navigué sur aucun site avec le protocole standard HTTP (et surtout pas sur Facebook évidemment).

Environ une demi-heure plus tard, j'avais récolté entre 20 et 40 identités. Puisque Facebook était de loin le service le plus représenté (et qu'il détient plus d'informations personnelles que Twitter) j'ai décidé d'envoyer aux utilisateurs des messages depuis leur propre compte, pour les avertir des risques auxquels ils s'exposaient. J'ai fait un modèle de message sympa qui précisait la localisation du Starbucks, la nature de la vulnérabilité, et comment y remédier. J'ai envoyé des messages aux 20 personnes autour de moi.

J'ai nettoyé le panneau latéral, retiré mes écouteurs, et j'ai attendu. J'ai entendu quelqu'un marmonner un juron pas très loin, et me suis demandé si mon message en était la cause. Pendant le quart d'heure suivant, je n'ai entendu strictement personne parler de ce qui venait se passer (pourtant ceux qui fréquentent les Starbucks ne sont le plus souvent pas du genre à tenir des conversations discrètes). Pourtant, j'ai pu vraiment constater une nette chute du nombre d'identités que je pouvais récolter quand j'ai relancé Firesheep.

C'était un soulagement – en voilà qui avaient compris le message. Avec un peu de chance, ils allaient alerter leurs amis, mettre à l'abri leur femme et leurs enfants. J'ai de nouveau nettoyé le panneau latéral, et après une vingtaine de minutes de conversations impromptues j'ai vu que cinq identités que j'avais déjà croisées étaient revenues dans mon troupeau.

C'était assez surprenant. Avaient-ils reçu le premier

message ? Je me suis mis sur leur compte avec leurs identifiants, et en effet ils l'avaient reçu. L'un d'entre eux était même sur Amazon.com, site contre lequel j'avais mis en garde dans mon premier message. Je l'ai choisi pour première cible : j'ai ouvert sa page perso sur Amazon, j'ai repéré un truc sur lequel il avait récemment jeté un coup d'œil et lui ai envoyé un mot : « non, c'est pas sérieux » sur Facebook depuis son propre compte, avec un clin d'œil sur ses goûts musicaux.

J'ai encore une fois effacé les identités, attendu dix minutes, et lorsque j'ai à nouveau rassemblé mon troupeau avec Firesheep, il était parti. Mais il y en avait encore quatre qui restaient là. Peut-être, me suis-je dit, qu'ils ont cru que c'était un message d'avertissement automatique les ciblant au hasard (bien que j'aie mentionné leur localisation dans un rayon d'une trentaine de mètres). Donc, un dernier message était nécessaire.

J'ai bricolé un très court message (le premier était peut-être trop long ?) et je l'ai envoyé aux quatre, une fois encore avec leur propre compte :

> *« C'était vraiment pas une blague l'avertissement sur la sécurité. Je n'enverrai plus d'autre message après celui-ci —— à vous de prendre sérieusement en main votre propre sécurité. Vous êtes au Starbucks XYZ connecté de façon non sécurisée, et absolument n'importe qui peut accéder à votre compte avec l'outil approprié nécessaire (et disponible à tous). »*

Vingt minutes ont passé, et tous les quatre utilisaient encore Facebook frénétiquement. Encore une fois, j'ai envisagé qu'ils auraient pu ne pas recevoir le message, mais en vérifiant leur compte j'ai vu qu'ils l'avaient bel et bien reçu.

Voilà ce qu'il y a de plus choquant à propos de la sécurité sur Internet : ce n'est pas que nous soyons tous scotchés sur

un réseau global qui tient avec des bouts de sparadrap et laisse béants d'horribles failles de sécurité ; ce n'est pas non plus qu'un outil librement disponible puisse récolter des cookies d'authentification ; et ce n'est toujours pas qu'il y ait des gens pas du tout au courant de l'un ni de l'autre. Ce qui est absolument incompréhensible, c'est qu'après avoir été averti d'un danger (et sur son propre compte !) on puisse tranquillement ignorer l'avertissement, et reprendre le fil de ses activités.

Mais enfin j'ai tenu parole et n'ai pas envoyé d'autre message. J'ai rangé mon matériel, fait un petit tour dans le café, et reconnu plusieurs personnes auxquelles j'avais montré leur vulnérabilité. Je n'avais pas laissé d'indices sur ma propre identité, moins par crainte de rétorsion que parce que l'intrusion dans la vie privée est encore plus traumatisante quand elle est commise par un étranger complet, dont on n'a pas la moindre chance de découvrir l'identité.

En revenant chez moi, j'ai réfléchi à ce que cette expérience révélait de notre société. Peu importe le nombre de mesures de sécurité que nous procurons au monde entier, il y aura toujours des gens qui laisseront la porte ouverte, même s'ils ont été victimes d'une intrusion. **Le maillon le plus faible de la sécurité c'est et ce sera toujours la décision de l'utilisateur.**

De retour dans mon appartement, j'ai commencé à m'installer – et c'est le moment où je me suis rendu compte que pendant toute la soirée j'avais eu la braguette grande ouverte. La preuve par neuf finalement : nous nous baladons tous avec des vulnérabilités qu'il nous reste à découvrir.

Addendum

Herding Firesheep Addendum

Gary LosHuertos – 04 novembre 2010 –

TechnologySufficientlyAdvanced.blogspot.com
Traduction Framalang : Siltaar, RaphaelH, Goofy

À la suite du billet précédent, je me suis dit qu'en voulant faire court j'avais omis quelques informations. Ceci sert donc d'addendum à mon précédent billet, et a été rédigé de la manière la plus courte possible.

Le message original envoyés aux clients était le suivant :

> *Comme vous utilisez Facebook sans chiffrement dans un Starbucks, votre compte a été compromis. Je ne suis qu'un amical client du Starbucks qui a souhaité vous prévenir de cette vulnérabilité.*
>
> *Vous pouvez en apprendre davantage en cherchant des informations sur « Firesheep ». Il n'y a pas vraiment de solutions disponibles pour protéger votre compte Facebook lorsque vous êtes connectés à un réseau public, et je vous recommande donc simplement de ne pas vous y connecter lorsque vous êtes dans un Starbucks. Cette faille affecte également Twitter, Amazon.com, Google (mais pas Gmail), et quantité d'autres services.*
>
> *Votre mot de passe n'a pas été compromis. Vous déconnecter de Facebook est tout ce que vous avez besoin de faire.*

Pour préciser mes motivations, laisser un compte Facebook sans protection ne signifie pas seulement que quelqu'un peut regarder vos photos, vos coups de cœurs et messages. Un compte Facebook compromis donne à quelqu'un d'autre l'accès à votre identité, lui permettant de se faire passer pour vous auprès de vos amis, ruinant potentiellement des relations. S'il est possible de rattraper les choses ensuite, le temps et l'énergie que ça demande sont importants, surtout pour quelqu'un qui a beaucoup d'amis. Quelqu'un envoyant un faux message à l'un de vos amis n'est peut être pas un gros problème, mais un faux message envoyé à 500 de vos amis est

déjà plus gênant. D'autant plus qu'il peut y avoir des collègues de travail, des membres de votre famille, ou des clients dans ces 500 personnes.

Concernant la légalité de mes actions : ça n'était pas l'objet de mon article. On peut toujours spéculer sur fait que je finisse en prison, mais c'est hors sujet par rapport à ce dont je parle dans mon billet : les sites non protégés comme Facebook et Twitter sont dangereux pour leurs utilisateurs. Il semble plus intéressant de consacrer son énergie à faire passer le mot plutôt que de troller sur mon éventuelle incarcération.

Enfin concernant ce que les utilisateurs peuvent faire, la meilleure réponse à l'heure actuelle est : rien. Ne vous connectez pas aux réseaux non protégés pour utiliser ces sites web, ou bien utilisez une application qui n'utilise pas d'authentification par cookie non protégée (pour ce que j'en sais, l'application Facebook pour iPhone ne le ferait pas). Assurez-vous que votre réseau WiFi domestique est chiffré en WPA, voire en WPA2 (le WEP est trivialement déchiffrable). Si vous utilisez Facebook au travail sur une connection sans-fil, vérifiez le chiffrement du réseau. **La faille de sécurité ne vient pas seulement de Firesheep, elle vient du manque de protection des connexions**. La menace la plus grande vient des outils automatisés qui existent depuis des années [3].

Notes

[1] Crédit : CarbonNYC *David Goehring* Creative Commons By

[2] Et le sujet ici, n'est pas savoir si cette confiance est bien placée…

[3] Voir la magie des Google Cars expliquées par PCINpact ou ZDNet par exemple…

Mon compte Facebook sait-il que je n'ai plus de toit ?

On n'y pense pas toujours mais en France près de la moitié des « foyers » n'est toujours pas connectée à Internet. Et que se passe-t-il si on n'a carrément pas de foyer ?

Doit-on renoncer à la « vie numérique » ? Pas forcément, mais on imagine sans peine les difficultés rencontrées.

C'est l'objet d'un récent reportage du Wall Street Journal. On peut se passer de télé, de radio, de journaux mais plus difficilement d'Internet, nous dit l'un des protagonistes. A fortiori quand on l'utilisait « comme tout un chacun » avant notre mise à la rue. A fortiori quand la crise est désormais susceptible d'atteindre plus encore les jeunes et les classe moyennes précarisées[1].

Dans la rue et sur Facebook : sans-abri mais branché sur le Web

On the Street and On Facebook: The Homeless Stay Wired

Phred Dvorak – 30 mai 2009 – Wall Street Journal
(Traduction Framalang : Cheval Boiteux, Tyah, Don Rico)

M. Pitts n'a pas d'adresse postale. Mais il a un ordinateur et

anime un forum sur Internet.

Comme la plupart des habitants de San Francisco, Charles Pitts a une vie en ligne. M. Pitts, 37 ans, a un compte sur Facebook, MySpace et Twitter, il anime un forum Yahoo, lit les journaux en ligne et garde le contact avec ses amis par courriel. Le plus difficile pour lui, c'est d'organiser sa vie numérique depuis son lieu de résidence : sous un pont d'autoroute.

« Pas besoin de télé, pas besoin de radio, même pas besoin de journaux papier », explique M. Pitts, poète amateur à la casquette violette et au blouson en polaire jaune, qui dit être SDF depuis deux ans. « Internet, par contre, c'est indispensable. »

L'exemple de M. Pitts démontre à quel point les ordinateurs et l'Internet ont imprégné la société. Il y a quelques années, certains craignaient qu'une « fracture numérique » sépare ceux qui ont accès aux nouvelles technologies et les autres. Les plus démunis n'ont certes pas les moyens de s'offrir un ordinateur et un accès à Internet. Pourtant, de nos jours aux États-Unis, même ceux qui n'ont pas de toit ressentent la nécessité d'avoir une adresse électronique.

La ville de New-York a installé quarante-deux ordinateurs dans cinq des neuf foyers qu'elle gère et projette d'équiper les quatre autres dans le courant de l'année. Environ la moitié des 190 autres foyers de la ville permettent d'accéder à un ordinateur. Selon le président de Central City Hospitality House, une association à but non lucratif de San Francisco, la moitié des visiteurs utilisant ces huit ordinateurs sont des sans-abri. Il y a une telle demande pour l'accès à ces postes que leur temps d'utilisation est limitée à 30 minutes.

D'après le personnel des foyers, le nombre de sans-abri équipés d'un ordinateur portable, qui reste faible, est en augmentation. SF Homeless *(NdT : Sans-Abri de San Francisco)*,

forum créé il y a deux ans, compte 140 membres. On y trouve les dates et horaires des réunions pour les logements sociaux et des informations provenant de groupes similaires actifs au Nouveau-Mexique, en Arizona, et dans le Connecticut. Il est complété par un blog qui propose des sondages en ligne sur la vie dans les foyers.

Les prix de plus en plus bas des ordinateurs et l'accès gratuit à Internet alimentent ce phénomène, ainsi que la maîtrise de l'outil informatique de plus en plus généralisée au sein de la population. Pour répondre à une offre d'emploi ou faire une demande de logement, les démarches se déroulent de plus en plus souvent en ligne. Selon certains membres d'associations d'aide aux sans-abri, la crise économique va jeter à la rue de nombreuses personnes issues de la classe moyenne habituées à l'Internet.

Âgé de 29 ans, Paul Weston se destine à une carrière de programmeur. Son Powerbook Macintosh, nous confie-t-il, est pour lui un véritable « canot de sauvetage » depuis qu'il a dû s'installer dans un foyer après avoir perdu son poste de réceptionniste d'hôtel en décembre dernier. Installé dans un magasin Whole Foods qui propose un accès Internet gratuit, M. Weston cherche du travail et écrit un programme informatique qu'il espère réussir à vendre. Il a envoyé des courriels aux élus de la ville pour demander l'amélioration des conditions de vie dans les foyers.

Lisa Stringer, qui dirige une formation où l'on apprend aux SDF et aux habitants défavorisés à chercher un emploi et à se servir de l'outil informatique, explique que certains de ses étudiants, alors qu'ils ne savent ni lire ni écrire, économisent pour se payer un ordinateur. « Dans la société actuelle, posséder un ordinateur signifie qu'on est à la page et connecté », analyse-t-elle. Il lui arrive parfois de conseiller vivement à ses étudiants sans-abri d'attendre que leur situation se soit stabilisée avant d'acheter un portable.

Avoir une vie en ligne lorsqu'on vit dans la rue exige une grande détermination. L'électricité et l'accès à Internet sont des denrées rares. S'ajoutent à ces difficultés les menaces telles que la pluie et le vol.

Robert Livingston, 49 ans, trimballe son portable Asus partout depuis qu'il a perdu son logement en décembre dernier. Homme soigné qui dépense une partie de son allocation mensuelle de 59 dollars chez le coiffeur, M. Livingston raconte qu'il a démissionné d'un poste d'agent de sécurité l'année dernière, et qu'il n'a pas réussi à retrouver du travail à cause de la crise.

Lorsqu'il s'est rendu compte qu'il allait devenir SDF, M. Livingston a acheté un sac à dos robuste pour ranger son matériel, un cadenas pour son casier du foyer et un compte Flickr Premium à 25 dollars pour diffuser ses photos numériques.

Il y a peu, installé dans un café où les clients peuvent parfois profiter de la connexion sans fil, M. Livingston montrait fièrement sa page personnelle, qui propose des liens pour des leçons de chinois.

M. Livingston affirme que son ordinateur l'aide à rester en lien avec la société et à garder son humanité. « Être dans la rue, c'est effrayant », nous confie-t-il. « Sur Internet, je suis sur un pied d'égalité avec tout le monde. »

Pour Skip Schreiber, philosophe amateur de 64 ans qui vit aujourd'hui dans une camionnette, le plus gros défi pour rester connecté, c'est l'électricité. M. Schreiber était chauffagiste avant que le stress et une dépression liés au travail ne le mettent sur la touche il y a quinze ans.

Pour son 60ème anniversaire, il a puisé dans sa pension d'invalidité mensuelle pour s'offrir un ordinateur portable, branché sur la batterie de son véhicule, et a appris seul à s'en servir. « J'aimais le concept d'Internet », explique

M.Schreiber, « cette source illimitée d'opinions et de réflexion ».

Récemment, M. Schreiber a changé de machine pour un Mac parce que celui-ci consomme moins. Quand il le peut, il coupe le ventilateur et l'antenne WiFi, et rafraîchit son portable en le posant sur un chiffon humide. Grâce à ces astuces, affirme-t-il, il réussit à faire durer sa batterie jusqu'à seize heures, à condition de proscrire les vidéos.

Dans sa camionnette où s'entassent caisses à outils, matériel électrique et couchage, M. Schreiber nous montre le contenu de son disque dur, qui comprend l'intégralité des codes civil et pénal de la Californie, ou encore des fichiers sur des penseurs tels que Thomas d'Aquin ou le psychologue Philip Zimbardo. M. Schreiber explique que les écrits sur le comportement et les aspirations des hommes l'aident à mieux appréhender son sort.

« Nul ne se conçoit comme un sans-abri », déclare-t-il. « Nous faisons nos choix au mieux, selon ce qui nous est donné. »

Michael Ross produit lui-même son électricité, grâce à un groupe électrogène installé à l'extérieur de sa tente jaune et bleue. Depuis un an, M. Ross assure la surveillance d'un parking où est entreposé du matériel de construction, grâce à un accord passé avec le propriétaire. M. Ross, qui n'a que sa pension de vétéran pour survivre, estime être SDF depuis une quinzaine d'années.

Sous la tente, ce cinquantenaire taciturne possède un laptop HP pourvu d'un écran de 17 pouces et d'un espace de stockage de 320 Go, ainsi que quatre disques durs externes supplémentaires d'une capacité totale de 1000 Go, l'équivalent de 200 DVDs. M Ross adore les films. Il en loue certains en ligne, sur Netflix et Blockbuster, et en télécharge d'autres grâce à une connection Ethernet à la bibliothèque publique de San Francisco.

L’autre soir, M. Ross s’est installé sur son sac de couchage pour regarder un épisode des X-Men, obligé d’écouter au casque pour couvrir le vacarme du groupe électrogène. Lorsqu’il se rend en ville, il emporte tout son matériel avec lui par sécurité. Son sac-à-dos est plein à craquer de cordons et de gadgets électroniques emballés dans du papier-bulle. Selon M. Ross, le poids ne lui pose pas problème.

M. Pitts, le poète qui vit sous un pont, retient de tête une liste d’endroits où il peut recharger sa batterie et se connecter à l’Internet, endroits parmi lesquels on trouve un coin peu fréquenté d’une des gares de la ville et des cafés équipés du WiFi, dont les patrons tolèrent que l’on s’y installe pour longtemps et avec beaucoup de sacs.

Expulsé de son appartement il y a deux ans, M. Pitts raconte : « Je me suis dit que mon existence et ma vie ne s’arrêtaient pas parce que je n’avais plus de toit ».

Il s’est alors acheté un portable Toshiba. Lorsque celui-ci a rendu l’âme, il l’a remplacé par un Dell d’occasion. Le mois dernier, l’écran du Dell s’est cassé. À présent, pour consulter son courrier électronique et participer à son forum consacré aux problèmes des sans-abri, il se sert des ordinateurs des bibliothèques et des campus universitaires, ou encore d’un portable caché par un de ses copains derrière le comptoir d’un café.

Ayant appris il y a un mois que le Dalaï Lama devait venir en viste dans une soupe populaire des environs, M. Pitts est allé sur Wikipédia faire une recherche sur le chef spirituel bouddhiste et a copié le texte de l’article sur son iPod pour le lire au lit, sous le pont qui l’abrite. « Sous ma couverture, à l’abri d’une bâche plastique, j’apprends des tas de trucs sur le Dalaï Lama. »

M. Pitts compte bientôt réussir à économiser assez d’argent pour se racheter un ordinateur. Il espère pouvoir en trouver

un à moins de 200 dollars.

Remarque : Sur le site d'origine du Wall Street Journal, on trouve un diaporama avec une dizaine de photographies « en situation » des personnes citées dans l'article.

Notes

[1] Crédit photo : Hrvoje Go (Creative Commons By)

Chérie, j'ai partagé le Wi-Fi !

Je dois avouer que mes connaissances en wi-fi ne dépassent pas le niveau de la mer mais ce n'est pas une raison pour ne pas en parler surtout quand il s'agit d'une traduction !

La traduction[1] en question est un peu technique mais elle est surtout là pour annoncer qu'il existe des solutions libres (et peu onéreuses au niveau matériel) pour déployer un réseau wifi maillé et partager internet en mutualisant quelques connexions.

J’en veux pour meilleure preuve l’installation récente au Marché Biron, au coeur des puces de Paris Saint-Ouen, d’un déploiement ambitieux « qui n’exploite que des technologies open source pour constituer un réseau maillé wifi afin de couvrir une grande surface pour un faible coût ». Pour en savoir plus je vous invite vivement à parcourir l’article Toonux et Entreprise Transparence déploient un réseau wifi communautaire 100% open source au Marché Biron.

Comme dirait Léo Ferré, c’est extra ! Oui mais il y a un hic (outre la question de la nocivité du wi-fi), ainsi que nous le rappelle Bluetouff sur son blog dans un billet intitulé : La riposte graduée menace le wifi des particuliers comme des professionnels.

> *« Tout pourrait aller pour le mieux dans le meilleur des mondes s’il n’y avait pas la menace de l’HADOPI qui entend que nous posions des dispositifs de filtrage visant à empêcher tout téléchargement « illicites »… Le problème de la responsabilité en cas d’avertissement se pose donc : qui est responsable ? « La personne qui partage sa bande passante » souhaite répondre l’HADOPI, sur le seul principe qu’elle semble reconnaître « une ip, un coupable ».*
>
> *Si tel était le cas, ce serait bien là la fin de l’aventure des réseaux mesh communautaires et ouverts pour servir les intérêts de maisons de disques et quelques ayants-droit dont une bonne partie ne paye même pas d’impôts en France. »*

Il faut bien que les professionnels (industries du disque, fournisseurs d’accès internet, etc.) gagnent justement leur croûte. Il n’empêche qu’une société qui stigmatise voire interdit le partage dans un nombre croissant de secteurs d’activité n’est clairement pas une société en bonne santé…

La révolution Open-Mesh

The Open-Mesh Revolution

Sam Churchill – 11 mars 2008 – DailyWireless.org

Il y a un an de cela le relais Wifi Meraki à 50$ était une petite révolution, une solution parfaite pour combler le fossé numérique. Puis Meraki a vu son prix augmenter et le boîtier bon marché s'est vu amputé de presque toutes ses fonctions (FAQ). La version de base ne permet plus maintenant la facturation, l'authentification des utilisateurs, le contrôle de l'accès ou l'affichage d'une page d'accueil personnalisée. Il vous faudra débourser 100$ par appareil pour retrouver la plupart des fonctionnalités auparavant gratuites. Meraki impose maintenant des publicités au travers de leurs services hébergés.

Voilà qui a vraiment énervé beaucoup de monde.

Beaucoup d'entreprises, comme Net Equality (appartenant maintenant à One Economy), employaient le Meraki pour fournir, gratuitement ou à bas prix, un accès Internet à des foyers aux revenus modestes. Ce changement de direction les a laissés en plan.

C'est là que Michael Burmeister-Brown intervient, il est le co-fondateur de Net Equality et le développeur du logiciel Dashboard qui permettait une gestion rapide, simple et peu coûteuse de douzaines, voire de centaines de relais Merakis.

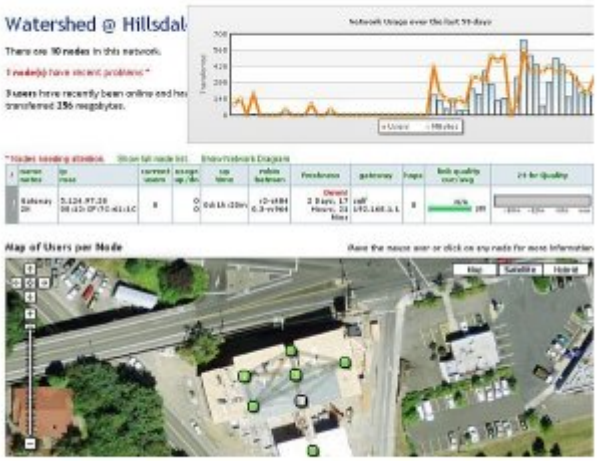
Aujourd'hui Michael Burmeister-Brown a annoncé un nouveau

produit et une nouvelle entreprise créés pour combler le vide laissé par Meraki : Open-Mesh.

Open-Mesh fait tout ce que faisait le Meraki original et même plus :

- C'est pas cher. Les relais Wifi Open-Mesh coûtent 49$ l'unité ou 39,95$ (quantité : 20);
- C'est sans publicité. Open-Mesh fait la promesse de ne jamais imposer de publicité sur vos réseaux. Vous décidez du contenu que vous voulez afficher;
- C'est 100% open-source et déployé sur OpenWRT. Vous pouvez modifier tout ce que vous désirez ;
- Vous pouvez re-flasher le firmware si vous voulez;
- Grâce au système de gestion Dashboard vous administrez votre réseau et suivez les alertes et le mappage librement. Vous pouvez configuer l'ESSID, la page d'accueil, les mots de passe et la bande passante allouée à vos réseaux;
- Les dispositifs s'auto-configurent. C'est simple de créer un réseau de quartier ou d'appartement. Vous n'êtes pas forcé d'utiliser leur système de gestion si vous ne voulez pas.

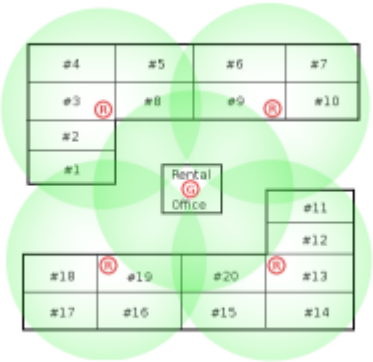
Contrairement à Meraki et FON leur architecture est 100% open source. Vous pouvez flasher le firmware si vous voulez, mettre une nouvelle page d'accueil ou utiliser leur logiciel libre de gestion (voir ci-dessous)… ou pas.



Les [petits mini-routeurs] (49$) sont livrés pré-flashés avec [ROBIN], le firmware open source de maillage. Vous n'avez qu'à le brancher et il est prêt à l'emploi. Pas de configuration requise.

Vous en branchez un sur votre connexion Internet et rajoutez d'autres mini-routeurs là où vous voulez étendre la couverture Wifi (chaque routeur devrait être situé à moins de 30 mètres d'un autre routeur). Ils marchent bien avec Covad parce que Covad supporte le partage du Wifi mais d'autres fournisseurs d'accès sont également compatibles. Open-Mesh n'a aucun lien commercial avec les fournisseurs d'accès Internet.

Le routeur est livré avec une antenne 2dbi et un câble ethernet pour le connecter à votre ligne xDSL ou à votre ordinateur. Le chipset Atheros utilisé est le même que dans le Meraki.



ROBIN (ROuting Batman INside) est un projet de maillage de réseau open source déployé par dessus OpenWRT. Il utilise l'algorithme de routage BATMAN (Better Approach to Mobile Ad-hoc Networking) pour les réseaux maillés ad-hoc multi-sauts.

Quel est le modèle économique d'Open-Mesh ?

« Nous n'essayons pas de nous enrichir », répondait Michael Burmeister-Brown lors d'un entretien téléphonique avec DailyWireless. « Nous espérons que d'autres entreprises et d'autres constructeurs utiliseront le logiciel open-source ROBIN dans leur matériel » explique-t-il.

La mission d'Open-Mesh est d'aider le sans-fil communautaire, l'éducation et les pays émergents à utiliser les réseaux sans fils maillés open-source. Simple. Bon marché. Sans publicité. A monter soi-même.

Douce équité. L'heure est peut être venue pour cette idée.

Notes

[1] Merci à Olivier, Daria et Siltaar pour la traduction Framalang