Le chiffrement, maintenant (5)

Un service de chat *furtif* : Off-the-Record (OTR)

Traduction : Feadurn, Paul, lamessen, goofy

Off-the-Record (OTR) est une couche de chiffrement qui peut être ajoutée à n'importe quel système de messagerie instantanée existant, pourvu que vous puissiez vous connecter à cette messagerie instantanée avec un client qui prend en charge l'OTR, comme Pidgin ou Adium. Avec OTR, il est possible d'avoir des conversations sécurisées, chiffrées de bout en bout, en passant par des services comme Google Talk ou Facebook sans que ni Facebook ni Google n'aient accès au contenu de ces conversations. Notez bien que c'est un système différent de l'option « off the record » de Google, qui n'est pas sécurisée. Et souvenez-vous : bien qu'une connexion HTTPS avec Google ou Facebook offre une très bonne protection à vos messages quand ils circulent, les deux services ont les clés de vos échanges et peuvent donc les communiquer aux autorités.

OTR remplit deux missions : le chiffrement des conversations de messagerie instantanée en temps réel et la vérification de l'identité des personnes avec lesquelles vous communiquez. Cette dernière est extrêmement importante mais beaucoup d'utilisateurs d'OTR la négligent. Même si OTR est bien plus facile à prendre en main que d'autres formes de chiffrement à clé publique, vous devez malgré tout en comprendre le fonctionnement et savoir à quelles attaques il peut être exposé si vous souhaitez l'utiliser en toute sécurité.

Fournisseurs de services et Jabber

OTR assure uniquement le chiffrement du contenu de vos conversations et non celui des métadonnées qui leur sont associées. Celles-ci comprennent vos interlocuteurs, quand et à quelle fréquence vous communiquez avec eux. C'est la raison pour laquelle je recommande d'utiliser un service qui n'est pas connu pour collaborer avec les services secrets. Cela ne protègera pas forcément vos métadonnées, mais vous aurez au moins une chance qu'elles restent privées.

Je vous conseille aussi d'utiliser un service XMPP (aussi appelé Jabber). Tout comme le courrier électronique, Jabber est un protocole ouvert et fédéré. Les utilisateurs d'un service Jabber comme riseup.net peuvent discuter tant avec des utilisateurs du service jabber.ccc.de qu'avec ceux du service jabber.org.

Clients OTR

Pour utiliser OTR, vous devrez télécharger un logiciel. Sous Windows, vous téléchargerez et installerez Pidgin et le plugin OTR séparément. Sous GNU/Linux, vous installerez les paquets pidgin et pidgin-otr. La documentation explique comment configurer vos comptes Pidgin avec OTR. Si vous êtes sous Mac OS X, vous pouvez télécharger et installer Adium, un client de chat libre qui intègre le support d'OTR. Là aussi, reportez vous à la documentation officielle pour configurer le chiffrement OTR avec Adium. Il existe aussi des clients Jabber et OTR disponibles pour Android (Giggerbot) et pour iOS (ChatSecure).

Votre clé

Quand vous commencez à utiliser OTR, votre client de chat génère une clé de chiffrement et la stocke dans un fichier de votre répertoire utilisateur personnel sur votre disque dur. Si votre ordinateur ou votre smartphone est perdu, volé ou rendu inutilisable par un logiciel malveillant, il est possible que l'inviolabilité de votre clé OTR soit compromise. Si c'est le cas, un attaquant aura la possibilité de prendre le contrôle de votre serveur Jabber et de lancer une attaque de l'homme du milieu (MIDTM) contre vous pendant que vous discutez avec des interlocuteurs qui avaient auparavant vérifié votre identité.

Sessions

Si vous souhaitez utiliser OTR pour discuter en privé avec vos amis, ces derniers doivent l'utiliser également. Une session chiffrée entre deux personnes nécessite deux clés de chiffrement. Par exemple, si vous-même et votre correspondant vous êtes tous deux identifiés sur le chat de Facebook en utilisant Adium ou Pidgin après avoir configuré OTR, vous pourrez discuter en privé. En revanche, si vous vous êtes logué en messagerie instantanée en utilisant Adium ou Pidgin mais que votre interlocuteur discute en utilisant directement facebook.com, vous ne pouvez pas avoir de conversation chiffrée.

Si vous souhaitez utiliser les services de Facebook ou Google pour discuter avec vos amis, je vous recommande de désactiver le chat de l'interface web pour ces services et de n'utiliser qu'Adium ou Pidgin pour vous connecter, et d'encourager vos amis à faire de même ; voici la marche à suivre pour Facebook et Google.

Quand vous lancez une session chiffrée avec OTR, votre logiciel client vous indique quelque chose comme :

```
Lancement d'une conversation privée avec utilisateur@jabberservice... Conversation non-vérifiée avec utilisateur@jabberservice/démarrage du client chat.
```

Si vous avez déjà vérifié l'empreinte OTR de la personne à laquelle vous parlez (voir plus bas), votre session ressemblera à ceci :

```
Lancement d'une conversation privée avec utilisateur@jabberservice... Conversation privée avec utilisateur@jabberservice/démarrage du client chat.
```

Quand vous commencez une nouvelle session OTR, votre logiciel OTR et celui de votre correspondant s'échangent une série de messages pour s'accorder sur une clé pour la nouvelle session. Cette clé temporaire n'est connue que par vos deux clients de messagerie instantanée, ne circule jamais sur Internet et sert à chiffrer et déchiffrer les messages. Une fois la session terminée, les deux logiciels clients « oublient » la clé. Si vous recommencez à chatter plus tard avec la même personne, votre client OTR génèrera une nouvelle clé de session.

De cette façon, même si une personne indiscrète enregistre toutes vos conversations chiffrées — ce que la NSA pense être légalement autorisée à faire même si vous êtes un citoyen étatsunien et qu'elle n'a pas un mandat ou une bonne raison de le faire — et que plus tard elle compromet votre clé OTR, elle ne pourra pas retrouver ni déchiffrer vos anciennes conversations.

Cette propriété est appelée sécurité *itérative*, et c'est une particularité d'OTR dont PGP ne dispose pas. Si votre clé PGP privée (article à venir sur les clés PGP) est compromise et que l'attaquant a eu accès à tous les messages chiffrés que vous avez reçus, il peut les retrouver et en déchiffrer l'intégralité.

Apprenez-en davantage sur la façon dont fonctionne la sécurité itérative, et la raison pour laquelle la majorité des grandes sociétés d'Internet devraient

l'adopter pour leurs site web ici. La bonne nouvelle, c'est que Google utilise déjà la sécurité itérative et que Facebook va l'implémenter dès que possible.

Vérification d'empreinte OTR

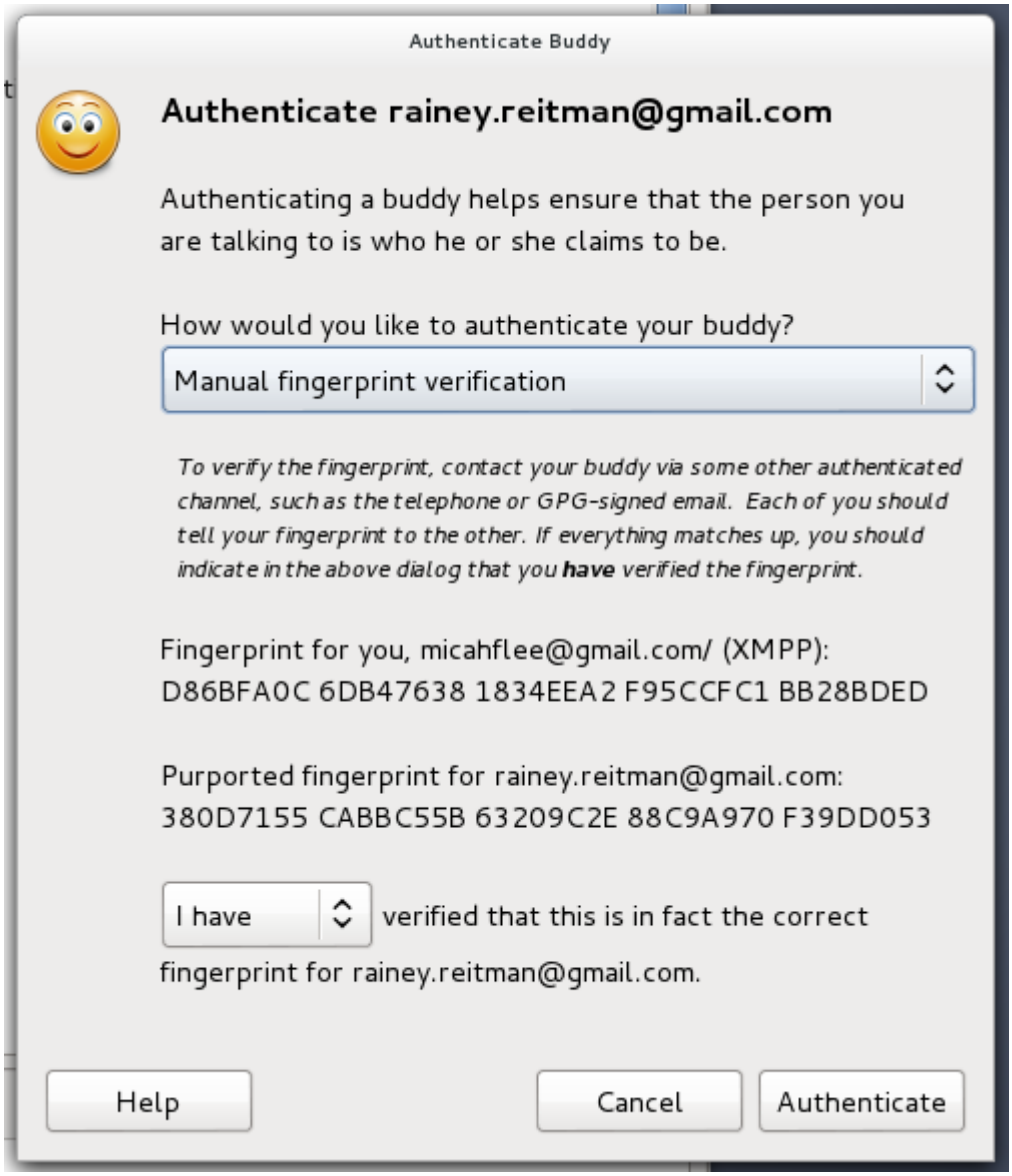
Quand vous commencez une nouvelle session OTR avec quelqu'un, votre logiciel de chat reçoit une empreinte[1] de sa clé de chiffrement et votre logiciel OTR se souvient de cette empreinte. Aussi longtemps que la personne utilise la même clé de chiffrement lorsqu'elle communique avec vous, probablement parce qu'elle utilise le même logiciel/client(?), elle aura la même empreinte. Si cette empreinte change, c'est soit parce que la personne utilise une clé OTR différente, soit que vous êtes tous deux victimes d'une attaque MITM.

Sans cette vérification de clés, vous n'avez aucun moyen de savoir si vous êtes victime d'une attaque MITM réussie et non détectée.

Même en étant sûr que la personne avec qui vous discutez est réellement votre interlocuteur, parce qu'elle connaît des choses qu'elle seule peut connaitre, et en utilisant un chiffrement OTR, un attaquant peut être en train de lire votre conversation. Peut-être avez vous en réalité une conversation chiffrée avec l'attaquant, lui-même en pleine conversation chiffrée avec votre interlocuteur, relayant les messages entre vous et ce dernier. Au lieu de l'empreinte de votre interlocuteur, votre client verra celle de l'attaquant. Tout ce que vous pouvez constater en tant qu'utilisateur est que la conversation est « non vérifiée ».

Les captures d'écran suivantes montrent les indications visuelles de Pidgin concernant la vérification de l'empreinte. Si vous avez vérifié l'empreinte OTR, votre discussion est privée : dans le cas contraire, votre conversation est chiffrée mais rien ne garantit que vous n'êtes pas en train de subir une attaque. Vous ne pouvez en avoir la certitude absolue qu'à condition de vérifier.

Si vous cliquez sur un lien non vérifié (sur Adium c'est une icône de cadenas), vous pouvez choisir « authentifier l'ami ». Le protocole OTR propose trois méthodes de vérification : le protocole du millionnaire socialiste, le secret partagé et la vérification manuelle de l'empreinte. Tous les clients OTR permettent la vérification manuelle de l'empreinte, mais pas forcément les autres types de vérification. Dans le doute, choisissez la vérification manuelle de l'empreinte.



Dans la capture d'écran ci-dessus, on voit l'empreinte OTR des deux utilisateurs de la session. Votre interlocuteur doit voir exactement les mêmes empreintes que vous. Pour être certain que chacun des interlocuteurs voit les mêmes empreintes, vous devez soit vous rencontrer en personne, soit avoir un échange téléphonique (si vous pouvez reconnaitre vos voix) soit trouver une autre solution en-hors du chat mais sécurisée pour vérifier les empreintes, comme envoyer un courriel PGP chiffré et signé.

Les empreintes OTR sont constituées d'une suite de 40 caractères hexadécimaux. Il est statistiquement impossible de générer deux clés OTR ayant la même empreinte, ce qui est appelé une collision. Il est toutefois possible de générer une clé OTR qui, sans être véritablement une collision, semble en être une lors d'une vérification superficielle. Par exemple, les premiers et derniers caractères peuvent identiques et les caractères centraux différents. Il est donc important de comparer chacun des 40 caractères un à un pour être sûr d'avoir la bonne clé

OTR.

Comme, en général, vous créez une nouvelle clé OTR chaque fois que vous utilisez un nouveau terminal (par ex., si vous voulez utiliser le même compte Jabber pour discuter à partir de votre téléphone Android avec Gibberbot et à partir de votre PC Windows avec Pidgin), vous vous retrouvez souvent avec plusieurs clés et, par conséquent, plusieurs empreintes. Il est important de répéter l'étape de vérification sur chaque terminal et pour chaque contact avec qui vous discutez.

Utiliser OTR sans vérifier les empreintes est toujours préférable à ne pas utiliser OTR du tout. Comme un attaquant qui tente une attaque MITM contre une session OTR court un risque important d'être pris, cette attaque n'est utilisée qu'avec prudence.

Journaux d'activité

Voici un extrait d'un des journaux de discussion entre Bradley Manning et Adrian Lamo, transmis aux autorités par ce dernier et publié par Wired.

(1:40:51 PM) bradass87 n'a pas encore été identifié. Vous devez authentifier cet utilisateur.

(1:40:51 PM) une conversation non vérifiée avec bradass87 a commencé.

(1:41:12 PM) bradass87: Salut

(1:44:04 PM) bradass87: Comment vas-tu?

(1:47:01 PM) bradass87: je suis analyste du renseignement à l'armée, à l'est de Bagdad et dans l'attente d'une décharge pour « trouble de l'adaptation » au lieu de « trouble de l'identité de genre ».

(1:56:24 PM) bradass87: Je suis sûr que tu es très occupé... Tu dois avoir plein de boulot...

(1:58:31 PM) bradass87: Si tu avais un accès privilégié à des réseaux classifiés 14 heures par jour, 7 jours sur 7 et plus de 8 mois dans l'année, que ferais-tu ?

(1:58:31 PM) info@adrianlamo.com: je suis fatigué d'être fatigué

(2:17:29 PM) bradass87: ?

(6:07:29 PM) info@adrianlamo.com: Quel est ton MOS[2]

Comme on peut le voir grâce à la ligne « une conversation non vérifiée avec bradass87 a commencé », les deux interlocuteurs utilisaient OTR pour chiffrer leur conversation, or cette dernière a été en définitive rendue publique sur le site web de Wired et utilisée comme pièce à conviction contre Bradley Manning. Il est possible que leur conversation ait fait l'objet d'une attaque MITM, mais c'est très improbable. Ce sont plutôt les clients OTR de Bradley Manning et Adian Lamo qui conservaient une copie de leur conversation sur leur disque dur, non chiffré.

Même s'il peut parfois être utile de garder des journaux de conversations, cela peut aussi gravement mettre en danger votre vie privée. Si Pidgin et Adium ne journalisaient pas les conversations par défaut, il est probable que ces journaux de conversations n'auraient pas fini sur la place publique.

Avec la sortie d'OTR 4.0 en septembre 2012, Pidgin a arrêté de journaliser les conversations OTR par défaut. Adium continue de le faire. Vous devez donc manuellement arrêter cette journalisation, ce qui est une faille d'Adium. Adium étant un logiciel libre avec un système ouvert de suivi de bogues, vous pouvez suivre et participer aux discussions concernant la résolution de cette faille ici et là.

(à suivre…)

Notes

[1] rien à voir avec les empreintes digitales que certains confient à leur iPhone

[2] Military Occupation Speciality, la classification des activités au sein de l'armée des États-Unis.