Groupe de travail Réseau
Request for Comments : 2804
Catégorie : Information

IAB & IESG
mai 2000
Traduction Claude Brière de L'Isle

Politique de l'IESG en matière d'écoutes

Résumé
Il a été demandé à l'équipe d'ingénierie de l'Internet (IETF, *Internet Engineering Task Force*) de prendre position sur l'inclusion, dans les documents en cours de normalisation de l'IETF, de fonctionnalités conçues pour faciliter les écoutes.

Le présent mémoire explique ce que l'IETF pense de la signification de la question, pourquoi sa réponse est "non", et ce que signifie cette réponse.

1. Résumé de la position

L'IETF a décidé de ne pas prendre en considération les exigences des écoutes au titre du processus de création et de maintenance des normes de l'IETF.

Elle prend cette position pour les raisons de base suivantes :

- L'IETF, organisme de normalisation international, pense qu'elle n'est pas le bon forum pour concevoir un protocole ou des caractéristiques d'équipement qui répondent à des besoins résultant des lois des différents pays, parce que ces lois varient largement à travers les zones où sont déployées les normes de l'IETF. Les organismes dont le domaine d'autorité correspond à un seul régime de juridiction sont plus appropriés pour cette tâche.

- L'IETF établit des normes pour les communications qui passent à travers des réseaux qui peuvent appartenir, être gérés et entretenus par des gens relevant de nombreuses juridictions avec de nombreuses exigences de confidentialité. Vu ces exigences potentiellement divergentes, l'IETF estime que le fonctionnement de l'Internet et les besoins de ses utilisateurs sont mieux servis en s'assurant que les propriétés de sécurité des connexions à travers l'Internet sont aussi bien connues que possible. Dans l'état actuel de nos connaissances cela signifie de les rendre aussi libres que possible à l'égard des pièges pour la sécurité.

- L'IETF estime que dans le cas du trafic qui passe aujourd'hui à travers l'Internet sans être protégé par les systèmes d'extrémité (par chiffrement ou par d'autres moyens) l'utilisation des caractéristiques existantes du réseau, si elles sont déployées intelligemment, fournissent de nombreuses opportunités d'écoute, et devraient être suffisantes pour les exigences de nombre des cas qu'on peut voir présentement. L'IETF ne voit pas de solution d'ingénierie qui permette de telles écoutes lorsque les systèmes d'extrémité prennent les mesures adéquates pour protéger leurs communications.

- L'IETF estime que l'ajout d'une exigence d'écoute rendrait la conception des protocoles affectés considérablement plus complexe. L'expérience a montré que la complexité compromet presque inévitablement la sécurité des communications même lorsque elles ne sont pas enregistrées par des moyens légaux ; il y a aussi des risques évidents soulevés par la nécessité de protéger l'accès au système d'écoute. Ceci entre en conflit avec l'objectif de liberté à l'égard des pièges pour la sécurité.

- L'IETF réaffirme qu'elle croît fermement, comme elle le déclare de façon plus détaillée dans la [RFC1984], que le développement commercial de l'Internet et une confidentialité adéquate pour ses usagers contre les intrusions illégales exigent une large disponibilité d'une forte technologie cryptographique.

- D'un autre côté, l'IETF estime que les mécanismes conçus pour faciliter ou permettre les écoutes, ou les méthodes d'utilisation d'autres facilités à de telles fins, devraient être décrites ouvertement, afin d'assurer la révision maximum des mécanismes et s'assurer qu'ils adhèrent d'aussi près que possible aux contraintes de leur conception. L'IETF estime que la

publication de tels mécanismes, et la publication des faiblesses connues de tels mécanismes, est une bonne chose.

2. Le processus Raven

La question que l'IETF travaille sur les technologies d'interception légale est apparue comme sous produit des travaux intensifs que fait maintenant l'IETF dans le domaine de la téléphonie fondée sur IP.

Dans le monde du téléphone, il y a une tradition de coopération (souvent obligatoire selon la loi) entre les agences d'application de la loi et les opérateurs d'équipement de téléphone en matière d'écoutes, conduisant les entreprises qui construisent les équipements de téléphonie à ajouter les dispositifs d'écoute à leurs équipements, et un consensus est apparu dans l'industrie sur la façon de construire et gérer de tels dispositifs. Certaines organisations traditionnelles de normalisation de la téléphonie ont soutenu cela en ajoutant des dispositifs d'interception à leurs normes sur la téléphonie.

Comme l'avenir du téléphone semble être intimement lié à l'Internet, il est inévitable que la principale organisation de normalisation de l'Internet se trouve confrontée à cette question un jour ou l'autre.

Dans ce cas, certains des participants à un groupe de travail de l'IETF travaillant sur une nouvelle norme pour les communications entre des composants d'un commutateur téléphonique réparti ont soulevé la question. Comme l'ajout de dispositifs de ce type aurait été quelque chose que l'IETF n'avait jamais fait auparavant, les dirigeants de l'IETF ont décidé d'avoir une discussion publique avant de décider si le groupe de travail devrait continuer sur cette voie. Une nouvelle liste de diffusion a été créée (la liste de diffusion Raven, voir http://www.ietf.org/mailman/listinfo/raven) pour cette discussion. Près de 500 personnes se sont abonnées à la liste et environ 10 % d'entre elles ont envoyé au moins un message à la liste. La discussion sur cette liste a précédé une discussion qui a eu lieu à la plénière de l'IETF de Washington, D.C.

Vingt neuf personnes ont pris la parole durant la session plénière. Les opinions allaient du libertaire : "les gouvernements n'ont aucun droit à l'écoute" - au pragmatique : "cela sera fait quelque part, le mieux est de le faire là où la technologie a été développée". À la fin de la discussion, il y a eu un vote à main levée pour indiquer les opinions : l'IETF devrait elle ajouter des dispositifs spéciaux, ne pas le faire, ou abstention. Très peu de personnes se sont prononcées fortement en faveur de l'ajout des dispositifs d'interception, tandis que beaucoup ont plaidé contre, mais une portion notable de l'audience a refusé de prendre position (ont levé la main pour "abstention" dans le vote à main levée).

C'est sur ces bases que le groupe de pilotage de l'ingénierie de l'Internet (IESG, *Internet Engineering Steering Group*) et le Bureau de l'architecture de l'Internet (IAB, *Internet Architecture Board*) ont été saisis pour formuler une politique.

3. Définition de l'écoute

Les divers statuts légaux qui définissent l'écoute ne donnent pas de définitions adéquates pour distinguer les écoutes de diverses autres activités au niveau technique. Pour les besoins du présent mémoire, on utilise la définition suivante de l'écoute :

L'écoute est ce qui se produit lorsque des informations passées sur l'Internet d'un usager à un ou plusieurs autres usagers sont livrées à un tiers :

1. sans que l'envoyeur ait connaissance de la présence du tiers,
2. sans qu'aucun des receveurs ait connaissance de la livraison au tiers,
3. lorsque les attentes normales de l'envoyeur sont que les informations ne soient vues que par les receveurs ou des usagers obligés de garder confidentielles les informations,
4. lorsque le tiers agit délibérément pour cibler la transmission du premier usager, soit parce qu'il s'y intéresse, soit parce qu'il s'intéresse à la réception du second usager.

Le terme "tiers", tel qu'utilisé ici, peut se référer à une personne, à un groupe de personnes, ou à un équipement agissant au nom de personnes ; le terme "tiers" est utilisé pour faire court.

Bien sûr, de nombreuses écoutes seront bidirectionnelles, surveillant le trafic envoyé par deux usagers ou plus les uns aux autres.

Donc, par exemple, surveiller des groupes de nouvelles publics n'est pas une écoute (la condition 3 est violée), la surveillance aléatoire d'une large population n'est pas une écoute (la condition 4 est violée), un receveur qui transfère un message électronique privé n'est pas une écoute (la condition 2 est violée).

Un équivalent Internet du traçage d'appel au moyen des enregistrements d'identification de compte (parfois appelés des "enregistreurs graphiques") qui sont un dispositif du réseau téléphonique est aussi de l'écoute selon cette définition, car l'attente

normale de l'envoyeur est que l'entreprise qui fait l'identification gardera cette information confidentielle.

L'écoute peut être vue comme trois étapes logiques distinctes :
- Capture – collecter sur le réseau les informations voulues.
- Filtrage – choisir les informations voulues parmi les informations collectées par accident.
- Livraison – transmettre les informations voulues à celui qui les veut.

Le terme s'applique au processus complet ; par exemple, une surveillance aléatoire suivie par un filtrage pour extraire les informations sur un plus petit groupe d'usagers serait de l'écoute, selon cette définition.

Dans toutes ces étapes existe la possibilité d'utiliser ou d'abuser des mécanismes définis à cette fin pour d'autres objectifs.

Cette définition n'inclut délibérément pas les considérations :
- du caractère légal ou non de l'écoute, car c'est une question juridique, non technique ;
- si l'écoute survient en temps réel, ou peut être effectuée après coup en cherchant dans les informations enregistrées à d'autres fins (comme dans l'exemple de la comptabilité donné plus haut) ;
- quel est le support ciblé par l'écoute – que ce soit la messagerie électronique, la téléphonie IP, la navigation sur la Toile, ou des transferts de données électroniques.

On estime que ces questions ne sont pas pertinentes pour la politique présentée dans le présent mémoire.

L'écoute est parfois aussi appelée "interception", mais ce terme est aussi utilisé dans un sens qui est considéré comme plus large que celui de la surveillance des données qui passent sur les réseaux, et il n'est donc pas utilisé ici.

4. Pourquoi l'IETF ne prend elle pas une position morale

Une grande partie des débats sur les écoutes se sont concentrées sur la question du caractère contraire à la morale de l'écoute, quel que soit celui qui la pratique, nécessaire dans toute société civilisée, ou un outil efficace pour arrêter des criminels qui ont sévi dans le passé et vont recommencer.

L'IETF a décidé de ne pas prendre position sur cette question, car :
- il n'y a pas de consensus clair sur une position unique dans l'IETF,
- il n'y a pas de moyen de détecter la moralité d'un acte "sur le réseau". Comme l'IETF traite de la normalisation des protocoles, et pas du déploiement des protocoles, elle n'est pas en position de décider si ses produits ne sont utilisés de que façon morale ou légale.

Cependant, on peut faire quelques observations :
- L'expérience montre que les outils qui sont efficaces pour un objet tendent à être utilisés pour cet objet.
- L'expérience montre que les outils conçus pour un objet et sont efficaces pour un autre tendent à être utilisés aussi pour cet autre objet, quelles que soient les intentions de ses concepteurs.
- L'expérience montre que si une vulnérabilité existe dans un système de sécurité, il est probable que quelqu'un en tirera parti tôt ou tard.
- L'expérience montre que les facteurs humains, non technologiques en eux-mêmes, sont la principale source de telles vulnérabilités.

Il en résulte que si il existe des outils efficaces pour les écoutes, il est probable qu'ils seront utilisés comme ils ont été conçus, pour des objets légaux dans leur juridiction, et aussi de façons pour lesquels ils n'étaient pas destinés, dans des façons qui ne sont pas légales dans cette juridiction. Lorsque on pèse le pour et le contre du développement ou du déploiement de tels outils, on devrait garder cela présent à l'esprit.

5. Considérations d'utilité

Lors de la conception de toute fonction de communications, il est pertinent de se demander si de telles fonctions effectuent de façon efficace les tâches pour lesquelles elles sont conçues, ou si le travail consacré à leur développement ne vaut pas les avantages qu'elles procurent.

Étant donné qu'il n'y a pas de proposition spécifique en cours de développement à l'IETF, l'IETF ne peut pas soupeser les avantages et inconvénients des propositions d'écoutes directement de cette manière.

Cependant, comme ci-dessus, on peut faire quelques observations générales :

- Les écoutes par copie des octets qui passent entre deux utilisateurs de l'Internet avec des points de rattachement statiques connus ne présentent pas de difficulté. Les fonctions standard conçues à des fins de diagnostic peuvent très bien faire cela.
- Corréler les identités des usagers avec ces points de rattachement à l'Internet peut être significativement plus dur, mais pas impossible, si l'usager utilise les moyens standard d'identification. Cependant, cela signifie de relier de nombreux sous systèmes de l'Internet utilisés pour l'allocation d'adresse, la résolution des noms et ainsi de suite ; ceci n'est pas trivial.
- Un adversaire a plusieurs contre-mesures simples disponibles pour contrer les tentatives d'écoute, même sans recourir au chiffrement. Cela inclut les cafés Internet et les téléphones anonymes, les messageries anonymes, les sessions de connexion multi bonds, et l'utilisation de supports de communications obscurs ; tous ces outils sont bien connus de la communauté des craqueurs de système.
- Bien sûr, les communications où le contenu est protégé par un chiffrement fort peuvent être facilement enregistrés, mais le contenu n'est pas disponible à celui qui écoute, contrant toute collecte d'informations en dehors de l'analyse du trafic. Comme les données de l'Internet sont déjà sous forme numérique, leur chiffrement est très simple pour l'utilisateur final.

Tout cela mis bout à bout signifie que bien que les écoutes soient un outil efficace dans des situations où la cible d'une écoute est soit ignorante, soit se croit innocente de tout mal, l'écoute fondée sur l'Internet est un outil moins utile que ce qu'on pourrait imaginer contre un adversaire en alerte et techniquement compétent.

6. Considérations pour la sécurité

Les écoutes, par définition (voir plus haut) livrent des informations que celui qui les envoie ne s'attend pas à voir divulguer.

Cela signifie qu'un système qui permet les écoutes doit contenir une fonction qui puisse s'exercer sans alerter l'envoyeur des informations du fait que son désir de confidentialité n'est pas satisfait.

Ceci, à son tour, signifie qu'on doit concevoir le système d'une façon telle qu'il ne puisse pas garantir un niveau de confidentialité ; au maximum, il peut seulement le garantir tant que la fonction d'écoute n'est pas exercée.

Par exemple, les conférences téléphoniques chiffrées ont été conçues de façon telle que les participants ne puissent pas savoir à qui le matériel de chiffrement partagé a été révélé. Cela signifie :
- que le système est moins sûr qu'il aurait pu l'être si cette fonction n'était pas présente,
- que le système est plus complexe qu'il aurait pu l'être si cette fonction n'était pas présente,
- étant plus complexe, le risque de fautes involontaires de sécurité dans le système est plus fort.

Les écoutes, même lorsque elles ne sont pas pratiquées, diminuent donc la sécurité du système.

7. Remerciements

Le présent mémoire est approuvé par l'IAB et l'IESG. Leurs membres sont :

Pour l'IAB : Harald Alvestrand, Randall Atkinson, Rob Austein, Brian Carpenter, Steve Bellovin, Jon Crowcroft, Steve Deering, Ned Freed, Tony Hain, Tim Howes, Geoff Huston, John Klensin.

Pour l'IESG : Fred Baker, Keith Moore, Patrik Falstrom, Erik Nordmark, Thomas Narten, Randy Bush, Bert Wijnen, Rob Coltun, Dave Oran, Jeff Schiller, Marcus Leech, Scott Bradner, Vern Paxson, April Marine.

Le nombre des contributeurs à la discussion est trop élevé pour en faire la liste.

8. Adresse de l'auteur

Le présent mémoire a été rédigé par l'IAB et l'IESG.

Les présidents en sont :

Fred Baker, IETF Chair
519 Lado Drive
Santa Barbara California 93111
téléphone : 408-526-4257
mél : fred@cisco.com

Brian E. Carpenter, IAB Chair
IBM
c/o iCAIR
Suite 150
1890 Maple Avenue
Evanston IL 60201
USA
mél : brian@icair.org

9. Références

[RFC1984] IAB, IESG, "Déclaration IAB IESG sur la technologie cryptographique dans l'Internet", août 1996. *(Info.)*

10. Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par l'Internet Society.