Équipe d'ingénierie de l'Internet (IETF)
Request for Comments : 7258
BCP 188
Catégorie : Bonnes pratiques actuelles
ISSN : 2070-1721

S. Farrell, Trinity College Dublin
H. Tschofenig, ARM Ltd.

mai 2014
Traduction Claude Brière de L'Isle

La surveillance envahissante est une attaque

Résumé
La surveillance envahissante est une attaque technique qui devrait être combattue dans la conception des protocoles de l'IETF, lorsque possible.

Statut de ce mémoire
Le présent mémoire documente les bonnes pratiques actuelles de l'Internet.

Le présent document a été produit par l'équipe d'ingénierie de l'Internet (IETF). Il représente le consensus de la communauté de l'IETF. Il a subi une révision publique et sa publication a été approuvée par le groupe de pilotage de l'ingénierie de l'Internet (IESG). Plus d'informations sur les normes de l'Internet sont disponibles à la Section 2 de la [RFC5741].

Les informations sur le statut actuel du présent document, tout errata, et comment fournir des réactions sur lui peuvent être obtenues à http://www.rfc-editor.org/info/rfc7258

1. La surveillance envahissante est une attaque à grande échelle contre la vie privée

La surveillance envahissante (PM, *Pervasive Monitoring*) est une surveillance largement répandue (et souvent cachée) au moyen du rassemblement intrusif d'objets de protocole, incluant du contenu d'applications, ou des métadonnées de protocole comme les en-têtes. La mise sur écoute active ou passive et l'analyse du trafic, (par exemple, des corrélations, des mesures de durées ou de taille de paquet) ou la subversion des clés de chiffrement utilisées pour sécuriser les protocoles peuvent aussi être utilisées au titre de la surveillance envahissante. La PM se distingue par son caractère non discriminatoire et à très grande échelle, plutôt qu'en introduisant de nouveaux types de compromission technique.

L'évaluation technique de la communauté de l'IETF est que la PM est une attaque contre la vie privée des utilisateurs et des organisations de l'Internet. La communauté de l'IETF a exprimé un fort consensus que la PM est une attaque qui doit être combattue lorsque possible, via la conception de protocoles qui rendent la PM significativement plus coûteuse, ou infaisable. La surveillance envahissante a été discutée à la réunion technique plénière de novembre 2013 de l'IETF [IETF88P] et ensuite par de larges échanges sur les listes de diffusion de l'IETF. Le présent document note le consensus de la communauté de l'IETF et établit la nature technique de la PM.

Le terme "attaque" est utilisé ici dans un sens technique qui diffère un peu de l'usage du français courant, dans lequel une attaque est une action agressive perpétrée par un opposant, destinée à appliquer la volonté de l'opposant sur la partie attaquée. Le terme est utilisé ici pour se référer au comportement qui subvertit l'intention des parties communicantes sans l'accord de ces parties. Une attaque peut changer le contenu de la communication, enregistrer le contenu ou les caractéristiques externes de la communication, ou par corrélation avec d'autres événements de communication, révéler des informations que les parties n'avaient pas l'intention de révéler. Elle peut aussi avoir d'autres effets qui subvertissent de façon similaire l'intention d'un communicant. La [RFC4949] contient une définition plus complète pour le terme "attaque". On utilise aussi ici le terme au singulier, même si dans la réalité la PM peut consister en un ensemble multi faces d'attaques coordonnées.

En particulier, le terme "attaque", dans son sens technique, n'a pas d'implication sur la motivation de l'acteur qui monte

l'attaque. Les motivations de la PM vont de la surveillance non ciblée de l'état de la nation, aux entreprises légales mais qui portent atteinte à la vie privée dans un but commercial, jusqu'aux actions illégales de criminels. Les mêmes techniques pour réaliser la PM peuvent être utilisées sans considération de motivation. Donc, on ne peut pas se défendre contre les plus abominables acteurs tout en permettant la surveillance par d'autres acteurs quelle que soit la bienveillance avec laquelle certains puissent les considérer, car les actions requises de l'attaquant ne peuvent pas être distinguées des autres attaques. La motivation de la PM est donc sans pertinence pour la façon dont la PM peut être atténuée dans les protocoles de l'IETF.

2. L'IETF travaillera à atténuer la surveillance envahissante

"Atténuation" est un terme technique qui n'implique pas la capacité d'empêcher complètement ou déjouer une attaque. Les protocoles qui atténuent la PM ne vont pas empêcher l'attaque mais peuvent significativement changer la menace. (Voir le diagramme sous l'entrée "$ attaque" à la page 12 de la RFC 4949 sur la relation entre les termes "attaque" et "menace".) Cela peut augmenter significativement le coût de l'attaque, forcer ce qui était caché à être révélé, ou à faire que l'attaque soit plus probablement détectée, éventuellement à retardement.

Les normes de l'IETF fournissent déjà des mécanismes pour protéger les communications Internet et il y a des directives [RFC3552] pour les appliquer dans la conception des protocoles. Mais ces normes ne visent généralement pas la PM, la confidentialité des métadonnées de protocole, l'opposition à l'analyse de trafic, ou la minimisation des données. Dans tous les cas, il va rester des informations qui touchent à la vie privée qui sont inévitablement divulguées par les protocoles. Avec les avancées de la technologie, des techniques qui n'étaient disponibles qu'à des acteurs ayant de gros moyens financiers deviennent plus largement accessibles. Atténuer la PM est donc une protection contre une large gamme d'attaques similaires.

Il est donc grand temps de revisiter les propriétés de sécurité et de confidentialité de nos normes. L'IETF va travailler à atténuer les aspects techniques de la PM, tout comme nous le faisons pour les vulnérabilités des protocoles en général. Les façons dont les protocoles de l'IETF atténuent la PM vont changer au fil du temps avec l'évolution des techniques d'atténuation et d'attaque, et elles ne sont donc pas décrites ici.

Ceux qui développent les spécifications de l'IETF doivent être capables de décrire comment ils ont considéré la PM, et, si l'attaque relève du travail à publier, être capables de justifier les décisions de conception qui s'y rapportent. Cela ne doit pas vouloir dire qu'une nouvelle section "Considérations sur la surveillance envahissante" est nécessaire dans la documentation de l'IETF. Cela signifie que, si on le demande, il faut qu'il y ait une bonne réponse à la question "la surveillance envahissante est elle une question pertinente dans ce travail et si oui, comment est elle considérée ?"

En particulier, les décisions architecturales, y compris quelle technologie existante est réutilisée, peuvent avoir un impact significatif sur la vulnérabilité d'un protocole à la PM. Ceux qui développent les spécifications de l'IETF doivent donc envisager d'atténuer la PM lorsque ils prennent des décisions d'architecture. Faire une revue adéquate et précoce des décisions d'architecture, incluant de savoir si une atténuation appropriée de la PM peut être faite est important. Revisiter ces décisions d'architecture plus tard dans le processus est très coûteux.

Alors que la PM est une attaque, d'autres formes de surveillance qui peuvent entrer sous la définition de la PM peuvent être bénéfiques et ne faire partie d'aucune attaque, par exemple, les fonctions de surveillance du réseau surveillent les paquets ou flux, et les mécanismes de défense contre les pourriels doivent voir le contenu des messages électroniques. Une certaine surveillance peut même faire partie de l'atténuation de la PM, par exemple, la transparence de certificat [RFC6962] implique de surveiller l'infrastructure de clés publiques selon des moyens qui pourraient détecter certaines techniques d'attaque de PM. Cependant, il y a un clair potentiel que les mécanismes de surveillance soient détournés pour la PM, de sorte que cette situation doit être l'objet d'une considération attentive dans la conception des protocoles. Rendre les réseaux ingérables pour atténuer la PM n'est pas un résultat acceptable, mais ignorer la PM irait à l'encontre du consensus documenté ici. Un équilibre approprié va émerger au fil du temps lorsque les enjeu réels de cette tension seront pris en considération.

Finalement, l'IETF, en tant qu'organisation de développement de normes, ne contrôle pas la mise en œuvre ou le déploiement de ses spécifications (bien que les participants à l'IETF soient les acteurs du développement de nombreuses mises en œuvre) pas plus que l'IETF ne normalise toutes les couches de la pile de protocoles. De plus, les aspects non techniques (par exemple, légaux et politiques) de l'atténuation de la surveillance envahissante sortent du domaine des obligations de l'IETF. La communauté de l'Internet au sens le plus large devra prendre des mesures pour contrer la PM, si cela doit être fait un jour.

Pour résumer, les capacités actuelles permettent à certains acteurs de surveiller les contenus et les métadonnées à travers l'Internet à une échelle jamais vue auparavant. Cette surveillance invasive est une attaque contre la confidentialité de l'Internet. L'IETF s'efforcera de produire des spécifications qui atténuent les attaques de surveillance invasive.

3. Note sur le processus

Dans le passé, des déclarations d'architecture de cette sorte, par exemple, la [RFC1984] et la [RFC2804], ont été publiées comme produits conjoints du groupe de pilotage de l'ingénierie de l'Internet (IESG, *Internet Engineering Steering Group*) et du bureau d'architecture de l'Internet (IAB, *Internet Architecture Board*). Cependant, depuis la publication de ces documents, l'IETF et l'IAB ont séparé leurs "flux" de publication comme décrit dans la [RFC4844] et la [RFC5741]. Ce document a été initié après discussions dans l'IESG et l'IAB, mais est publié comme document faisant l'objet du consensus du flux IETF, afin d'assurer qu'il reflète bien le consensus de la communauté IETF toute entière.

4. Considérations sur la sécurité

Le présent document est entièrement consacré à la confidentialité. On trouvera plus d'informations sur les relations entre les menaces pour la sécurité et celles pour la confidentialité dans la [RFC6973]. Le paragraphe 5.1.1 de la [RFC6973] traite spécifiquement de la surveillance comme une menace combinée sur la sécurité et la confidentialité.

5. Remerciements

Nous remercions les participants à la plénière technique IETF 88 de leurs retours. Merci en particulier aux personnes suivantes pour leurs utiles suggestions ou commentaires : Jari Arkko, Fred Baker, Marc Blanchet, Tim Bray, Scott Brim, Randy Bush, Brian Carpenter, Benoit Claise, Alissa Cooper, Dave Crocker, Spencer Dawkins, Avri Doria, Wesley Eddy, Adrian Farrel, Joseph Lorenzo Hall, Phillip Hallam-Baker, Ted Hardie, Sam Hartmann, Paul Hoffman, Bjoern Hoehrmann, Russ Housley, Joel Jaeggli, Stephen Kent, Eliot Lear, Barry Leiba, Ted Lemon, Subramanian Moonesamy, Erik Nordmark, Pete Resnick, Peter Saint-Andre, Andrew Sullivan, Sean Turner, Nicholas Weaver, Stefan Winter, et Lloyd Wood. De plus, nous tenons à remercier tous ceux qui ont contribué par des suggestions à la façon d'améliorer la sécurité et la confidentialité sur l'Internet ou qui ont fait des commentaires sur ce sujet sur les diverses listes de diffusion de l'IETF, comme ietf@ietf.org et perpass@ietf.org.

6. Références pour information

[IETF88P] IETF, "IETF 88 Plenary Meeting Materials", novembre 2013, < http://www.ietf.org/proceedings/88/ >.

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

[RFC2804] IAB, IESG, "Politique de l'IETF en matière d'écoutes", mai 2000. *(Information)*

[RFC3552] E. Rescorla, B. Korver, "Lignes directrices pour la rédaction d'une section de considérations sur la sécurité dans les RFC", juillet 2003. (BCP0072)

[RFC4844] L. Daigle, éd., Internet Architecture Board, "La série des RFC et l'éditeur des RFC", juillet 2007. *(Information)*

[RFC4949] R. Shirey, "Version 2 du glossaire de la sécurité sur Internet", août 2007. (*Remplace* RFC2828) (FYI0036) *(Info.)*

[RFC5741] L. Daigle et O. Kolkman, éd., IAB, "Flux de RFC, en-têtes et mentions communes", décembre 2009. *(Info. Remplacée par* RFC7841)

[RFC6962] B. Laurie, A. Langley, E. Kaspe, "Transparence de certificat", juin 2013. *(Exp.)*

[RFC6973] A. Cooper et autres, "Considérations de confidentialité pour les protocoles de l'Internet", juillet 2013. *(Info.)*

Adresse des auteurs

Stephen Farrell
Trinity College Dublin
Dublin 2
Ireland

Hannes Tschofenig
ARM Ltd.
6060 Hall in Tirol
Austria

téléphone : 1-896-2354
mél : stephen.farrell@cs.tcd.ie

mél : Hannes.tschofenig@gmx.net
URI : http://www.tschofenig.priv.at