Groupe de travail Réseau
Request for Comments : 3365
BCP : 61
Catégorie : Bonnes pratiques actuelles

J. Schiller, Massachusetts Institute of Technology
août 2002

Traduction Claude Brière de L'Isle

Exigence d'une sécurité forte dans les protocoles standard de l'IETF

Statut de ce mémoire
Le présent document spécifie les bonnes pratiques actuelles de l'Internet pour la communauté de l'Internet, et appelle à la discussion et à des suggestions pour son amélioration. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le consensus de l'IETF s'est établi sur l'idée que les protocoles standard de l'IETF DOIVENT faire usage des mécanismes appropriés de sécurité forte. Le présent document décrit l'histoire et les raisons de cette doctrine et établit cette doctrine comme bonnes pratiques actuelles.

Table des Matières

1. Introduction

L'objet du présent document est de rapporter le consensus de l'IETF sur les exigences de sécurité pour les protocoles ainsi que de définir leurs fondements et leur motivation.

L'Internet est un réseau mondial de réseaux et hôtes gérés de façon indépendante. À ce titre, il n'y a pas une autorité centrale responsable du fonctionnement du réseau. Il n'y a pas non plus d'autorité centrale chargée d'assurer la sécurité à travers le réseau.

La sécurité doit être assurée de bout en bout ou d'hôte à hôte. Le rôle de l'IETF dans la sécurité est de s'assurer que les protocoles standard de l'IETF ont les caractéristiques nécessaires pour assurer une sécurité appropriée pour l'application comme elle peut être utilisée à travers l'Internet. Des mécanismes de mise en œuvre obligatoire devraient assurer une sécurité adéquate pour protéger les applications commerciales sensibles.

2. Terminologie

Bien qu'on ne définisse pas une norme de protocole dans le présent document, on utilisera les termes DOIT, PEUT, DEVRAIT et leurs composés dans le sens défini dans la [RFC2119].

3. Services de sécurité

La [RFC2828] donne une liste complète des services de sécurité inter réseau et de leur définition. On reprend ici trois définitions essentielles :

* Service d'authentification : c'est un service de sécurité qui vérifie une identité revendiquée par ou pour une entité, qu'elle soit un processus, un système informatique, ou une personne. À la couche inter réseau, cela inclut de vérifier qu'un datagramme vient d'où il prétend arriver. À la couche application, cela inclut de vérifier que l'entité qui effectue une opération est celle qu'elle prétend être.

* Service de confidentialité des données : service de sécurité qui protège les données contre la divulgation non autorisée à des individus ou processus non autorisés. (Les documents de normes de l'Internet NE DEVRAIENT PAS utiliser "confidentialité des données" comme un synonyme de "vie privée", qui est un concept différent. Vie privée se réfère au droit d'une entité, normalement une personne, agissant en son nom propre, de déterminer le degré auquel elle va interagir avec son environnement, incluant le degré auquel l'entité veut partager les informations sur elle-même avec les autres.)

* Service d'intégrité des données : service de sécurité qui protège contre les changements non autorisés aux données, y compris les changements intentionnels (incluant la destruction) et les changements accidentels (incluant la perte) en s'assurant que les changements aux données sont détectables.

4. Quelques propriétés de l'Internet

Comme mentionné plus haut, l'Internet n'assure aucune sécurité inhérente. Des îlots de réseautage existent où les utilisateurs croient que la sécurité est fournie par l'environnement même. Un exemple serait un réseau d'entreprise non connecté à l'Internet mondial.

On peut imaginer que les protocoles conçus pour fonctionner dans un tel isolat ne vont pas exiger de services de sécurité, car la sécurité est assurée par l'environnement.

L'histoire non montre que les applications qui fonctionnent en utilisant la suite de protocoles TCP/IP sont partout utilisées dans l'Internet. Ceci est vrai même lorsque il n'était pas envisagé que l'application d'origine soit utilisée dans un environnement d'Internet de "large zone". Si une application n'est pas conçue pour assurer la sécurité, les usagers de l'application vont découvrir qu'ils sont vulnérables aux attaques.

5. Technologie de sécurité de l'IETF

L'IETF a plusieurs protocoles et normes de sécurité. La sécurité IP (IPsec) [RFC2411], la sécurité de la couche transport (TLS, *Transport Layer Security*) [RFC2246] sont deux protocoles bien connus. La couche simple d'authentification et de sécurité (SASL, *Simple Authentication and Security Layer*) [RFC2222] et l'interface générique de programme d'application de service de sécurité (GSSAPI, *Generic Security Service Application Programming Interface*) [RFC2743] fournissent des services dans le contexte d'un protocole "d'hôte". Ils peuvent être vus comme une "boîte à outils" à utiliser au sein d'un autre protocole.

Un des choix critiques qu'un concepteur de protocole doit faire est de savoir si il doit utiliser un des protocoles existants, concevoir son propre protocole de façon à utiliser un des outils standard ou faire quelque chose de complètement différent.

Il n'y a pas une réponse correcte pour tous les protocoles et les concepteurs ont réellement besoin d'examiner les menaces qui pèsent sur leur propre protocole et concevoir les contre mesures appropriées. L'objet de la Section "Considérations pour la sécurité" dont la présence est exigée dans une RFC en cours de normalisation dans l'Internet est de fournir un endroit où les concepteurs de protocoles documentent les menaces et expliquent la logique de leur concept de sécurité.

6. La doctrine Danvers

À la 32ème réunion de l'IETF tenue à Danvers, Massachusetts, en avril 1995, l'IESG a demandé à la plénière un consensus sur la force de la sécurité qui devrait être fournie par les normes de l'IETF. Bien que la question immédiate avant l'IETF ait été de prendre en charge ou non la sécurité de niveau "export" (qui signifie en fait une sécurité faible) dans les normes, la question soulevait le problème générique de la sécurité.

Le consensus très majoritaire était que l'IETF devrait normaliser l'utilisation de la meilleure sécurité disponible, sans considération des politiques nationales. On se réfère souvent à ce consensus sous le nom de "doctrine de Danvers".

On a au fil du temps étendu l'interprétation de la doctrine de Danvers à l'implication que tous les protocoles de l'IETF devraient fonctionner en toute sécurité. Qui pourrait objecter à cela ?

Depuis 1995, l'Internet a été de plus en plus soumis à des attaques de la part de divers acteurs malveillants. En 2000, une couverture significative de la presse était dédiée aux attaques de déni de service réparties. Cependant, nombre de ces attaques étaient lancées en compromettant d'abord un système informatique connecté à l'Internet. De nombreux systèmes sont habituellement compromis afin de lancer une attaque répartie significative.

La conclusion qu'on peut tirer de tout cela est que si on échoue à fournir des protocoles sûrs, l'Internet va devenir moins utile pour fournir une infrastructure internationale de communications, ce qui paraît être son destin.

Un des arguments qu'on entend continuellement contre la construction de la sécurité dans les protocoles est qu'un certain protocole n'est destiné à être utilisé que dans des environnements "protégés" où la sécurité ne sera pas un problème.

Cependant il est très difficile de prédire comment un protocole sera utilisé à l'avenir. Ce qui pouvait n'être destiné qu'à un environnement restreint peut fort bien finir par être déployé dans l'Internet mondial. On ne peut pas attendre cela pour corriger les problèmes de sécurité. Le temps qu'on réalise que ce déploiement s'est fait, il est trop tard.

La solution est que nous DEVONS mettre en œuvre une sécurité forte dans tous les protocoles pour prévoir le jour toujours trop proche où le protocole devient d'usage courant dans l'Internet mondial.

7. Obligatoire pour les mises en œuvre

On dit souvent que la sécurité est une obligation pour les mises en œuvre. Il vaut la peine de noter qu'il y a une différence significative entre obligation de mise en œuvre et obligation d'utiliser.

Comme on l'a mentionné précédemment, certains protocoles peuvent être déployés dans des enclaves sécurisées pour lesquelles la sécurité n'est pas un problème et le traitement d'un protocole de sécurité peut ajouter une dégradation significative des performances. Donc, il est parfaitement raisonnable que les dispositifs de sécurité soient une option que l'utilisateur final du protocole peut choisir de désactiver. Noter qu'on utilise ici une définition floue de "utilisateur final". On veut dire non seulement l'ultime utilisateur d'extrémité, mais tout déploiement d'une technologie, qui peut être une entreprise entière.

Cependant, la sécurité doit être une OBLIGATION DE MISE EN ŒUVRE afin que les utilisateurs finaux aient l'option de l'activer lorsque la situation l'exige.

8. Le chiffrement est il un MUST ?

Pas nécessairement. Cependant il faut ici être un peu plus précis. Quels services de sécurité sont appropriés pour un certain protocole dépend beaucoup de l'application qu'il met en œuvre. Beaucoup de gens supposent que chiffrement signifie confidentialité. En d'autres termes, le chiffrement du contenu des messages du protocole.

Il y a cependant de nombreuses applications où la confidentialité n'est pas une exigence, mais où l'authentification et l'intégrité le sont.

Un exemple pourrait être celui d'une application de contrôle d'un bâtiment où on utilise une technologie IP pour faire fonctionner les commandes de température et de ventilation. Il n'y a vraisemblablement aucune exigence que soient protégée la confidentialité des messages qui font ouvrir et fermer la ventilation de l'air conditionné. Cependant, il est vraisemblable que l'authentification et la protection de l'intégrité sont importantes si on veut protéger le bâtiment contre un acteur malveillant qui élèverait ou abaisserait la température à son gré.

Et donc on a souvent besoin des techniques de chiffrement pour mettre en œuvre l'authentification et la protection de l'intégrité des messages de protocole. De sorte que si la question est "DOIT on mettre en œuvre la confidentialité ?" la réponse sera "cela dépend". Cependant, si la question est "DOIT on utiliser la technologie cryptographique ?" la réponse est "vraisemblablement".

9. La cryptographie sonne mal à l'oreille

La mention de technologie cryptographique fait froncer les sourcils dans de nombreux forums de l'IETF et la résistance augmente.

De nombreuses personnes semblent associer le mot "cryptographie" avec des problèmes comme le contrôle des exportations et des performances. Certains se plaignent de ne pas la comprendre et se dérobent donc à son utilisation. Cependant, beaucoup de ces craintes sont sans fondement.

Le contrôle à l'exportation d'aujourd'hui, au moins à partir de la plupart des pays développés, est en train de devenir un problème moins brûlant. Et même là où c'est un problème, il ne porte pas tant sur la cryptographie elle-même que sur son utilisation pour assurer la confidentialité.

Il y a des problèmes de performances quand on utilise les techniques cryptographiques. Cependant, à l'IETF, on est fier d'être des ingénieurs. C'est un exercice pour ingénieurs de représenter la façon appropriée d'utiliser les techniques cryptographiques de façon à éliminer ou au moins de minimiser l'impact de l'utilisation de la cryptographie au sein d'un certain protocole.

Finalement, pour ce qui concerne la compréhension de la cryptographie, on n'a pas à le faire. En d'autre termes, on n'a pas besoin de devenir cryptographe pour utiliser effectivement une technique cryptographique. On utilise à la place les chiffrements, et les suites de chiffrement, bien compris qui existent pour résoudre le problème d'ingénierie posé.

Un des objectifs du domaine Sécurité de l'IETF est d'élaborer des lignes directrices afin que les mises en œuvre de protocoles puissent choisir la technologie appropriée sans avoir à en comprendre les détails.

10. Considérations sur la sécurité

Le présent document traite de l'exigence de l'IETF que la sécurité soit considérée dans la mise en œuvre des protocoles. Il est donc entièrement consacré à la sécurité !

11. Remerciements

L'auteur tient à remercier de leur participation les membres du groupe consultatif du domaine de la sécurité et en particulier Rob Shirey, Ran Atkinson, Steve Bellovin, Marc Blanchet, Steve Kent, Randy Bush, Dave Crocker, Stephen Farrell, Paul Hoffman, Russ Housley, Christian Huitema, Melinda Shore, Adam Shostack et Kurt D. Zeilenga.

12. Références

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997.

[RFC2222] J. Myers, "Authentification simple et couche de sécurité (SASL)", octobre 1997. (*Obsolète, voir* RFC4422, RFC4752) (*MàJ par* RFC2444) *(P.S.)*

[RFC2246] T. Dierks et C. Allen, "Protocole TLS version 1.0", janvier 1999.

[RFC2411] R. Thayer, N. Doraswamy, R. Glenn, "Feuille de route pour la sécurité sur IP", novembre 1998. *(Remplacée par* RFC6071*)*

[RFC2743] J. Linn, "Interface générique de programme d'application de service de sécurité, version 2, mise à jour 1", janvier 2000. (*MàJ par* RFC5554)

[RFC2828] R. Shirey, "Glossaire de la sécurité sur l'Internet", FYI 36, mai 2000. (*Obsolète, voir* RFC4949)

13. Adresse de l’auteur

Jeffrey I. Schiller
MIT Room W92-190
77 Massachusetts Avenue
Cambridge, MA 02139-4307
USA

téléphone : +1 (617) 253-8400
mél : jis@mit.edu

14. Déclaration complète de droits de reproduction

Remerciement

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