

afnic

Chiffrement, sous le contrôle de qui ? (1/8)

Stéphane Bortzmeyer

bortzmeyer@nic.fr

afnic

Nos communications sont-elle surveillées ?

Nos communications sont-elle surveillées ?

- Oui,

Nos communications sont-elle surveillées ?

- Oui,
- Révélations Snowden,

Nos communications sont-elle surveillées ?

- Oui,
- Révélations Snowden,
- Diverses lois (exposé des motifs de la Loi Renseignement « on le fait déjà mais on serait rassuré de le faire légalement »),

Nos communications sont-elle surveillées ?

- Oui,
- Révélations Snowden,
- Diverses lois (exposé des motifs de la Loi Renseignement « on le fait déjà mais on serait rassuré de le faire légalement »),
- Catalogues des équipementiers réseau, remplis de solutions techniques pour l'interception,

Nos communications sont-elle surveillées ?

- Oui,
- Révélations Snowden,
- Diverses lois (exposé des motifs de la Loi Renseignement « on le fait déjà mais on serait rassuré de le faire légalement »),
- Catalogues des équipementiers réseau, remplis de solutions techniques pour l'interception,
- Un opérateur réseau au FIC en 2015 « avec le chiffrement, on ne pourra plus savoir ce que font les clients »,

Nos communications sont-elle surveillées ?

- Oui,
- Révélations Snowden,
- Diverses lois (exposé des motifs de la Loi Renseignement « on le fait déjà mais on serait rassuré de le faire légalement »),
- Catalogues des équipementiers réseau, remplis de solutions techniques pour l'interception,
- Un opérateur réseau au FIC en 2015 « avec le chiffrement, on ne pourra plus savoir ce que font les clients »,
- Le RFC 8404 « *Effects of Pervasive Encryption on Operators* » ou « c'est triste, je ne peux plus faire ce que je veux ».

Nos communications sont-elle modifiées ?

Nos communications sont-elle modifiées ?

- Oui,

Nos communications sont-elle modifiées ?

- Oui,
- Orange Tunisie en juillet 2018 (ajout de publicités dans les pages Web),

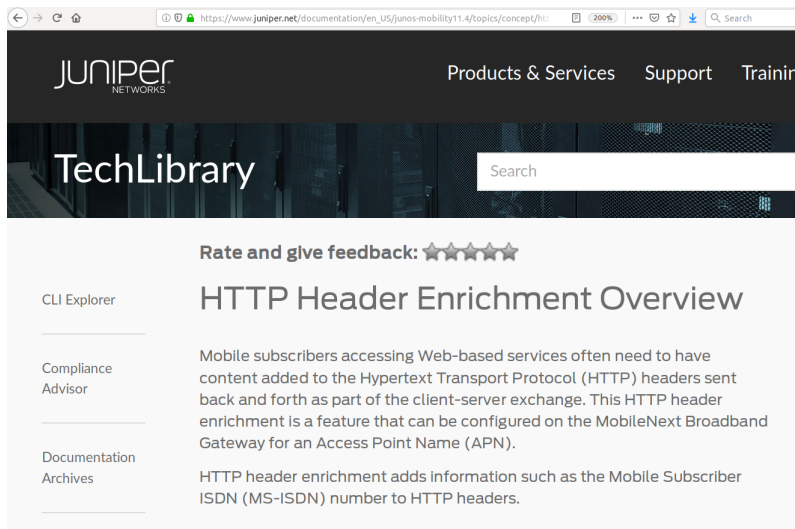
Nos communications sont-elle modifiées ?

- Oui,
- Orange Tunisie en juillet 2018 (ajout de publicités dans les pages Web),
- Vodafone Afrique du Sud qui ajoute le numéro de téléphone de l'abonné dans un en-tête HTTP,

Nos communications sont-elle modifiées ?

- Oui,
- Orange Tunisie en juillet 2018 (ajout de publicités dans les pages Web),
- Vodafone Afrique du Sud qui ajoute le numéro de téléphone de l'abonné dans un en-tête HTTP,
- SFR qui ajoute un en-tête de pistage `x-bluecoat-via:.`

Violer la neutralité du réseau, avec nos produits



The screenshot shows a web browser window displaying the Juniper Networks TechLibrary page. The URL in the address bar is https://www.juniper.net/documentation/en_US/junos-mobility11.4/topics/concept/ht. The page features the Juniper Networks logo in the top left, navigation links for 'Products & Services', 'Support', and 'Training' in the top right, and a 'TechLibrary' header with a search bar. Below the header, there is a section for 'Rate and give feedback' with five stars. The main content area is titled 'HTTP Header Enrichment Overview' and includes a sidebar with links for 'CLI Explorer', 'Compliance Advisor', and 'Documentation Archives'. The main text describes how mobile subscribers need content added to HTTP headers for Web-based services and mentions the MobileNext Broadband Gateway for an Access Point Name (APN).

Rate and give feedback: ★★★★★

CLI Explorer

Compliance Advisor

Documentation Archives

HTTP Header Enrichment Overview

Mobile subscribers accessing Web-based services often need to have content added to the Hypertext Transport Protocol (HTTP) headers sent back and forth as part of the client-server exchange. This HTTP header enrichment is a feature that can be configured on the MobileNext Broadband Gateway for an Access Point Name (APN).

HTTP header enrichment adds information such as the Mobile Subscriber ISDN (MS-ISDN) number to HTTP headers.

Le chiffrement est donc indispensable

Le chiffrement est donc indispensable

- Bien sûr, il faut des lois (RGPD ?),

Le chiffrement est donc indispensable

- Bien sûr, il faut des lois (RGPD ?),
- Et des principes (neutralité du réseau),

Le chiffrement est donc indispensable

- Bien sûr, il faut des lois (RGPD ?),
- Et des principes (neutralité du réseau),
- Mais, dans le monde numérique, il est très difficile d'assurer leur respect,

Le chiffrement est donc indispensable

- Bien sûr, il faut des lois (RGPD ?),
- Et des principes (neutralité du réseau),
- Mais, dans le monde numérique, il est très difficile d'assurer leur respect,
- Il faut donc aussi des mesures techniques, notamment le chiffrement.

Les limites du chiffrement

Les limites du chiffrement

- Mais aucune solution technique n'est parfaite,

Les limites du chiffrement

- Mais aucune solution technique n'est parfaite,
- Les logiciels ont des bogues,

Les limites du chiffrement

- Mais aucune solution technique n'est parfaite,
- Les logiciels ont des bogues,
- Et des portes dérobées,

Les limites du chiffrement

- Mais aucune solution technique n'est parfaite,
- Les logiciels ont des bogues,
- Et des portes dérobées,
- Le chiffrement ne protège pas contre les extrêmes :
 - Sécurité de la machine terminale,
 - Sécurité du serveur distant.

Qui contrôle ?

Qui contrôle ?

- Le chiffrement doit être de bout en bout, autrement il ne vaut pas grand'chose (le réseau peut être contrôlé par un adversaire),

Qui contrôle ?

- Le chiffrement doit être de bout en bout, autrement il ne vaut pas grand'chose (le réseau peut être contrôlé par un adversaire),
- Le logiciel doit être libre, pour permettre son examen (attention : condition nécessaire mais pas suffisante),

Qui contrôle ?

- Le chiffrement doit être de bout en bout, autrement il ne vaut pas grand'chose (le réseau peut être contrôlé par un adversaire),
- Le logiciel doit être libre, pour permettre son examen (attention : condition nécessaire mais pas suffisante),
- Le contrôle de la machine terminale est un enjeu important,

Qui contrôle ?

- Le chiffrement doit être de bout en bout, autrement il ne vaut pas grand'chose (le réseau peut être contrôlé par un adversaire),
- Le logiciel doit être libre, pour permettre son examen (attention : condition nécessaire mais pas suffisante),
- Le contrôle de la machine terminale est un enjeu important,
- Décentralisation : chiffrer n'est pas très utile si tout passe par un GAFA.

Merci !

afnic

www.afnic.fr
contact@afnic.fr

afnic