La NSA a t-elle une webcam dans votre salle de bains ?

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 14 mars 2014. Dernière mise à jour le 15 mars 2014

https://www.bortzmeyer.org/security-day-nsa.html

Hier, 13 mars 2014, à l'ESGI à Paris, j'ai participé au « "*Security Day*" <http://www.globalsecuritymag.fr/13-mars-Paris-Security-Day-ESGI,20140227,43264.html> » avec un exposé de spéculation sur les capacités effectives de la NSA. Peut-elle tout écouter et déchiffrer même ce qu'on a chiffré avec les meilleures clés RSA ? HTTPS nous protège t-il contre un tel ennemi ?

Les supports de l'exposé :

— En version adaptée à la vue sur écran (en ligne sur https://www.bortzmeyer.org/files/esgi-security-day-nsa-SHOW.pdf),
— En version adaptée à l'impression (en ligne sur https://www.bortzmeyer.org/files/esgi-security-day-pdf),
— Bien sûr le source (en ligne sur https://www.bortzmeyer.org/files/esgi-security-day-nsa.tex),
— Quant à la vidéo, elle est disponible <https://www.youtube.com/watch?v=DTxqZI8U27g> sur les serveurs de NSA Tube. (Errata : Grigori Perelman n'a pas démontré la conjecture de Riemann mais celle de Poincaré.)

Parmi les autres exposés de la journée, je vous recommanderais bien celui de Damien Cauquil sur la sécurité des "*set-top boxes*" mais, pour des raisons de sécurité, rien n'est en ligne (résumé : il est trivial de pirater une télé, notamment parce que le chiffrement n'est pas utilisé, et cela fait des jolies copies d'écran).

Merci à Manuel Pégourié-Gonnard pour sa relecture. Et merci aux organisateurs, notamment Dylan Dubief, pour tout le travail. Et merci pour la bière « Cuvée des trolls » en cadeau :-)