La sécurité est-elle l'amie ou l'ennemie des droits humains ? (1/12)

Stéphane Bortzmeyer
stephane+jsecin@bortzmeyer.org

Journée de la Sécurité Informatique en Normandie, Rouen, 29 novembre 2018

Liberté et sécurité

Liberté et sécurité

- Débat politique classique, souvent binaire.

Liberté et sécurité

- Débat politique classique, souvent binaire.
- Les deux sont cruciales.

Liberté et sécurité

- Débat politique classique, souvent binaire.
- Les deux sont cruciales.
- Attention, la sécurité est souvent un prétexte.

Liberté et sécurité

- Débat politique classique, souvent binaire.
- Les deux sont cruciales.
- Attention, la sécurité est souvent un prétexte.
- Dans le monde numérique, peu de discussions sur les conséquences politiques des choix de sécurité.

Liberté et sécurité

- Débat politique classique, souvent binaire.
- Les deux sont cruciales.
- Attention, la sécurité est souvent un prétexte.
- Dans le monde numérique, peu de discussions sur les conséquences politiques des choix de sécurité.
- La sécurité, c'est compliqué, ce qui contribue à dépolitiser le débat.

La liberté

La liberté

- Liberté théorique et liberté réelle (sortir dans la rue...)

La liberté

- Liberté théorique et liberté réelle (sortir dans la rue...)
- Personne n'ose dire ouvertement qu'il est contre la liberté...

La liberté

- Liberté théorique et liberté réelle (sortir dans la rue...)
- Personne n'ose dire ouvertement qu'il est contre la liberté...
- Mais beaucoup le pensent.

La liberté

- Liberté théorique et liberté réelle (sortir dans la rue...)
- Personne n'ose dire ouvertement qu'il est contre la liberté...
- Mais beaucoup le pensent.
- Liberté de critiquer la sécurité ? « Si vous êtes contre cette mesure de sécurité, c'est que vous êtes pour les terroristes ou, pire, pour les pirates qui copient les œuvres protégées. »

La sécurité

La sécurité

- Tout le monde veut être en sécurité. Dans le monde numérique comme ailleurs.

La sécurité

- Tout le monde veut être en sécurité. Dans le monde numérique comme ailleurs.
- La sécurité de qui : qui protège-t-on ? Quels intérêts sont sûrs ? Toujours garder un regard critique.

La sécurité

- Tout le monde veut être en sécurité. Dans le monde numérique comme ailleurs.
- La sécurité de qui : qui protège-t-on ? Quels intérêts sont sûrs ? Toujours garder un regard critique.
- Être en sécurité pour profiter de la liberté.

Quelques cas

Quelques cas

- Problèmes complexes, à étudier soigneusement, et dans le détail.

Quelques cas

- Problèmes complexes, à étudier soigneusement, et dans le détail.
- Ne pas se laisser impressionner par les injonctions « c'est pour des raisons de sécurité ».

NAT

NAT

- Traduction d'adresses N$\longleftrightarrow$1.

NAT

- Traduction d'adresses N$\longleftrightarrow$1.
- Originellement pour traiter le problème de la pénurie d'adresses IPv4.

NAT

- Traduction d'adresses N$\longleftrightarrow$1.
- Originellement pour traiter le problème de la pénurie d'adresses IPv4.
- Aujourd'hui vendu comme « améliorant la sécurité ».

NAT

- Traduction d'adresses N$\longleftrightarrow$1.
- Originellement pour traiter le problème de la pénurie d'adresses IPv4.
- Aujourd'hui vendu comme « améliorant la sécurité ».
- Conséquences : pas de serveur chez soi, pair-à-pair difficile.

NAT

- Traduction d'adresses N$\longleftrightarrow$1.
- Originellement pour traiter le problème de la pénurie d'adresses IPv4.
- Aujourd'hui vendu comme « améliorant la sécurité ».
- Conséquences : pas de serveur chez soi, pair-à-pair difficile.
- Pas de gain en sécurité : les attaques peuvent être internes, ou utiliser le contenu.

NAT

- Traduction d'adresses N$\longleftrightarrow$1.
- Originellement pour traiter le problème de la pénurie d'adresses IPv4.
- Aujourd'hui vendu comme « améliorant la sécurité ».
- Conséquences : pas de serveur chez soi, pair-à-pair difficile.
- Pas de gain en sécurité : les attaques peuvent être internes, ou utiliser le contenu.
- Si on veut un pare-feu, on installe un pare-feu.

Générativité et engins fermés

Généralité et engins fermés

- Apple contrôle ce qui peut aller dans l'AppStore.

Généralité et engins fermés

- Apple contrôle ce qui peut aller dans l'AppStore.
- Sur iOS et la plupart des Android, on n'est pas root.

Générativité et engins fermés

- Apple contrôle ce qui peut aller dans l'AppStore.
- Sur iOS et la plupart des Android, on n'est pas root.
- « Générativité » (Jonathan Zittrain) : la capacité d'une technique à permettre des choses non prévues.

Générativité et engins fermés

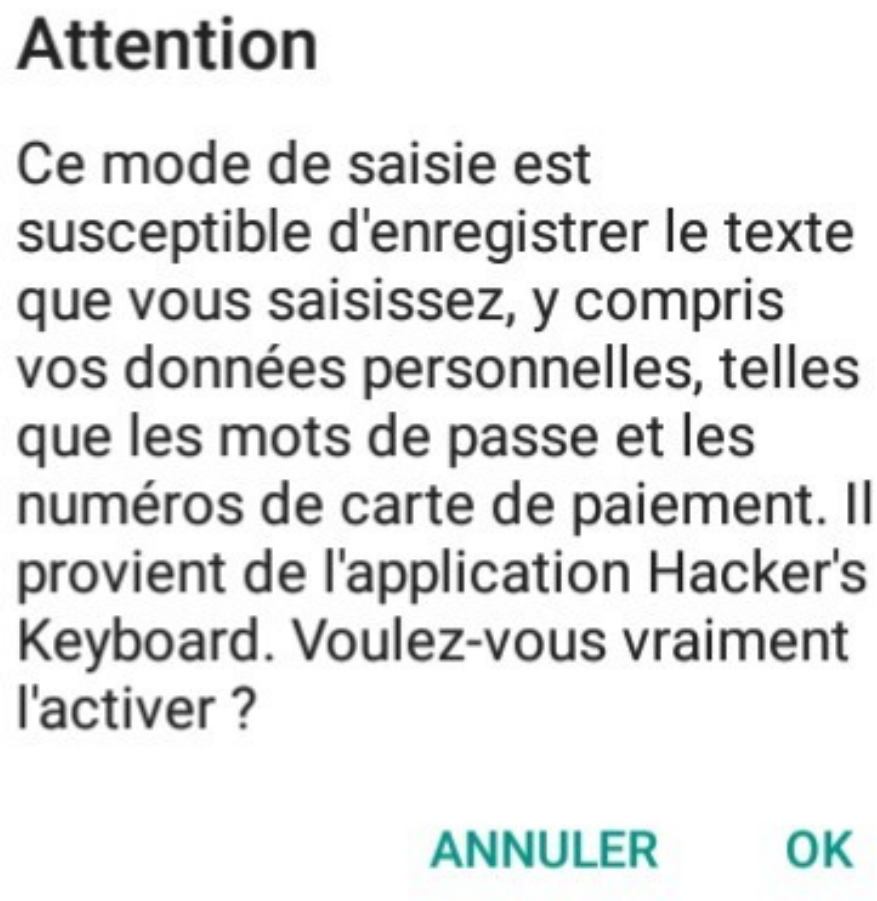
- Apple contrôle ce qui peut aller dans l'AppStore.
- Sur iOS et la plupart des Android, on n'est pas root.
- « Générativité » (Jonathan Zittrain) : la capacité d'une technique à permettre des choses non prévues.
- Une générativité absolue peut être dangereuse mais si une technique n'est pas générative, il n'y a pas de liberté, pas d'innovation.

Générativité et engins fermés

- Apple contrôle ce qui peut aller dans l'AppStore.
- Sur iOS et la plupart des Android, on n'est pas root.
- « Générativité » (Jonathan Zittrain) : la capacité d'une technique à permettre des choses non prévues.
- Une générativité absolue peut être dangereuse mais si une technique n'est pas générative, il n'y a pas de liberté, pas d'innovation.
- L'ordiphone doit-il être verrouillé ? La voiture non-hackable ? Et qui décide ? « *We agree with Apple that security is at the heart of all data privacy and privacy rights. Where we disagree is in who holds the keys. Your data isn't truly private or secure, if someone else holds the keys.* » (Puri.sm)

Google défend nos données personnelles contre les méchants

Android, avec un clavier virtuel alternatif :



Chiffrement et ses conséquences

« Sécurité » est un terme vague, qui désigne beaucoup de choses différentes.

Chiffrement et ses conséquences

« Sécurité » est un terme vague, qui désigne beaucoup de choses différentes.

- Chiffrer permet aux gentils de protéger leurs communications.

Chiffrement et ses conséquences

« Sécurité » est un terme vague, qui désigne beaucoup de choses différentes.

- Chiffrer permet aux gentils de protéger leurs communications.
- Chiffrer permet aux méchants de protéger leurs communications.

Chiffrement et ses conséquences

« Sécurité » est un terme vague, qui désigne beaucoup de choses différentes.

- Chiffrer permet aux gentils de protéger leurs communications.
- Chiffrer permet aux méchants de protéger leurs communications.
- Est-ce que ça améliore la sécurité ?

Chiffrement et ses conséquences

« Sécurité » est un terme vague, qui désigne beaucoup de choses différentes.

- Chiffrer permet aux gentils de protéger leurs communications.
- Chiffrer permet aux méchants de protéger leurs communications.
- Est-ce que ça améliore la sécurité ?
- Note technique : la plupart des intercepteurs TLS sont horriblement bogués et diminuent la sécurité.

Chiffrement et ses conséquences

« Sécurité » est un terme vague, qui désigne beaucoup de choses différentes.

- Chiffrer permet aux gentils de protéger leurs communications.
- Chiffrer permet aux méchants de protéger leurs communications.
- Est-ce que ça améliore la sécurité ?
- Note technique : la plupart des intercepteurs TLS sont horriblement bogués et diminuent la sécurité.
- Même sans ces bogues, l'interception de communications en entreprise améliore-t-elle la sécurité ? Celle de qui ?

Chiffrement et ses conséquences

« Sécurité » est un terme vague, qui désigne beaucoup de choses différentes.

- Chiffrer permet aux gentils de protéger leurs communications.
- Chiffrer permet aux méchants de protéger leurs communications.
- Est-ce que ça améliore la sécurité ?
- Note technique : la plupart des intercepteurs TLS sont horriblement bogués et diminuent la sécurité.
- Même sans ces bogues, l'interception de communications en entreprise améliore-t-elle la sécurité ? Celle de qui ?
- RFC 8404, le chiffrement gênerait certaines pratiques « de sécurité » ?

Attaques par déni de service

Attaques par déni de service

- Une plaie de l'Internet.

Attaques par déni de service

- Une plaie de l'Internet.
- Une menace directe contre la liberté d'expression.

Attaques par déni de service

- Une plaie de l'Internet.
- Une menace directe contre la liberté d'expression.
- Les petits sont désavantagés. Les attaques DoS favorisent les déjà gros.

Attaques par déni de service

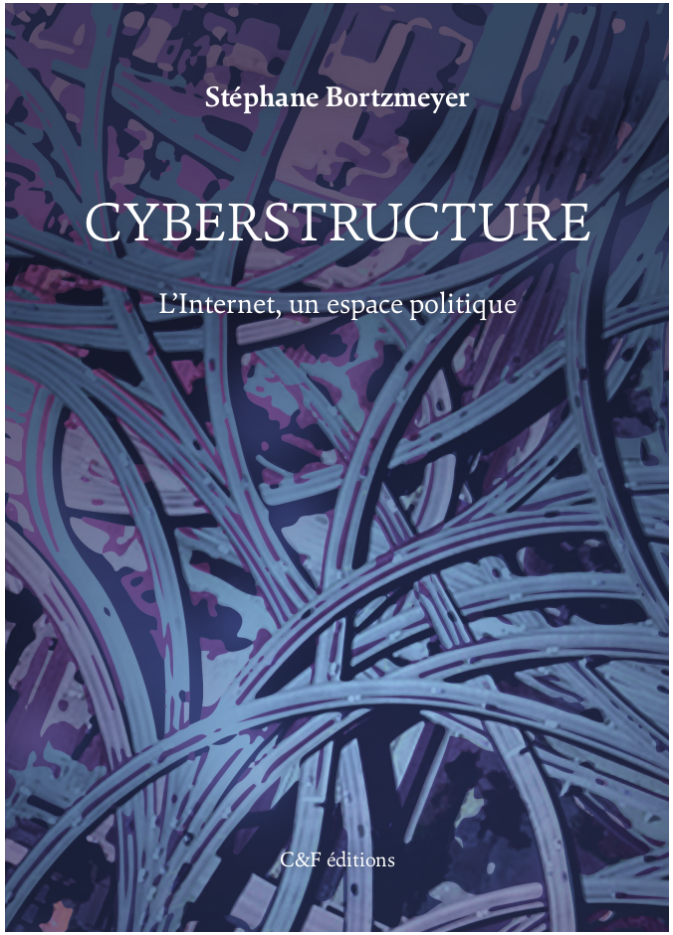
- Une plaie de l'Internet.
- Une menace directe contre la liberté d'expression.
- Les petits sont désavantagés. Les attaques DoS favorisent les déjà gros.
- Les remèdes sont-ils pires que le mal ? « Tout le monde chez Cloudflare » ?

Attaques par déni de service

- Une plaie de l'Internet.
- Une menace directe contre la liberté d'expression.
- Les petits sont désavantagés. Les attaques DoS favorisent les déjà gros.
- Les remèdes sont-ils pires que le mal ? « Tout le monde chez Cloudflare » ?
- « Protection » ? Comme le seigneur féodal protège ses serfs ?

Un peu de pub

Mon livre « Cyberstructure » sort le 10 décembre. On y parle aussi de sécurité.



Conclusion

Conclusion

- « Faut-il privilégier la liberté ou la sécurité ? » La question n'a pas de sens.

Conclusion

- « Faut-il privilégier la liberté ou la sécurité ? » La question n'a pas de sens.
- Les deux se nourrissent l'une l'autre.

Conclusion

- « Faut-il privilégier la liberté ou la sécurité ? » La question n'a pas de sens.
- Les deux se nourrissent l'une l'autre.
- Sans sécurité, pas de liberté, et réciproquement.

Conclusion

- « Faut-il privilégier la liberté ou la sécurité ? » La question n'a pas de sens.
- Les deux se nourrissent l'une l'autre.
- Sans sécurité, pas de liberté, et réciproquement.
- La sécurité n'est pas un problème technique mais social. Comme pour tout problème social, il faut discuter des conséquences politiques.