

(Cliquez sur) “Ajouter une exception”

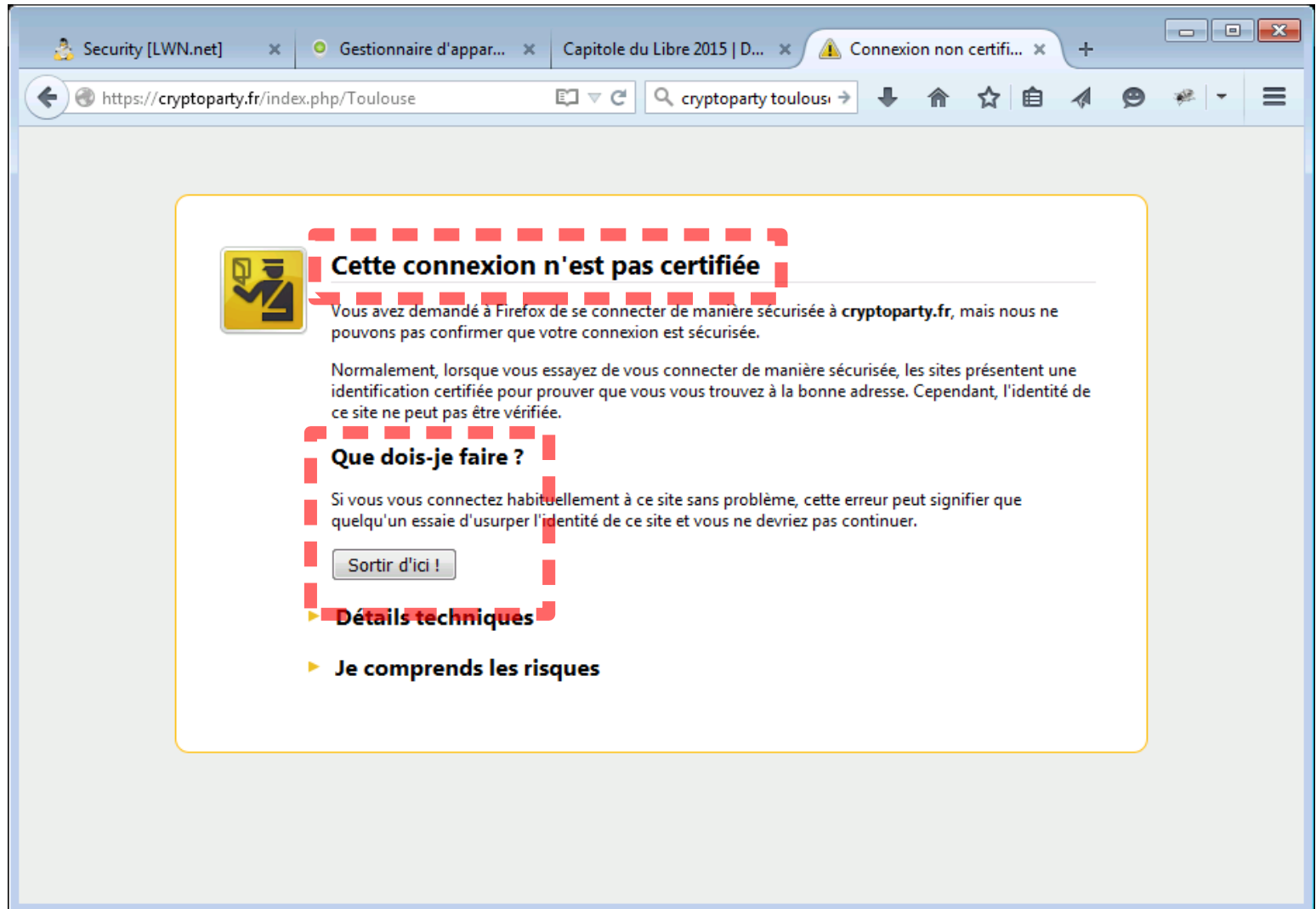
5 minutes pour comprendre

Rodolphe Ortalo

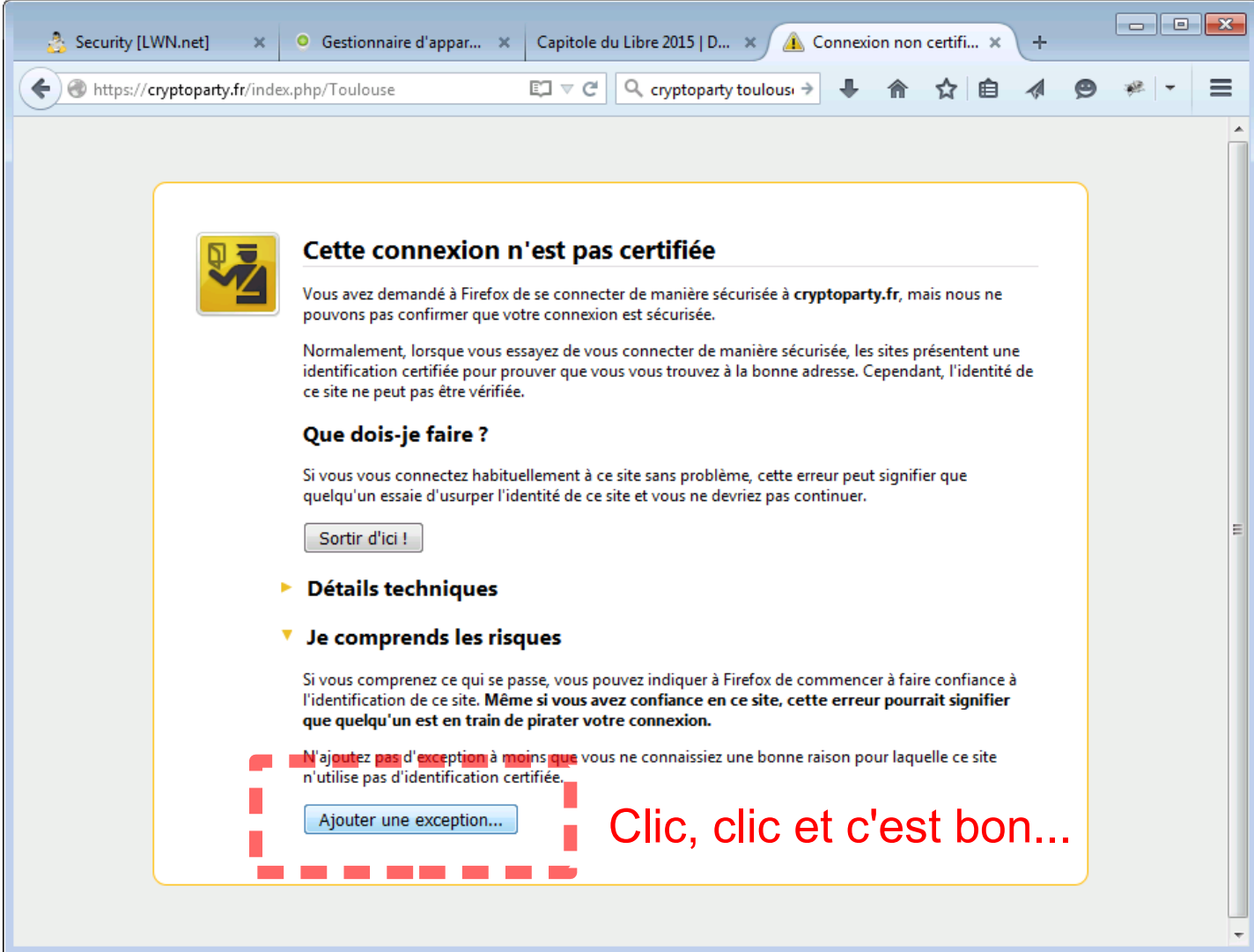
Dans les navigateurs

- Les avertissements de sécurité
 - quand on atteint un (nouveau) site Web
 - *Certificats X.509*
- La confession récente de votre navigateur
 - au sujet des *cookies* dont il se goinfre

Je vais vers un nouveau site



La « solution » réflexe



Security [LWN.net] x Gestionnaire d'appar... x Capitole du Libre 2015 | D... x Connexion non certifi... x

https://cryptoparty.fr/index.php/Toulouse

cryptoparty toulousi

Cette connexion n'est pas certifiée

Vous avez demandé à Firefox de se connecter de manière sécurisée à **cryptoparty.fr**, mais nous ne pouvons pas confirmer que votre connexion est sécurisée.

Normalement, lorsque vous essayez de vous connecter de manière sécurisée, les sites présentent une identification certifiée pour prouver que vous vous trouvez à la bonne adresse. Cependant, l'identité de ce site ne peut pas être vérifiée.

Que dois-je faire ?

Si vous vous connectez habituellement à ce site sans problème, cette erreur peut signifier que quelqu'un essaie d'usurper l'identité de ce site et vous ne devriez pas continuer.

Sortir d'ici !

- ▶ **Détails techniques**
- ▼ **Je comprends les risques**

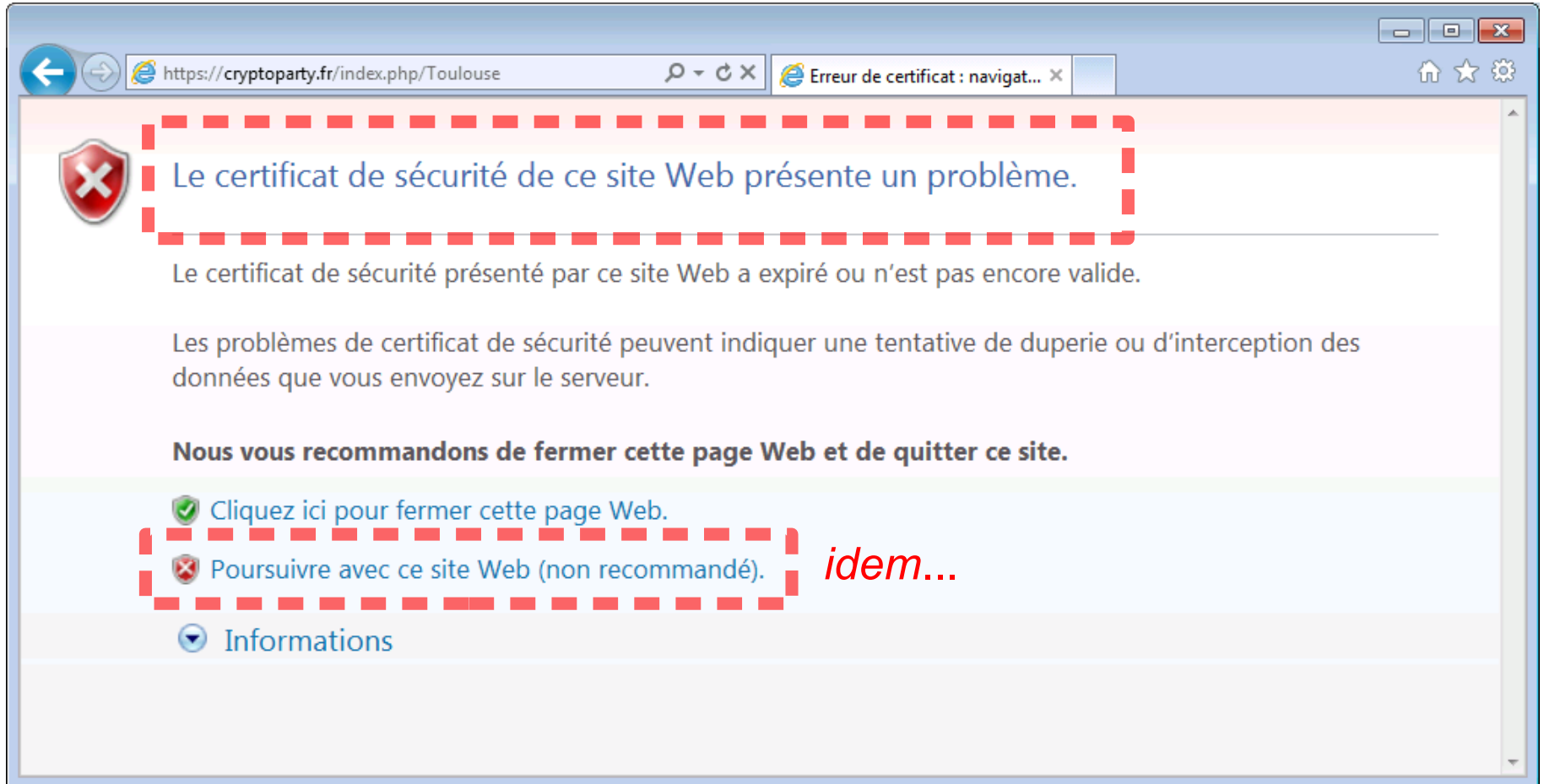
Si vous comprenez ce qui se passe, vous pouvez indiquer à Firefox de commencer à faire confiance à l'identification de ce site. **Même si vous avez confiance en ce site, cette erreur pourrait signifier que quelqu'un est en train de pirater votre connexion.**

N'ajoutez pas d'exception à moins que vous ne connaissiez une bonne raison pour laquelle ce site n'utilise pas d'identification certifiée.

Ajouter une exception...

Clic, clic et c'est bon...

Variante (mais pas libre)



L'explication

- Un certificat
 - C'est la pièce d'identité du site Web
 - C'est une clef publique (cryptographique)
- L'avertissement
 - La pièce d'identité est périmée
 - C'est une pièce d'identité « non-gouvernementale »
 - Certificat auto-signé
 - **C'est une pièce d'identité invalide**
(Celui là, on le voit jamais...)

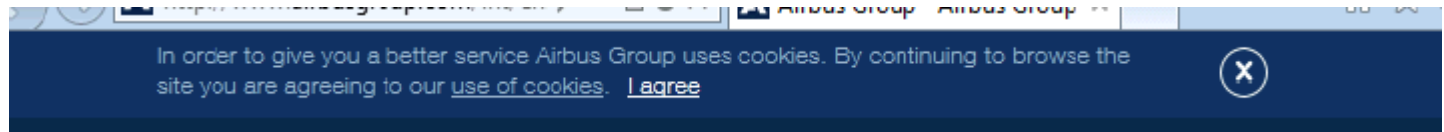
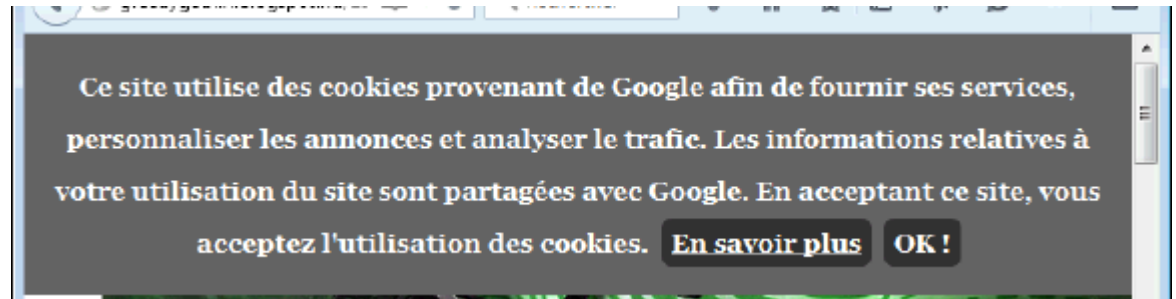
Et alors... ?

- Les utilisateurs ne comprennent généralement pas pourquoi on leur soumet ces alertes. Ils les ignorent de plus en plus.
- En plus, ils n'ont pas tort
 - La sécurité du canal de communication n'est **pas** compromise
 - En pratique, un certificat expiré ou auto-signé est souvent le signe que le propriétaire du site possède **plus** de compétences que la moyenne !
 - On pense à un certain exemple...
 - L'identité du serveur cible n'est pas vérifiée par les instances « officielles »
 - Peu d'importance dans la plupart des cas

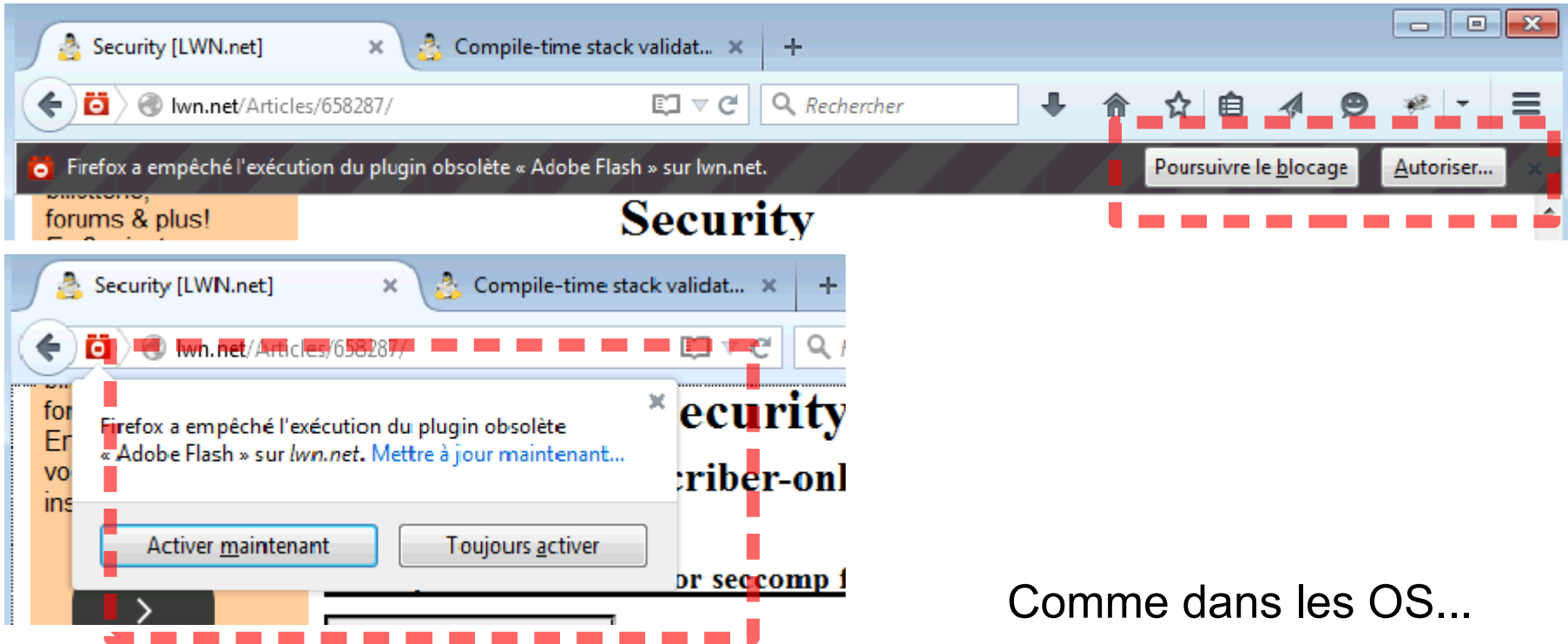
Et les sucreries ?

Les cookies

(dans nos contrées)



Des autorisations aussi (*plugin*)



Comme dans les OS...

Conclusions empiriques

- La plupart des « validations utilisateurs » sont
 - soit inutiles et de pure forme
 - soit des ordres en blanc
- L'effet sur le niveau d'information du public est probablement faible (nul?)
- En matière de sécurité des sites Web, une exception de sécurité est souvent bon signe (!)