La situation de l'Internet

Sciences & Vie, décembre 2008

« Internet au bord de l'explosion »

- Des problèmes de sécurité tout le temps (dDoS, spam, hameçonnage. . .)
- Peu de vie privée, trop de traces numériques laissées partout
- Peu de contrôle, n'importe quel pirate cagoulé peut envoyer n'importe quoi, en restant anonyme dans le Dark Web
- Congestions fréquentes, vidéos de loutres qui se bloquent soudain
- Difficulté à déployer de nouveaux services (pare-feux partout, innovation nulle part)
- Encore parfois des problÃ¨me d'encodages intolÃ©rables

Mal conçu ou mauvaise évolution ?

On dit souvent que l'Internet a été mal conçu dès le départ. . .

- Il y a deux façons de concevoir un système complexe : tout prévoir à l'avance (y compris les applications, dans le style du lancement du RNIS en France dans les années 1990), ou bien se lancer et corriger au fur et à mesure
- L'Internet a clairement été conçu de la seconde manière
- En 1969 ou même en 1982 (déploiement de TCP et d'IPv4), qui aurait pu prévoir les usages et les outils d'aujourd'hui ?

Exemple de la sécurité

- Chouinement fréquent « c'est nul que les protocoles Internet aient été conçus sans sécurité »
- C'est vrai qu'ajouter la sécurité après est difficile (DNSSEC toujours pas assez déployé)
- Mais les protocoles sécurisés par les experts en sécurité ne sont pas utilisés : trop complexes et trop restrictifs
- RFC 5218 « *What Makes For a Successful Protocol ?* » : les protocoles lancés sans sécurité sont durs à sécuriser ensuite, ceux lancés avec sécurité sont des échecs en terme d'adoption.

Pourquoi une si mauvaise sécurité ?

- Parce que les développeurs originaux étaient des hippies barbus libertaires irresponsables au lieu d'être des costards-cravate sérieux et polytechniciens avec Légion d'Honneur ?
- Ou bien parce que le problème est **difficile** ?
- Évidemment, tout dépend du cahier des charges. Si je suis Président à Vie de l'Internet, avec autorité sur les câbles, les routeurs, les logiciels clients et serveurs, et qu'il faut me demander une autorisation avant chaque publication de logiciel, avant chaque mise en service d'un site, je résoud plein de problèmes de sécurité.

Les raseurs de table

- « Internet est trop broquenne, il faut repartir de zéro, faire table rase » (*Clean Slate* dans la langue de Steve Crocker)
- Cela semble du bon sens : arrêtons de patcher et de repatcher, refaisons le truc en propre.
- Exemples de projets : Clean Slate, GENI, RINA et ICN aujourd'hui

Exemple : ICN

- *Information-centric Networking* RFC 7476
- L'objet central est le contenu, identifié par une adresse propre (imaginez un réseau qui route les *magnets*)
- Intelligence dans le réseau, réduit à permettre l'accès au contenu
- Apprécié des ayant-tous-les-droits (facilitera le contrôle d'accès)
- Disruptif, oui, mais est-ce que ce sera un progrès ?

Caractéristiques communes à beaucoup de ces projets

- *Back of the enveloppe* Des projets qui ne sont « même pas faux »
- Beaucoup de marketing et peu de déploiement
- Beaucoup de promesses, souvent contradictoires
- Confusion entre recherche fondamentale et ingéniérie

Les conditions objectives du processus de production

- La chasse aux crédits
- On n'obtient pas de crédits de recherche si on ne promet pas des choses grandioses
- Et il y a le goût des médias aussi, et ceux-ci réclament du sensationnel et des phrases fracassantes

La question cruciale du cahier des charges

- Un des principaux traits des raseurs de table est qu'ils ne décrivent que rarement leur cahier des charges. Cela leur permet de promettre le beurre et l'argent du beurre.
- Veut-on assurer une vraie vie privée ou bien au contraire avoir une identification systématique de chaque paquet ?
- Exemple du spam. Si le cahier des charges est « il faut éliminer le spam », le problème est trivial : on exige une autorisation du CSA avant chaque envoi de message. Si le cahier des charges est « on veut éliminer le spam à un coût raisonnable tout en permettant à n'importe qui d'écrire à quelqu'un avec qui il n'avait pas été en contact avant. », alors, c'est plus compliqué...
- « *You won't necessarily want to communicate with everybody* » (RINA) Avec un tel cahier des charges, ce n'est plus Internet...

Dans l'arène des idées, la lutte est inégale

- L'Internet actuel est réel et (très) imparfait
- Alors que les promesses volent dans la stratosphère
- « Sécurisé, rapide, fiable, propre, vert... »
- Le présent brille moins que le futur

Architecture et urbanisme

- Architecture : on peut souvent faire une maison en partant de zéro
- Urbanisme : on ne peut quasiment jamais refaire une ville de zéro

Le rêve dangereux d'un système parfait

- Internet n'est pas une machine, c'est un écosystème. En effet, personne ne l'a conçu, et c'est très bien.
- « *Every real ecosystem has parasites* » (Cory Doctorow).
- Les raseurs de table sont souvent des admirateurs du zoo, système parfait, contrôlé et sans parasite.

Retour à la technique

- Séparation identificateur/localisateur
- Aujourd'hui, l'adresse IP est à la fois un identificateur (elle sert à étiqueter une session TCP) et un localisateur (elle indique le point d'attachement au réseau)
- Cela rend difficile, par exemple, d'avoir plusieurs FAI
- Propositions de séparation :
  - ILNP (dans les machines terminales)
  - HIP (dans les machines terminales, crypto pour l'identité)
  - LISP (dans les routeurs)

GNUnet

- `https://gnunet.org/`
- *a framework for secure peer-to-peer networking that does not use any centralized or otherwise trusted services*

Conclusion

- Aura-t-on un jour un autre réseau ? Certainement. Rien n'est éternel.
- Sera-t-il meilleur que l'Internet ? Peut-être.
- Est-ce que ce sera facile à faire ? Plus dur que de donner un interview à Sciences & Vie.
- Qui le fera ? Pas les raseurs de table médiatiques.