SÉCURITÉ DU WEB 2.0

Nicolas RUFF
EADS-IW SE/CS
nicolas (dot) ruff (à) eads (dot) net

Plan

- Introduction
- Définition
- Fondamentaux
- *Success stories*
- Risques
- L'avenir
- Conclusion
- Bibliographie & remerciements

Définition

1998

- Le "Web Sémantique"
- Invention des formats XML, RDF, etc.

2004

- O'Reilly : "*Web 2.0 is the business revolution in the computer industry caused by the move to the internet as platform, and an attempt to understand the rules for success on that new platform*"

2007

- Tout le monde dit faire du Web 2.0, 2.5 ou même … 3.0

Définition

Web 1.0

- L'utilisateur consulte
- Il accède à des sites

Web 2.0

- L'utilisateur interagit
- Il utilise un service en ligne

"The machine is us/ing us"

- http://youtube.com/watch?v=6gmP4nk0EOE

Définition


DoubleClick
Google AdSense
Ofoto
Flickr
Akamai
BitTorrent
Britannica Online
Wikipedia
Sites perso
Blogs
Pages vues
Coût au clic
Publication
Participation
CMS
Wiki
Arborescence (taxonomie)
Tags ("folksonomie")

Définition

- Le Web 2.0 n'est *pas* une technologie
  - Le Web 2.0 n'est pas AJAX …
    - AJAX = XMLHTTPRequest( )

Fondamentaux

Agrégation (*mash-up*)

Réseau social / communautaire

- Perso : blogs, *MySpace*, *FaceBook*
- Pro : *Viadeo, Linkedin, OpenBC, Orkut*

Basé sur la réputation

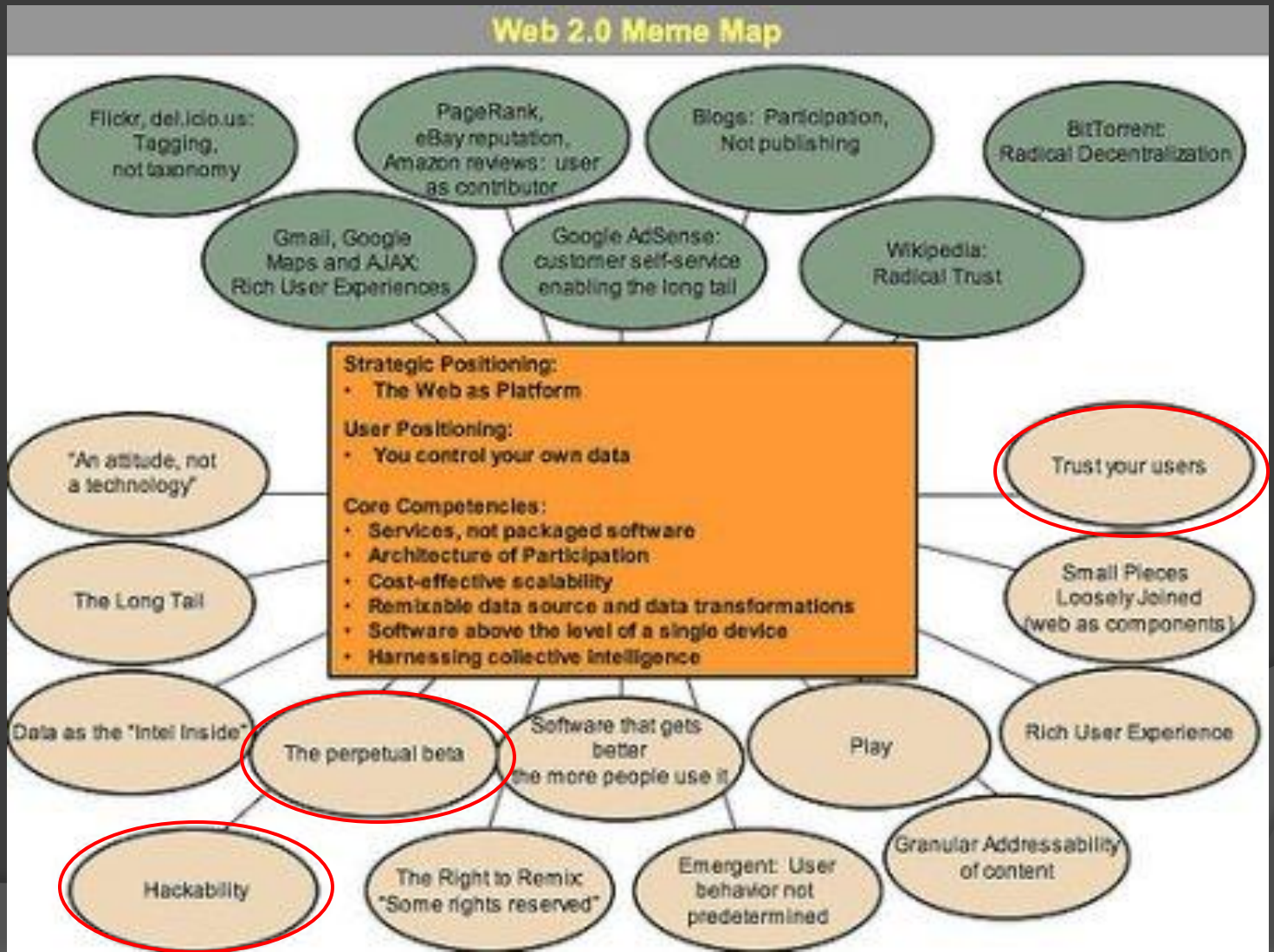
- *Technorati, Digg, Delicious, Reddit*
- *eBay*

Simple / convivial

- Personnalisable
- Pas de prérequis technique

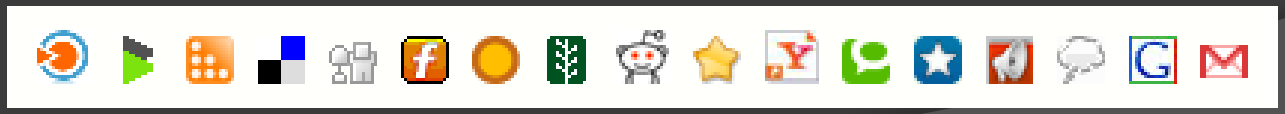
Fondamentaux

Selon O'Reilly



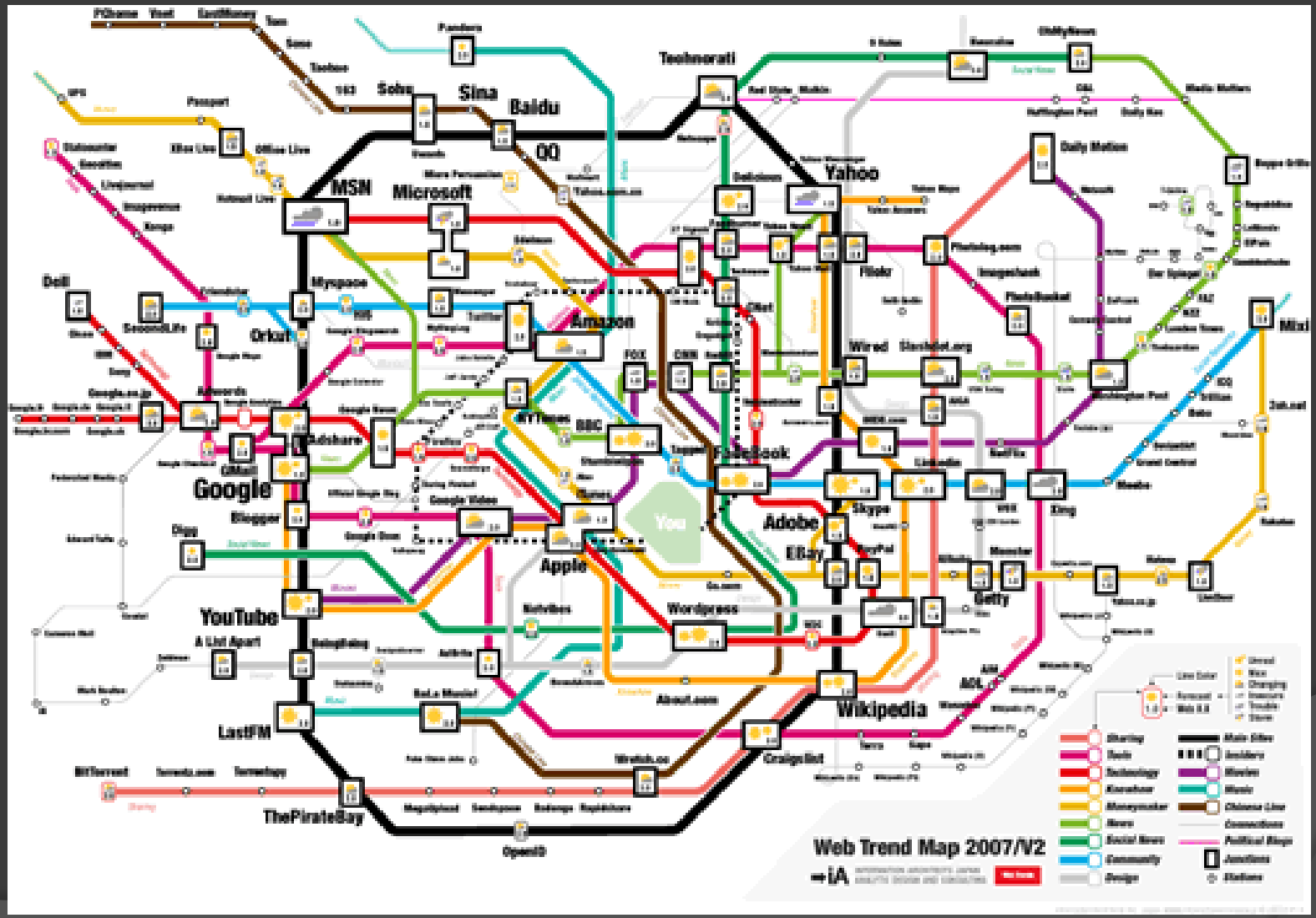
Success stories

Skyblog	8 068 570 blogs	379 025 000 articles	838 000 000 commentaires	3ème site français le plus visité
MySpace	100 000 000 utilisateurs	230 000 nouveaux utilisateurs *par jour*		
FaceBook	46 000 000 utilisateurs	Microsoft achète 5% du capital	Valorisé 10 milliards de dollars	
Et aussi …	Google	Wikipedia	YouTube	



Source : Wikipedia , juillet 2007

Success stories



http://www.informationarchitects.jp/slash/ia_trendmap_start.html

Risques

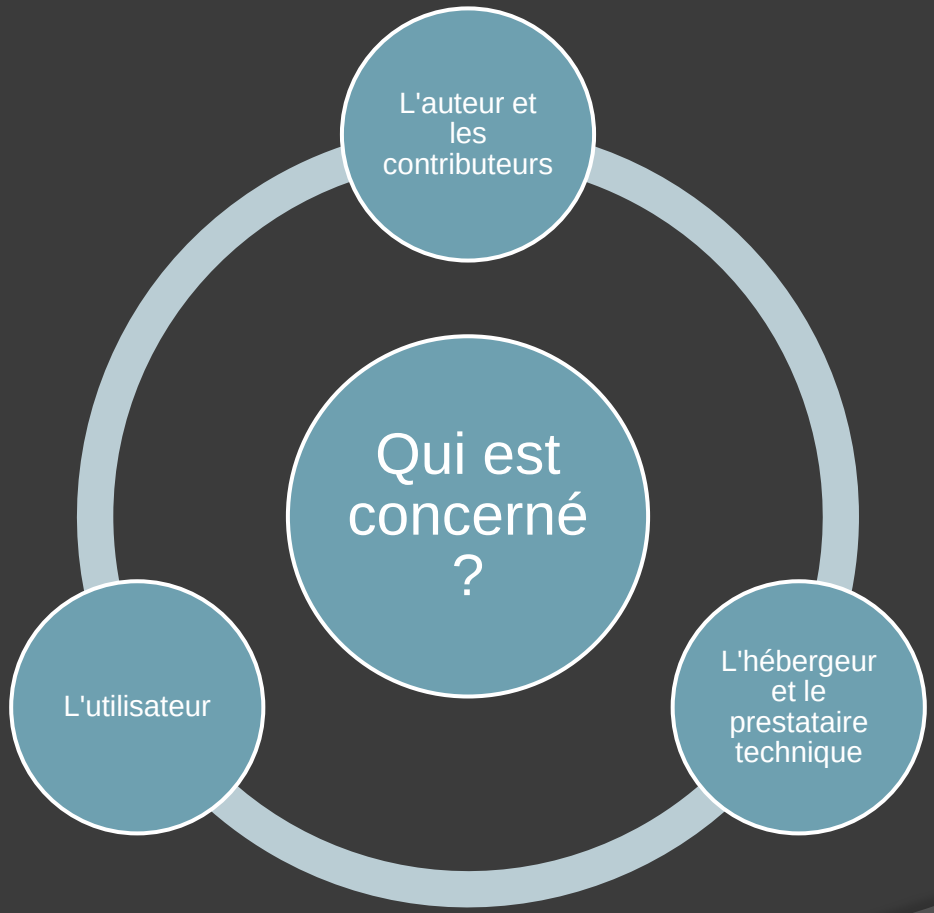
Sécurité 1.0

- Failles techniques
  - *"buffer overflow"*
  - "*heap overflow*"
- Personne ne comprend rien
- Le ROI n'est pas quantifiable
- Peu d'affaires jugées

Sécurité 2.0

- Ancré dans le monde réel
  - eBay vend des voitures
- Touche un large public
- Impacts financiers
  - Vol de données
  - Rapt
  - Manipulation de l'information
- Nombreux procès

Risques


L'auteur et les contributeurs
Qui est concerné ?
L'utilisateur
L'hébergeur et le prestataire technique

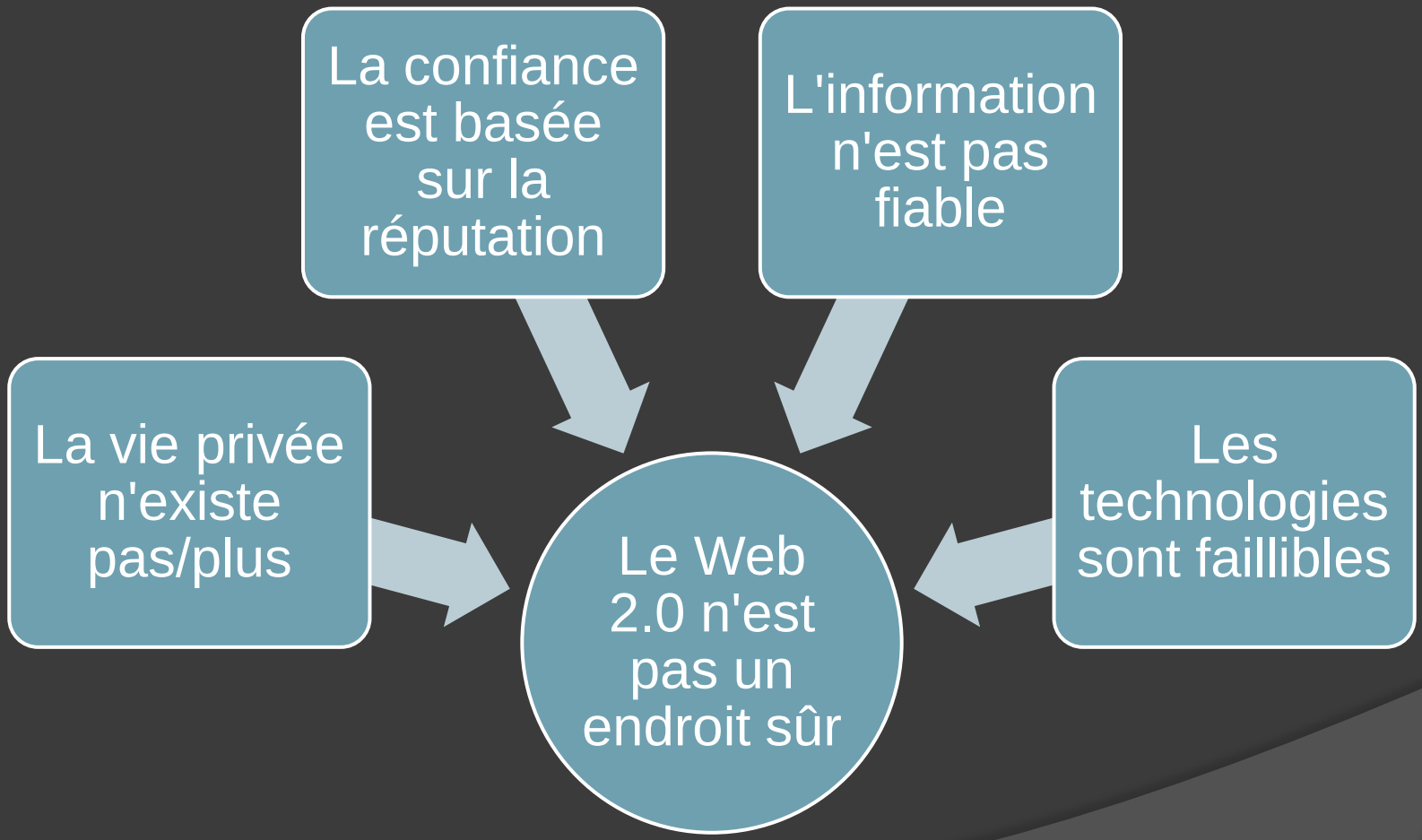
Risques : auteur(s)

- Poursuites judiciaires
  - Les faits sont facilement qualifiables
    - Atteinte à la réputation
      - Ex. diffamation
    - Atteinte à un secret
      - Ex. professionnel, secret de l'instruction, …
  - Affaires célèbres
    - "monputeaux.com"
    - "petite anglaise"
    - Blogs professionnels fermés
      - Inspecteur du travail, policier, proviseur, …
    - Blog des voyageurs Paris-Rouen

Risques : hébergeur

- Poursuites judiciaires
  - Affaires célèbres
    - Affaire "radiateur"
      - Commentaire posté dans un blog
  - Remarque : la LCEN impose aux hébergeurs d'être prudents

Risques : utilisateur



Risques : utilisateur

Vie privée

- Web 2.0 et vie privée
  - La majorité des sites sont hébergés aux USA
    - C'est la loi américaine qui s'applique
  - Le Web 2.0 est financé par la publicité
    - Un ciblage plus fin assure un meilleur revenu
    - Ex. FaceBook, Gmail, Google Analytics

Risques : utilisateur

Vie privée

- Les utilisateurs publient trop d'information
  - Exemples : FaceBook, SkyBlogs, …
  - Résultats :
    - Vol d'identité *complète*
      - Il ne s'agit pas d'un numéro de CB
      - Mais de : mails, agenda, contacts de téléphone portable, adresses enregistrées, amis, etc.
    - MySpace poursuivi en justice pour des affaires de viol
    - Campagne "Everyone knows your name"
- Les moteurs d'indexation sont puissants … et n'oublient rien
  - Ex. ZoomInfo, Paterva (principes)
  - Affaire de la fuite de données AOL

Risques : utilisateur

Vie privée

- Internet semble "anonyme" et "virtuel"
  - Résultats :
    - Défacement de Wikipedia via le réseau Tor
    - Menaces de mort postées dans des blogs
- Les utilisateurs du Web 2.0 sont peu sensibilisés à la sécurité
  - Résultat :
    - Syndrome du "*clic yes*"

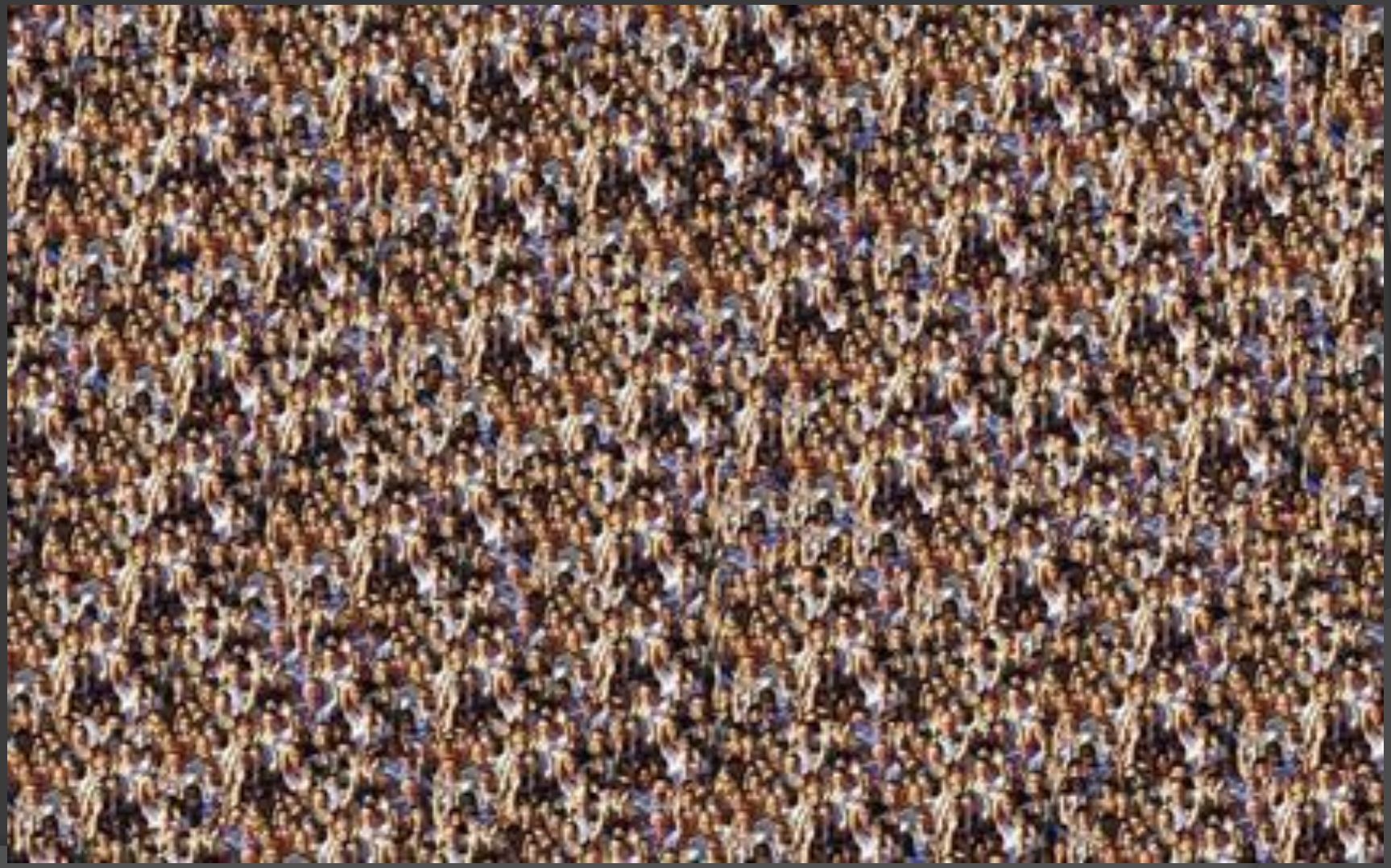
Risques : utilisateur

Confiance

- Web 2.0 et confiance
  - Question : comment gérer les relations entre … 100,000,000 d'utilisateurs ?
  - Réponse : la confiance est basée sur la réputation
  - Problème : la réputation peut être manipulée … ou achetée

Risques : utilisateur

Confiance



Risques : utilisateur

Confiance

- Exemples
  - "Pourquoi les gens sont fascinés par les foules"
    - Achat de votes du Digg par Wired
  - Installation de composants ActiveX et signature AuthentiCode™
  - eBay
    - Vol de comptes à bonne réputation
    - Manipulation de la réputation par JavaScript
      - Source : WebSense

Risques : utilisateur

Confiance

- Autres techniques "marketing"
  - *Google Bombing*
  - Faux blogs (*splogs*)
  - Fausses critiques de produits (ex. Amazon)
  - Exemple : analyse d'un spam FaceBook
    - Source : WebSense

Risques : utilisateur

Information

- Web 2.0 et fiabilité de l'information
  - Emballement de la blogosphère
    - "L'affaire" du purin d'orties
    - Fuite de la clé AACS : 900 000 sites créés en une journée
  - Manipulation de Wikipedia
    - Election présidentielle 2007 : réacteur EPR
    - Certains auteurs mentent sur leurs diplômes
    - Du malware a été ajouté dans certaines pages
    - WikiScanner

Risques : utilisateur

Technologies

- Web 2.0 et technologies
  - Côté client : le navigateur
    - Complexité des protocoles ⇨ failles binaires
    - Conception des normes ⇨ failles conceptuelles
      - Une seule défense : la "Same Origin Policy"
      - Mise à mal par les proxies et les aggrégateurs (ex. Myspace)
    - Exemples
      - Month of the Browser Bugs, failles WMF, VML, ANI, …
  - Côté client : les plugins
    - *Usual suspects* : Quicktime, Flash, Acrobat Reader
    - ActiveX : cf. Month of the ActiveX Bugs

Risques : utilisateur

Technologies

- Côté serveur
  - Deux facteurs de risque majeurs
    - La technologie PHP
      - Cf. Month of PHP Bugs : plus de 50 failles critiques exploitables à distance …
    - Son utilisation par des développeurs peu formés
      - Aucun site PHP qui ne présente un XSS ou une injection …
    - De nombreux outils sont disponibles en phase de post-exploitation
      - Cf. C99shell et autres backdoors Web

Risques : utilisateur

Menaces

- Sécurité côté fournisseur
  - La notion de site "de confiance" n'existe plus
    - Webmaster malicieux
    - Publicité hostile
    - Site compromis par une faille
    - Exemples
      - Web Hacking Incidents Database
      - Technologies SiteAdvisor, SafeBrowsing, etc.
  - Outils de compromission "tout en un"
    - Exemple : MPack
  - L'agrégation de contenus augmente les risques
    - Exemples :
      - Widgets Vista
      - www.google.com/signout ☺

Risques : utilisateur

Menaces

- Attaque niveau 1 : failles PHP "simples"
  - Faille include, injection SQL, évaluation d'expression, etc.
  - Exemple : décembre 2004, ver Santy sur phpBB
- Attaque niveau 2 : injection de code JavaScript
  - XSS permanent, CSRF, etc.
  - Exemples
    - Octobre 2005, ver Samy sur Myspace
    - Month of MySpace bugs
  - Les attaques en cross-site scripting (XSS) deviennent réellement dangereuses !
- Attaque niveau 3 : frameworks JavaScript
  - Exemples : jQuery, AttackAPI, Jikto
  - Attaque de redirection permanente sur GMail

L'avenir

- Le "Web 2.5"
  - Nouveaux services bâtis sur des services Web 2.0
    - Utilisation massive de l'agrégation (*mash-up*)
    - Cf. la liste impressionnante d'APIs JavaScript chez Google
      - http://code.google.com/apis/
    - Et les réalisations obtenues
      - http://www.trivop.com/
      - http://www.netvibes.com/
      - http://www.wikio.fr/
      - Etc.

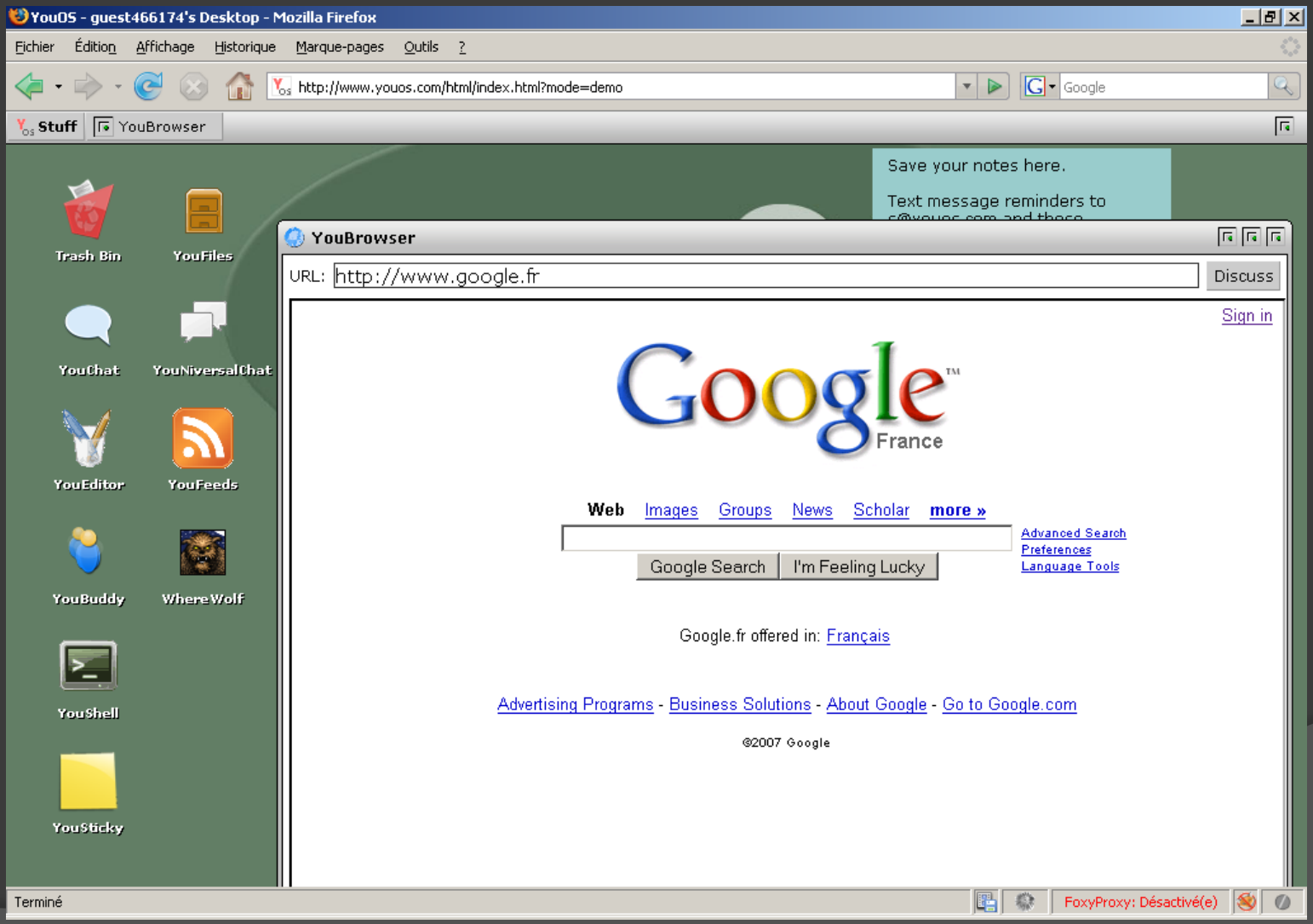
L'avenir

- Le "Web 3.0"
  - Les univers virtuels
    - Second Life, Sony Home, …
    - Il existe un vrai *business model* actuellement
      - Cf. Cisco, IBM, …
  - La transition vers les mobiles
    - Projets
      - Microsoft : SilverLight / Expression
      - Adobe : Flash Light / Device Central
    - D'après Vinton Cerf, c'est l'avenir d'Internet
    - Une chose est sûre : c'est la fin de l'orthographe ☺

L'avenir

- Le remplacement du système d'exploitation par une page Web
  - Projets
    - Adobe : Apollo ⇨ AIF
    - Microsoft : Windows Presentation Foundation
    - Google prépare probablement quelque chose
  - Un aperçu : YouOS.com
    - Un navigateur dans le navigateur

L'avenir


YouOS - guest466174's Desktop - Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
http://www.youos.com/html/index.html?mode=demo
Google
Stuff
YouBrowser
Save your notes here.
Text message reminders to
Trash Bin
YouFiles
YouChat
YouNiversalChat
YouEditor
YouFeeds
YouBuddy
WhereWolf
YouShell
YouSticky
YouBrowser
URL: http://www.google.fr
Discuss
Sign in
Google
France
Web Images Groups News Scholar more »
Advanced Search
Preferences
Language Tools
Google Search I'm Feeling Lucky
Google.fr offered in: Français
Advertising Programs - Business Solutions - About Google - Go to Google.com
©2007 Google
Terminé
FoxyProxy: Désactivé(e)

L'avenir

- Des projets plus exotiques et/ou inclassables
  - Un avatar dans son navigateur
    - http://www.weblin.com/
  - Une "intelligence artificielle" en JavaScript
    - http://www.mycybertwin.com/

Conclusion

- On ne peut pas définir les limites du Web 2.0
  - Mais il existe bel et bien pour ses centaines de millions d'utilisateurs !
- La sécurité "technique" reste une composante du Web 2.0
  - Sécurité des navigateurs
  - Sécurité des serveurs Web
- Mais les *challenges* pour la sécurité posés par le Web 2.0 sont autrement plus difficiles à résoudre
  - Aspects juridiques
  - Contrôle de l'information / lutte contre la rumeur
  - Flux et stockage de l'information distribués
  - Circulation de contenus actifs (frontière code / données floue)
  - Absence d'outils de protection efficaces
  - Etc.

Conclusion

- L'offre de services explose
  - Les applications en ligne sont souvent meilleures que les applications lourdes …
    - En ce qui concerne l'expérience utilisateur (simplicité, mobilité)
  - Les utilisateurs adhèrent massivement
    - Ex. utilisation de Google Calendar et GMail en lieu et place de la messagerie d'entreprise
      - Remplace avantageusement le VPN dans la plupart des usages
    - Ex. Webex
      - Traverse efficacement la NAT et les protections périmétriques
- L'explosion rapide et anarchique des services se fait sans aucune exigence de sécurité

Conclusion

- Quelques pistes pour le RSSI
  - Enumérer les services couramment utilisés
  - Sensibiliser les utilisateurs et offrir des services supplémentaires plutôt que des les contraindre
  - Protéger le navigateur contre les failles
  - Utiliser les outils du Web 2.0 au lieu de lutter contre
    - Alertes Google, identification des blogs d'entreprise, veille des sources d'information, etc.
- Le Web 2.0 reste une plaie pour le contrôle de l'information dans l'entreprise
  - Web 2.0 = réseau humain
  - Donc la participation des utilisateurs est essentielle

Bibliographie et remerciements

- Bibliographie
  - Open Web Application Security Project (OWASP)
    - "Jeopardy in Web 2.0"
  - GNU Citizen
    - "Hacking Web 2.0"
- Remerciements
  - Jean-Denis Gorin, pour sa définition du Web 2.0
  - Renaud Feil (HSC)
  - L'équipe EADS-IW SE/CS