Sécurité du Web 2.0

Nicolas RUFF

EADS-IW SE/CS

nicolas.ruff (à) eads (dot) net

Plan

- Introduction
- Les utilisateurs
- Les utilisateurs : risques
- Les technologies
- Les technologies : risques
- L'avenir
- Conclusion
- Bibliographie & remerciements

Introduction

Qu'est-ce que le Web 2.0 ?

- En 1998 on parlait déjà de "Web sémantique"
  - http://en.wikipedia.org/wiki/Semantic_Web
  - Invention des formats XML, RDF …
- Le terme "Web 2.0" a été "officiellement" inventé par O'Reilly en 2004
  - http://en.wikipedia.org/wiki/Web_2
  - "*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*"
  - Définition très large
  - Aujourd'hui tout le monde dit faire du "2.0" (ou même du "3.0")

Introduction
Définition

- Il n'existe pas de définition "technique"
  - Mais plutôt une définition "sociologique"
  - Dans le Web 1.0 l'utilisateur consulte du contenu
    - Il accède à des sites
  - Dans le Web 2.0 l'utilisateur interagit avec le contenu
    - Il utilise un service
      - Il est à la fois lecteur et auteur
      - Les facteurs clés : simple, convivial, social et communautaire
- Voir également : "the machine is us/ing us"
  - http://youtube.com/watch?v=6gmP4nk0EOE

Introduction
Web 1.0 vs Web 2.0

Web 1.0	*Web 2.0*
DoubleClick	Google AdSense
Ofoto	Flickr
Akamai	BitTorrent
mp3.com	Napster
Britannica Online	Wikipedia
Sites perso	Blogs
Pages vues	Coût au clic
Publication	Participation
CMS	Wiki
Arborescence (taxonomie)	Tags ("folksonomie")
Rigidité du contenu	Syndication

- Source : http://web2rules.blogspot.com/2006/01/what-is-web-20-par-tim-oreilly-version.html

Introduction

- **Web 2.0 = deux facettes**
  - **Les technologies**
    - **Côté client (dont le fameux "AJAX")**
    - **Côté serveur**
  - **Les utilisateurs**
    - **Honnêtes mais manipulables**
    - **Malveillants**
- **Les utilisateurs sont beaucoup plus importants que la technologie**
  - **Pour la sécurité … et le reste (contenu, légalité, …)**

Les utilisateurs

- **Les principes fondateurs pour un service qui marche**
  - **Principe général : 1+1 = 3**
  - **Principes détaillés**
    - **Agrégation (*mash-up*)**
    - **Réseau social / communautaire**
      - **Réseau personnel : blogs, Myspace, …**
      - **Réseau professionnel : Viadeo, Linkedin, OpenBC, Orkut, …**

    - **Basé sur la réputation**
      - **Exemples : Technorati, Digg, Delicious, Reddit … mais aussi eBay**
    - **Simplicité**
      - **Personnalisable sans connaissances techniques**

Les utilisateurs

- Ca n'est pas la technologie qui fait la différence
  - (Si elle fonctionne)

- Exemples de réussites :
  - MSN Messenger / Windows Live Messenger
    - Plusieurs millions d'utilisateurs en France
  - Skyblog
    - 8 068 570 blogs / 379 025 000 articles / 838 000 000 commentaires
    - 3ème site français le plus visité
    - (Source : Wikipedia)
  - MySpace
    - Plus de 100 000 000 d'utilisateurs
    - 230 000 nouveaux inscrits *par jour*
    - (Source : Wikipedia)

- On ne parlera pas des "géants"
  - Google, Wikipedia, YouTube, …

Les utilisateurs
Les risques

- **Avec le Web 2.0, les risques sont nombreux … et réels !**
  - **Contrairement à la sécurité informatique "technico-technique"**
    - **= *buffer overflow*, etc.**
    - **Les non-spécialistes ne comprennent rien**
    - **Peu de plaintes déposées après intrusion**
    - **Peu d'affaires jugées**
  - **Au contraire, le Web 2.0 est ancré dans le monde réel**
    - **Procès, vol d'identité, rapt, manipulation de l'information …**

Les utilisateurs
Les risques

- **Risque #1a : poursuites judiciaires (auteur)**
  - **Les faits sont facilement qualifiables**
    - **Atteinte à la réputation (ex. diffamation)**
    - **Atteinte à un secret (ex. professionnel, secret de l'instruction, …)**
  - **Exemples d'affaires célèbres impliquant des auteurs de blogs**
    - **Affaire "monputeaux.com"**
    - **Affaire "petite anglaise"**
    - **Blogs professionnels fermés : inspecteur du travail, policier, proviseur, …**
    - **Blog des voyageurs Paris-Rouen**

Risque #1b : poursuites judiciaires (hébergeur)

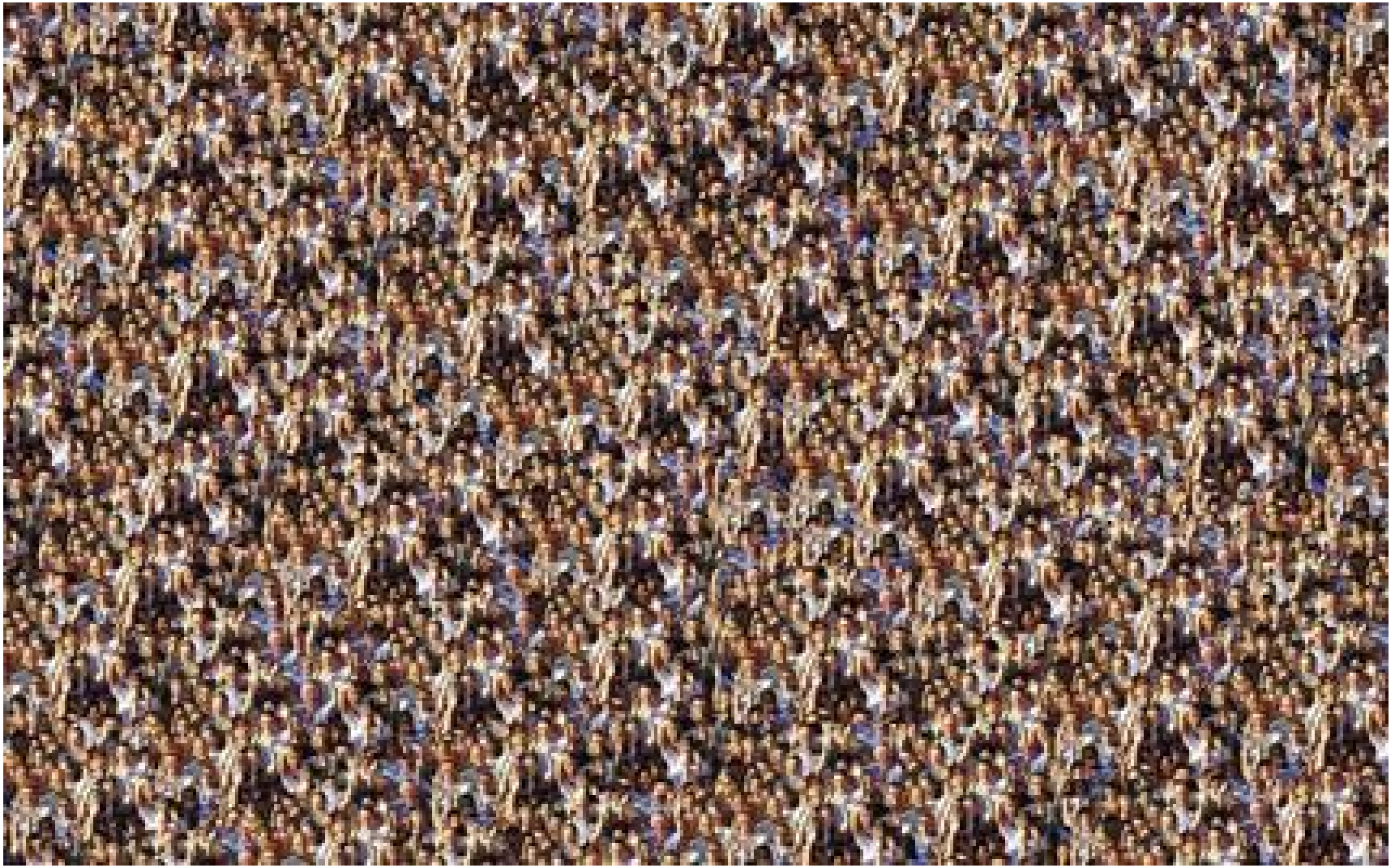
- Exemples d'affaires célèbres impliquant des hébergeurs
  - Affaire "radiateur" (commentaire posté dans un blog)
  - MySpace poursuivi en justice pour des affaires de viol
    - http://www.01net.com/article/339043.html
  - Wikipedia est-il fiable ?
    - Certains auteurs mentent sur leurs diplômes
    - Du malware a été ajouté dans certaines pages

- Remarque : la LCEN impose aux hébergeurs d'être prudents

Les utilisateurs
Les risques

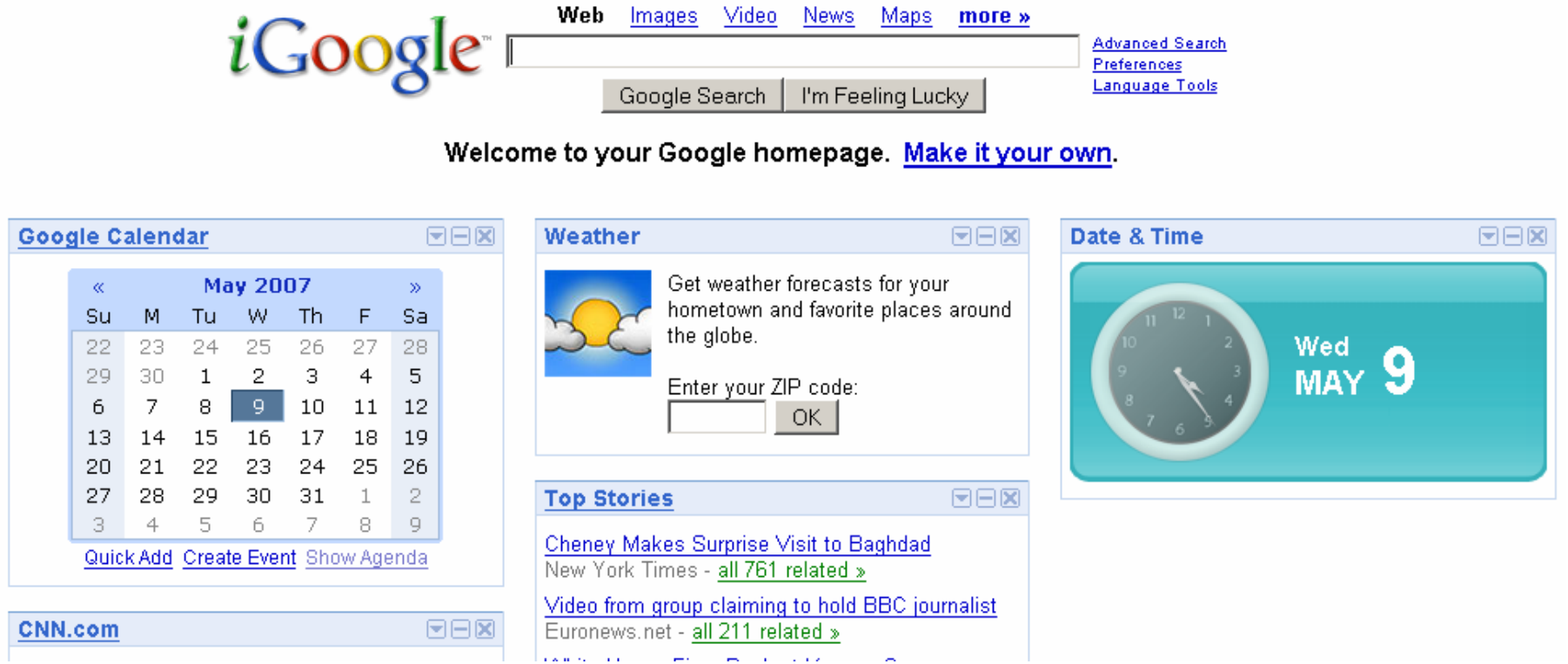
- **Risque #2 : manipulation de l'information**
  - **Le Web 2.0 est basé sur la réputation et l'intelligence collective**
  - **Quelques exemples**
    - **Affaire "pourquoi les gens sont fascinés par les foules"**
      - **Wired a acheté des votes sur Digg (pour quelques centaines de dollars)**
      - **Le journaliste a hissé une image sans intérêt au premier rang du site**
    - **Techniques similaires largement utilisées dans le marketing**
      - ***Google Bombing***
      - **Publication de commentaires élogieux sur les sites de commerce en ligne**
    - **Escroqueries sur eBay avec des comptes à bonne réputation (100%)**
    - **Achat de liens sponsorisés sur des mots clés tendancieux**
    - **Fuite de la clé AACS : 900 000 sites créés en une journée !**
    - **Election présidentielle 2007 et affaire Wikipedia / EPR**

Les utilisateurs
Les risques



- **Risque #3 : 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
        - http://www.webappsec.org/projects/whid/whid.shtml
      - Technologies SiteAdvisor, SafeBrowsing, etc. intégrées aux moteurs de recherche
  - L'agrégation de contenus augmente les risques de propagation automatique d'une attaque
    - Exemple trivial avec Google : que se passe-t-il si l'un des flux inclut www.google.com/signout ? ☺

Les utilisateurs
Les risques



Les utilisateurs
Les risques

- **Risque #4 : sécurité côté utilisateur**
  - Le Web 2.0 draine de nombreux utilisateurs insensibles à la technique
    - Risque de manipulation accru
    - Risque d'infection accru (le syndrome du clic "yes")
    - Vol d'identité
      - Il ne s'agit pas d'un numéro de CB
      - Mais d'une identité complète
        - Mails, agenda, contacts de téléphone portable, adresses enregistrées, amis, etc.
    - Méconnaissance des lois et règles élémentaires
      - Physique du monde réel != Internet

Les utilisateurs
Les risques

- **Remarque : Internet est perçu comme "anonyme"**
  - **Exemples**
    - **Défacement de Wikipedia via le réseau Tor**
    - **Menaces de mort postées dans des blogs**
    - **Diffusion d'informations qui n'auraient pas lieu d'être**
      - **Il suffit de surfer sur Skyblog pour s'en rendre compte**
      - **Cf. campagne de protection de l'enfance américaine**
        - **"Everyone knows your name"**
        - **http://www.youtube.com/watch?v=hOwpGF1SOQM**

Les technologies

- **HTML / DHTML / XML**
  - **Les technologies de base**
    - **Très simples sur le principe**
    - **Déclinée dans des sous-formats spécialisés (XHTML, RSS, Atom, …)**
- **CSS : les feuilles de style**
  - **Très simple également**
  - **Mais très importante pour la "personnalisation" (*skinning*)**
- **JavaScript**
  - **Un langage de programmation complet orienté object**
  - **Interpréteur *stand-alone* (SpiderMonkey)**
  - **Ex. ViaMichelin réalise le calcul d'itinéraire côté client en JavaScript**
- **AJAX**
  - **AJAX = Asynchronous Javascript And XML = XMLHTTPRequest( )**
  - **L'aspect "asynchrone" est beaucoup plus important que l'aspect XML !**

Les technologies

- JSON (JavaScript Object Notation)
  - Sérialisation d'objets (donc de code) JavaScript
- Technologies de support côté client
  - Java, Flash, QuickTime, …
    - Mais tout ce qui nécessite une phase de compilation n'est pas "interactif"
- Technologies de support côté serveur
  - Finalement peu nombreuses
    - Tout le travail est effectué côté client sur le navigateur

Les technologies
Côté client : dangers

- Le navigateur
  - Complexité incroyable => failles
    - Sans compter les plugins
  - Fonctions non intégrées à la conception => failles
    - Ex. exécution asynchrone de scripts
  - Exemples
    - Failles WMF, VML, ANI, …
    - Month of the Browser Bugs
  - Seule défense : la "Same Origin Policy"
    - Mise à mal par les proxies et les aggrégateurs (ex. Myspace)
- Le danger venait de l'extérieur
  - Quicktime : exécution de code JavaScript, faille Java, …
  - Flash : ActionScript 3.0 a une méthode connect() …
  - Acrobat Reader : faille d'exécution de script via les paramètres
  - ActiveX : cf. Month of the ActiveX Bugs

Les technologies
Côté serveur : dangers

EADS

- **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**
      - **http://michaeldaw.org/projects/web-backdoor-compilation/**

Les technologies
Historique des attaques

- **Phase 1 : exploitation de failles PHP "simples" par de l'injection de code PHP**
  - **Faille *include*, injection SQL, évaluation d'expression, etc.**
  - **Exemple : décembre 2004, ver Santy sur phpBB**
- **Phase 2 : exploitation de failles par de l'injection de code JavaScript**
  - **XSS permanent, faille QuickTime, etc.**
  - **Exemples**
    - **Octobre 2005, ver Samy sur Myspace**
    - **Month of MySpace bugs**
  - **Les attaques en *cross-site scripting* (XSS) deviennent réellement dangereuses !**
- **Phase 3 : *frameworks* complets d'intrusion en JavaScript**
  - **Exemples : jQuery, AttackAPI, Jikto**

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.**

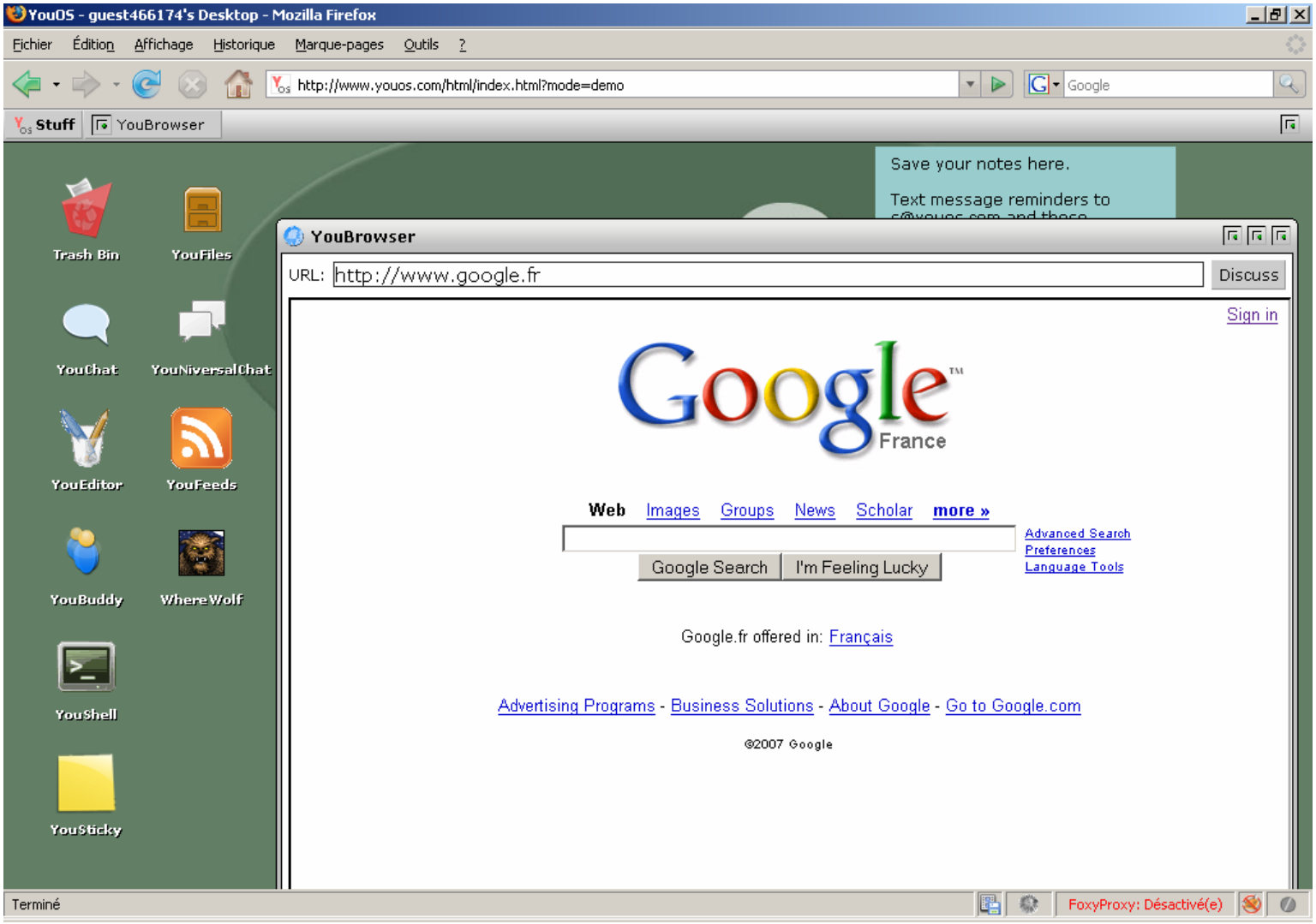
L'avenir

- **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**
    - **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"
  - http://www.owasp.org/index.php/OWASP_Papers/Jeopardy_in_Web_2_0

Remerciements

- Jean-Denis Gorin, pour sa définition du Web 2.0
- Renaud Feil (HSC)
- L'équipe EADS-IW SE/CS