

Histoire et actualité de l'informatique

Évolution, problèmes, perspectives

Sacha Krakowiak

Université de Grenoble

Séance 5
Le World Wide Web,
les nouvelles applications
Années 1990-2000

dimanche 6 février 2011

Les années 1990-2000

- ❖ Naissance et expansion du World Wide Web
- ❖ Les applications réparties
- ❖ Les systèmes embarqués
- ❖ Sécurité de fonctionnement
Disponibilité, sécurité, qualité de service
- ❖ La bio-informatique
- ❖ Les applications médicales
- ❖ Les applications «grand public» et la numérisation du monde

© 2011, S. Krakowiak
dimanche 6 février 2011

Histoire de l'informatique

5 -2

Naissance du World Wide Web

❖ Un besoin d'utilisateurs ...

Des physiciens du CERN (Centre Européen de Recherche Nucléaire) souhaitent partager des données réparties dans le monde (sur des machines hétérogènes)

En 1990, Tim Berners-Lee (avec Robert Cailliau) propose un outil à base de liens hypertexte, le World Wide Web

En 1991, le système est ouvert à tous sur l'Internet, mais ses principaux utilisateurs restent des physiciens



❖ Le début de l'essor

1993 : Le premier navigateur graphique, Mosaic, est créé à l'université d'Illinois par Marc Andreessen et Eric Bina

1994 : Mosaic est à la base de la création de  Netscape
Première conférence internationale sur le Web
Création du World Wide Web Consortium 

© 2011, S. Krakowiak
dimanche 6 février 2011

Histoire de l'informatique

5 -3

C'est quoi, au juste, le Web ?

❖ La notion de base, le lien hypertexte

Idée ancienne : Vannevar Bush, *As We May Think*, 1945

Forme courante, l'URL (*Uniform Resource Locator*) [aussi l'URN]

http:// ... pour une «page» sur un site de l'Internet

file:/// ... pour un fichier sur une machine, mailto:// pour une adresse mail, ...

❖ Un langage de description de documents : HTML

Utilise des marqueurs (annotations dans le texte)

Permet d'insérer des liens dans le texte des pages Web

❖ Un protocole de communication : HTTP

❖ Il faut aussi des outils ...

Le navigateur : pour se déplacer en suivant les liens

Le moteur de recherche : pour chercher l'information

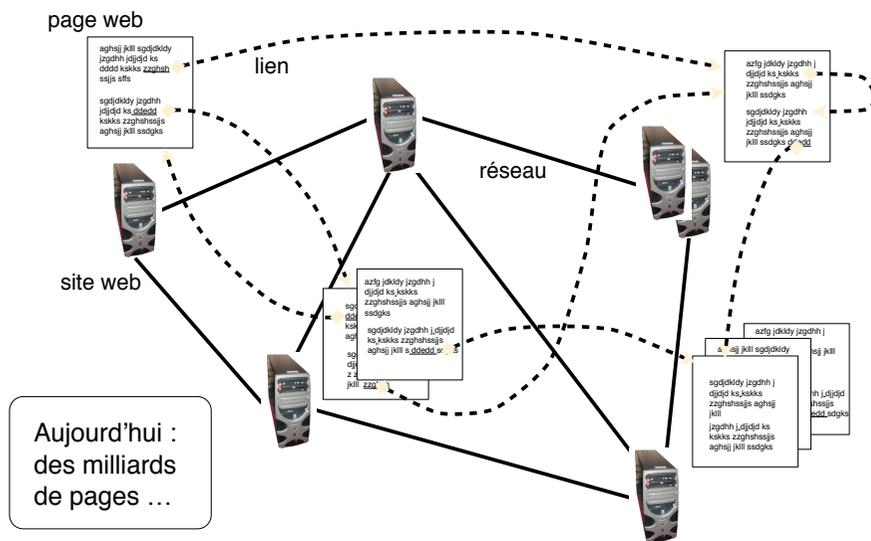
L'éditeur : pour fabriquer des pages Web

© 2011, S. Krakowiak
dimanche 6 février 2011

Histoire de l'informatique

5 -4

Organisation du Web



Brève histoire du développement du Web

❖ Les outils de base

Navigateurs :

Netscape (1994), Internet Explorer (1995), Mozilla (1998) et Firefox (2005), Chrome (2008), ...

Moteurs de recherche et annuaires :

AltaVista (1995), Yahoo! (1995), Google (1998), Exalead (2006), Bing (2009)

Construction de sites : des centaines, beaucoup de livres, PHP-MySQL, ...

Un langage : Java (Sun, 1995) - dépasse beaucoup le cadre du Web

❖ Les applications

Commerce électronique

Services : Transports, voyages, banque, météo, ...

Administration : Impôts, information, inscriptions, ...

Diffusion de contenu : Presse, agences, radio, vidéo, publication scientifique, bibliothèques, ...

Réseaux sociaux : TheGlobe, Geocities (1994), ... Facebook (2005)

2001 : la bulle
des «dot-com»

La numérisation du monde

❖ Le passage des informations sous forme numérique ...

Documents

Dessins, graphiques, photos, ...

Vidéo, films

Son (parole, musique)

❖ ... et ses conséquences

L'accès à l'information devient indépendant du matériel

L'ordinateur comme moyen d'accès et moyen de production

L'importance des normes publiques (PDF, JPEG, MP3, etc.)

❖ Un nouveau paysage

Les services : le web comme point d'entrée universel

Les systèmes embarqués : l'informatique interagit avec le monde

Le Web aujourd'hui

❖ Le Web interactif

Les utilisateurs ne se contentent pas de lire : ils interagissent et apportent du contenu

Exemples

les blogs (*weblog*), les forums, ...

les réseaux sociaux

la publication en ligne (articles, cours, ...)

❖ Le Web sémantique

Objectif ambitieux, à long terme

Idee : fournir un meilleur service aux utilisateurs, en automatisant davantage de tâches par un «raisonnement» sur le sens

Exemple : moteur de recherche plus «intelligent»

Moyens : intelligence artificielle, nouveaux langages permettant des associations, ...

Les systèmes embarqués

❖ Quelques définitions

Système embarqué : système informatique associé à un objet physique

Interaction dans les deux sens : mesure (capteurs), commande (actionneurs)

Système en temps réel : système soumis à des contraintes de temps

Système critique : système dont la défaillance peut entraîner des conséquences catastrophiques (pertes de vie humaines, ...)

Beaucoup de systèmes embarqués sont aussi temps réel et critiques

❖ Brève histoire

Années 60 : systèmes de guidage de missiles (militaires)

Années 70 : routeurs, guidage de fusées (Apollo), fabrication automatisée, chimie

Années 80 et 90 : large extension (transports, énergie, télécommunications, satellites, carte à puce, terminaux de paiement, etc.)

Années 2000 : croissance explosive (téléphones, électro-ménager, puces radio (RFID), réseaux de capteurs, voitures, trains, avions, équipements médicaux, ...)

Les systèmes embarqués

❖ Des problèmes ...

Les s.e. sont soumis à des contraintes : coût (d'où limites sur mémoire, processeurs), consommation d'énergie, environnement

S'y ajoutent les aspects «temps réel» : respect des échéances

Pour les systèmes critiques, la sûreté de fonctionnement est cruciale

❖ ... et quelques voies d'approche

Conception conjointe matériel-logiciel

«Durcissement» du matériel (pour environnement hostile)

Programmes optimisés (taille, élimination des fonctions inutiles)

Modèles d'exécution spécifiques (langages synchrones)

Vérification rigoureuse (*model checking*)

Noyaux de systèmes spécialisés et certifiés

Tolérance aux fautes

Confiance *justifiée* dans le bon fonctionnement

Tolérance aux fautes

❖ Les systèmes informatiques, comme tout système, sont sujets à des défaillances ...

Défaillance : le système ne remplit pas sa fonction

il ne fonctionne pas du tout (et ne fait rien)

il fonctionne, mais donne des résultats incorrects, ou pas à temps

il fait «n'importe quoi» ...

❖ À l'origine d'une défaillance, il y a toujours une «faute»

Usure du matériel, circonstances extérieures (météo, etc.)

Erreur humaine (conception, programmation, ...) ou malveillance

❖ Il n'est pas possible d'éliminer toutes les fautes

Il faut donc vivre avec !

La tolérance aux fautes repose sur la redondance

Données et traitements en double, triple, ...

Solutions techniquement complexes, progrès dans les années 1990

Les bugs (bogues)

❖ Il n'y a pas de *bugs* informatiques, il n'y a que des erreurs humaines

“Les programmeurs parlent de *bugs* pour préserver leur santé mentale. Reconnaître un pareil nombre d'erreurs serait psychologiquement insupportable.”

Martin Hopkins, 1968

❖ Quelques *bugs* (tristement) célèbres

Les accidents d'irradiation de Therac 25 (1985-87)

Le ver de Morris (exploitation malveillante d'un *bug* d'Unix, 1988)

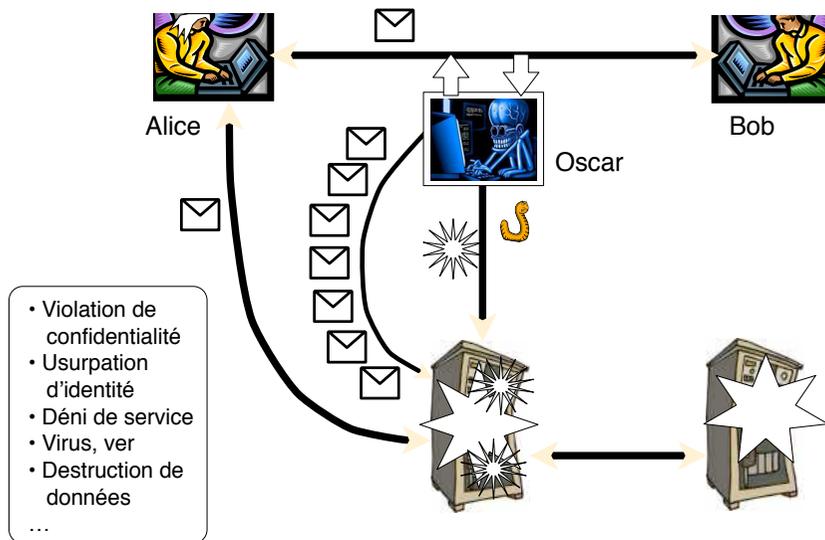
La panne du réseau téléphonique ATT (1990)

La perte d'Ariane 5 lors de son premier vol (1996)

La perte de la sonde Mars Climate Orbiter (1999)

La panne d'électricité au Nord-Est des États-Unis (2003)

Problèmes de sécurité informatique



Quelques instruments de la sécurité

- ❖ Dissimuler une information
 - La rendre indéchiffrable même si elle est captée (cryptographie)
 - La cacher dans une autre information d'apparence anodine (stéganographie)
- ❖ Authentifier une personne ou une organisation
 - Fournir une preuve certifiée de son identité
- ❖ Authentifier un document
 - Signature électronique
- ❖ Protéger l'accès à une ressource
- ❖ Détecter une intrusion
 - Au besoin, la provoquer pour piéger l'adversaire ...
- ❖ Détecter et détruire un virus

La sécurité reste un problème encore mal maîtrisé ...

Une avancée importante pour la sécurité

❖ La cryptographie à clé publique

Diffie, Hellman, Merkle (1976) ; Rivest, Shamir, Adleman (1978)

La cryptographie «classique» repose sur le *partage* d'une clé secrète

Mais un secret partagé risque de ne pas rester secret

❖ Deux clés pour chacun ...

Une clé publique, connue de tous

Elle sert à chiffrer les messages envoyés

Une clé privée, *connue de son détenteur seul*

Elle sert à déchiffrer les messages reçus

Il est (bien sûr) *très difficile* de trouver la clé privée ...

❖ Une propriété remarquable

Le même principe permet aussi l'authentification (preuve d'identité)



RSA : un protocole très utilisé dans le commerce électronique, la banque, etc. (le petit cadenas sur les pages web)



Aspects de la sécurité informatique

❖ Aspects scientifiques et techniques

Les outils techniques existent ...

... mais des progrès à faire sur les aspects fondamentaux

Une base logique pour la sécurité ?

❖ Aspects légaux et réglementaires

Infrastructure à clés publiques

Signature électronique, certificats

Tiers de confiance

❖ Aspects sociétaux

Des progrès à faire sur la diffusion de la culture de sécurité ...

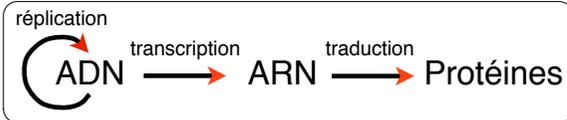
Appréciation des risques, comportements dangereux

Utilisation des outils

... et sur l'équilibre entre sécurité et respect de la vie privée

La bio-informatique

- ❖ Schéma de base de la biologie moléculaire



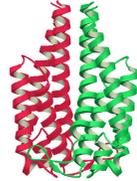
- ❖ Analyse de l'information génétique

Séquencement du génome humain (2004)

3,2 milliards de paires de bases, environ 30 000 gènes

- ❖ Analyse de la structure des protéines

Repliement des protéines, analyse en 3 dimensions



- ❖ Dynamique de la transcription

- ❖ Bio-informatique des populations

- ❖ Qu'apporte l'informatique ?

Algorithmique, analyse d'images, fouille de données, analyse statistique, ...

Une discipline en développement rapide

L'informatique médicale

- ❖ Imagerie médicale

une révolution : scanner, IRM

- ❖ Chirurgie assistée par ordinateur

assistance aux gestes diagnostique ou thérapeutique

objectif : réduire l'invasivité, augmenter la précision

s'appuie sur les techniques d'imagerie et de modélisation

- ❖ Traitement et stockage de l'information médicale

informatisation des dossiers médicaux

systèmes d'information hospitaliers

- ❖ Aide à la décision

aide au diagnostic

aide à la prescription

- ❖ Assistance en temps réel

monitoring

télésurveillance

Bilan des années 1990-2000

- ❖ Avancées

L'explosion du Web et l'informatique grand public

La «numérisation du monde»

Le développement des systèmes embarqués

Des progrès dans la construction de programmes corrects

Des avancées en bio-informatique et informatique médicale

- ❖ Limites

La sécurité reste un problème mal résolu

Le calcul parallèle est encore mal compris

Les impacts sociétaux sont mal évalués et mal maîtrisés