

# La génération «Technologies de l' Information»

Un point de vue technique



Vous avez peut-être déjà été confrontés à une situation similaire, du moins si vous avez un âge relativement proche du mien (ce que je ne vous souhaite pas forcément, enfin bref). Voilà la situation : Vous passez un après-midi agréable chez de très bon amis de longue date, et vous vous remémorez quelques événements et aventures marquants que vous avez passé ensemble. Bien sûr, les péripéties ayant présenté un certain risque sont celles dont on se souvient le plus volontiers. «Tu te rappelles, lorsque nous étions sur ce glacier à plus de 3000 mètres, dans la tempête, avec deux touristes en hypothermie dont l'un s'était fait une entorse, et qu'on ne savait plus comment s'en sortir...». A ce point de l'évocation, peut-être avez-vous entendu une voix juvénile intervenir «Mais pourquoi vous avez pas téléphoné pour appeler à l'aide ?». Alors, vous lui avez expliqué qu'à cette époque, il n'y avait pas de réseaux mobiles, et que de ce fait, on ne pouvait pas simplement téléphoner pour appeler «Au secours». Là, votre jeune interlocuteur a peut-être lâché : «Oh, mais alors, c'était il y a très longtemps !».... Oui, ben, bonjour le coup de vieux !

Le fait est que la génération du tournant du siècle n'a que peu d'expérience d'un monde où l'information n'est pas à portée immédiate, toujours et partout. De plus en plus, il faut faire un effort pour ne plus être exposé à l'information, alors que les générations précédentes ont plutôt l'expérience inverse, où c'est l'accès à l'information qui demande un effort notable. Cette situation a été rendue possible par la technologie, une

technologie que les générations précédentes ont développée, et que la génération actuelle devra améliorer et adapter. Mon propos n'est pas de me livrer à une étude sociologique de la génération actuelle confrontée à ces technologies, mais d'esquisser grossièrement comment sont nées ces technologies, et comment cet arsenal que nous avons créé pourrait être amélioré pour et par la génération actuelle. Avons-nous bien créé la technologie appropriée pour le monde que nous voulions pour nos enfants ? Vaste question, qui n'a pas de réponse univoque, mais question qui mérite qu'on se la pose aussi souvent que possible, en tant qu'ingénieur et en tant qu'*homo sapiens*. Le propos sera donc essentiellement technologique; bien entendu, c'est l'occasion d'enfoncer quelques portes ouvertes : cela tombe plutôt bien, parce qu'avec l'âge, on devient un peu paresseux, et il est moins fatigant d'enfoncer des portes ouvertes que fermées à double tour...

Nous commencerons par énumérer brièvement quelques étapes (sans aucun souci d'exhaustivité) ayant conduit au paysage technologique actuel, puis nous examinerons d'un œil critique quelques aspects de ce paysage actuel



## D'abord... Communiquer

- Tamtams, signaux de fumée, ...
- Télégraphe électromagnétique (Morse 1837)
- Câble transatlantique (1866) 4200 km, 7000 t
- Téléphone (1876) Alexander Bell et Elisha Gray
- Radio (1900) Nikola Tesla, Guglielmo Marconi
- Numérisation d'un signal de parole (Reeves, 1937)
- Étalement de spectre (H. Lamarr et G. Antheil, 1941)

- La peinture est de Frédéric Remington, le célèbre peintre du Far West américain. Il semble ainsi démontrer que les signaux de fumée chers à Lucky Luke se fondent sur des faits réels...
- La communication, dans les temps reculés, consiste essentiellement à transmettre un ou deux bits d'information, correspondant à l'apparition ou non d'un événement donné : dans le tableau ci-dessus, on peut imaginer que des éclaireurs annoncent à la tribu que les bisons arrivent. Dans un autre contexte, cette même fumée annoncera qu'on a réussi à flanquer la pâtée à nos ennemis. Oui, parce que si on a pris la pâtée, il n'y a probablement plus personne pour le signaler...
- On a de tous temps cherché à communiquer à distance; la plus ancienne communication dont nous ayons gardé la trace (à ma connaissance) date du XII<sup>ème</sup> siècle avant JC, dans l'Odyssée d'Homère, quand Ulysse relate la prise de Troie à l'aide du fameux cheval creux, il signale par des signaux lumineux aux Grecs cachés sur l'île de Ténédos que la ville de Troie est ouverte et peut être prise. Pour la petite histoire, connaissant la distance approximative entre le site de Troie et l'île en question, il a probablement fallu un demi-stère de bois pour le feu. En somme, beaucoup d'énergie pour transmettre un bit d'information...
- En 1937, Reeves avait démontré, prototype à l'appui, que l'on pouvait transmettre un signal analogique (la voix) de manière numérique; c'est la modulation par impulsions et codage (MIC) qui
- Signalons en particulier la technique à étalement de spectre, imaginée par l'actrice

Hedy Lamarr et le compositeur George Antheil en 1941; cette technique est actuellement presque universellement utilisée par les communications mobiles, le WiFi et les communications sans fil de proximité. Il n'est pas toujours nécessaire d'avoir fait de grandes études scientifiques pour avoir de grandes idées...



## Les théoriciens...

Claude Shannon est considéré comme le père de la théorie de l'information, mais beaucoup d'autres ont contribué, comme Alan Turing, John von Neumann, etc...

Les premiers calculateurs électroniques (Z1 de Konrad Zuse), ou ENIAC (conçu par J.W. Mauchly) voient le jour dès 1941, mais n'ont aucune application commerciale

- Claude Shannon est la figure importante de la théorie de l'information; en réalité, on devrait plutôt parler d'une théorie de la transmission de l'information. Il n'existe actuellement pas de théorie permettant d'attribuer une valeur à l'information elle-même, cette valeur étant essentiellement subjective. C'est heureux pour de nombreux auteurs de «news», dont certains dirigeants politiques, d'ailleurs...
- Avant Shannon, les télécommunications concernent essentiellement les humains, ou la téléphonie. On sait téléphoner à travers l'Atlantique, mais la communication entre des machines n'est pas d'actualité : forcément, puisqu'il n'y a pas de machines qui pourraient communiquer ensemble ! La deuxième guerre mondiale va créer un besoin pour des mécanismes permettant de communiquer de manière discrète et cryptée, le cryptage manuel se révélant insuffisant pour les radiocommunications télégraphiques. Parallèlement, les besoins en calcul balistique pour les tirs d'artillerie à longue distance accentuent le besoin de calculateurs spécialisés. C'est cette application qui motivera le développement d'ENIAC, un ordinateur à programme câblé.

## Les premiers ordinateurs...



UNIVAC est commercialisé en 1951..



FORTRAN est décrit à partir de 1954, puis LISP, ALGOL et COBOL.

- UNIVAC est le premier ordinateur commercial. Il pèse 13 tonnes et ses 5200 tubes à vide consomment 125 kW. A la base, c'est un développement d'ENIAC. Son plus célèbre exploit est d'avoir prédit l'élection de Eisenhower à l'élection présidentielle de 1952, alors que les sondages «humains» l'annonçaient perdant. Une performance pas si anodine que cela si l'on se souvient de quelques sondages récents réalisés avec toute la puissance des ordinateurs dits modernes... Avec UNIVAC vont aussi apparaître les premiers langages de programmation, sous l'impulsion de John Backus et Grace Hopper.
- Parmi les grandes figures de l'informatique dans les années 50, citons Grace Hopper (la «mère» du langage COBOL, Common Business Oriented Language, la seule femme sur l'image ci-dessus) et John Backus (inventeur de FORTRAN, a FORMula TRANslator). Les deux principales utilisations de l'ordinateur de l'époque sont déjà claires : le commercial avec COBOL, et le calcul scientifique, d'abord à usage militaire, puis plus purement orienté vers la recherche, avec FORTRAN. Mais par derrière se profile déjà l'application algorithmique, avec ALGOL, dont sera plus tard tiré une large famille de langages dont C, PASCAL, et Java, et l'intelligence artificielle avec LISP.
- J'aurais beaucoup aimé connaître Grace Hopper : cette dame est sans doute une des personnalités les plus hors du commun de l'histoire de l'informatique : jusque peu avant son décès en 1992, à l'âge de 86 ans, elle continue à être employée par Digital Equipment, entreprise pour laquelle elle donne des conférences. Elle a travaillé

pendant la majeure partie de sa vie dans un univers machiste (l'armée) où même l'actuel président des Etats-Unis passerait pour féministe... En 2016, Barack Obama lui décernera à titre posthume la médaille présidentielle de la Liberté.



## L'apparition du transistor

- CDC-1604
- Premier ordinateur transistorisé en 1960 (design de Seymour Cray)
- 192 kByte de RAM, fréquence d'horloge de 300 kHz



- PDP-8 (Digital Equipment Corporation)
- Considéré comme le premier mini-ordinateur
- Tenait sur un chariot...

- Le début des années soixante voit l'apparition du CDC (Control Data Corporation) 1604, ordinateur à transistors. Il sera suivi par de nombreux autres modèles jusqu'en 1992, lorsque la société fut vendue à une filiale de British Telecom.
- L'un des fondateurs de CDC fut Seymour Cray, qui fonda par la suite Cray Research, qui développa des super-calculateurs dont la série Cray X-MP, par exemple.
- Le premier ordinateur que j'aie programmé (très modestement) était un CDC 6600.
- Digital Equipment Corporation, fondé en 1957, propose ses premiers ordinateurs de «petite» taille. Cette gamme d'ordinateurs va jouer un rôle essentiel dans le développement de l'informatique actuelle. La gamme PDP-11, de coût relativement réduit, sera un immense succès et permettra à de nombreuses personnes d'accéder aux développements en informatique.



## Les années 70, l'âge d'or...

- La révolution informatique !
- Naissance du système d'exploitation UNIX par Kenneth Thompson
- Naissance de C par Dennis Richie, puis réécriture de UNIX en C
- Diffusion de UNIX en dehors du cercle de Bell Labs
- L'université de Californie à Berkeley décide de participer au développement (premières versions «BSD»)

- Les années 70 sont les années où presque toute l'informatique telle que nous la connaissons a été inventée.
- Bell Labs se sert de son monopole des télécommunications pour entretenir une équipe de chercheurs redoutablement efficaces. Citons outre Kenneth Thompson et Dennis Richie, Brian Kernighan
- La disponibilité d'ordinateurs devenant abordables (PDP-7, puis PDP-11), lié à la disponibilité d'ingénieurs enthousiastes suite à l'abandon du projet Multics par Bell Labs permet de réaliser quelques produits qui restent toujours d'actualité, 50 ans après. Bell Labs va ouvrir le code source, réécrit en C, de Unix à la communauté, entre autres l'université de Berkeley, ce qui a rendu Unix pérenne (Mac OS, Linux, iOS).
- Mac OS est un lointain descendant de UNIX (noyau du système d'exploitation UNIX BSD 4.2). Il en va de même pour iOS.
- Linux est à la base une réécriture de UNIX; donc, Android est également tributaire de UNIX; partant, la quasi-totalité des téléphones portables a des racines UNIX. Il en va de même pour les téléviseurs modernes, qui utilisent des versions customisées de Linux ou d'Android (Android TV, Web OS, etc...).
- C reste actuellement encore un des langages les plus utilisés dans le monde; de nombreux langages s'inspirent de C, comme Java et C++.
- Certains ont pensé que C avait été écrit pour faire perdre du temps aux développeurs; en réalité, la généreuse permissivité du langage fit d'abord perdre du temps aux

dépanneurs confrontés à des erreurs de logiciel fort obscures. Ce qui est certain, c'est que C est probablement le langage qui a coûté le plus de temps en discussions sur la pertinence d'un langage. La plupart des guerres de religion en informatique sont liées de près ou de loin au langage C. Moi-même, lorsque je suis arrivé dans cette école, venant de l'industrie et de C++, j'ai été pris à partie par des collègues partisans de langages «meilleurs» et mieux construits. «C est un bricolage qui n'aurait jamais dû sortir des laboratoires», ou «C est une aberration inutilisable pour la constitution d'un programme informatique sérieux», ai-je pu ainsi entendre. Et moi qui venais d'une équipe qui avait publié des dizaines de milliers de lignes en C et C++... Enfin, c'est toujours intéressant d'apprendre que ce que vous avez réalisé était une bêtise.

- Parallèlement, mentionnons la firme Digital Equipment Corporation, qui développe le système d'exploitation VMS (Virtual Memory System) qui sera commercialisé en 1981. Une partie de l'équipe de développement de VMS va plus tard se retrouver chez Microsoft, où ils développeront Windows NT. De VMS à WNT, il n'y a que le décalage d'une lettre dans l'alphabet...

## La micro-informatique



- Premiers ordinateurs «personnels»
- IBM 5100
- HP 98XX
- Apple I et II, puis III
- ARPAnet (l'ancêtre de Internet) est développé dans les universités et va profiter de la disponibilité de UNIX
- Il y a 5 machines connectées à ARPAnet dans le monde.

- Après 1975 apparaissent les premiers ordinateurs «personnels» ainsi que les premières calculatrices programmables.
- IBM est le premier à proposer une machine, mais trop chère et qui n'aura pas de succès. Hewlett Packard est orienté vers le calcul scientifique et l'acquisition de données de mesure, et ses calculatrices programmables ne sortiront guère des universités et laboratoires.
- L'Apple II va devenir le premier ordinateur personnel vraiment «grand public», conçu par Steve Wozniak, il possède des cartes permettant d'étendre ses fonctionnalités. Indépendamment de Apple, un jeune programmeur indépendant, Dan Bricklin, publie le programme Visicalc, qu'il met librement à disposition des utilisateurs de Apple II. Ce premier tableur grand public sera un succès mondial, mais Dan Bricklin ne récoltera rien en retour, bien que son programme soit sans doute un artisan majeur dans le succès de l'Apple II, et de Apple en général.
- Après l'Apple II, Apple règne en maître absolu sur l'informatique personnelle. C'est un immense succès commercial.
- Le successeur de l'Apple II, l'Apple III, réalisé à partir d'une idée de base de Steve Jobs, sera un flop commercial sans précédent (et à ce jour sans équivalent connu). Steve Wozniak dira plus tard de l'Apple III qu'il a connu un taux d'échecs de 100%.
- Comme quoi...Etre un grand visionnaire ou un grand idéaliste n'implique pas d'avoir raison, ni d'avoir le succès mérité...
- Avec le début des années 1970 et la disponibilité de Unix dans diverses universités,

ARPAnet est développé : plus tard, cela deviendra Internet.



## La démocratisation

- Sortie de l'IBM PC en 1981
- Malgré ses très nombreux défauts, ce sera un immense succès
- Malgré le succès, IBM ne croira pas en l'avenir de ce produit, allant même jusqu'à brader le système d'exploitation à une jeune firme méconnue
- Il y a 300 machines connectées à Internet dans le monde
- L'Europe téléphone en numérique, avec ISDN (RNIS)

- 1981, alors que Apple a manqué de trouver un successeur à l'Apple II, IBM propose l'IBM PC. Le nom d'IBM suffira de faire de ce produit assez bâclé un standard industriel.
- IBM a toujours considéré le PC comme un jouet, indigne de ses mainframes
- IBM confie l'écriture d'un OS à une firme peu connue alors, Microsoft, qui jusque là faisait un interpréteur BASIC pour l'Apple II entre autres. Il accorde une licence d'exploitation pleine et complète à Microsoft qui va en faire bon usage. L'une des plus monumentales erreurs stratégiques de l'histoire de l'informatique !
- Quelques années plus tard, IBM se verra menacé dans son existence par le succès des concurrents du PC, qu'IBM a contribué à créer...
- ISDN (ou RNIS) sera finalement installé juste à temps pour être remplacé par la Voix sur IP, sous la pression des constructeurs nord-américains qui préfèrent une solution tout-IP
- Fait remarquable, les Européens n'ont pas été en mesure de défendre leurs solutions, pourtant techniquement plus avancées que IP
- ARPAnet adopte la suite TCP/IP

## La mobilité



- En 1992, IBM joue avec l'idée d'un téléphone multifonctions; c'est l'IBM Angler (Simon)
- La norme GSM pour la téléphonie mobile numérique connaît un succès foudroyant
- Le finlandais Nokia devient très vite le leader mondial
- Apple, au bord de la faillite, est sauvé par... Microsoft
- Il y a 8 millions de machines connectées à Internet

- Se connecter à un réseau numérique avec son téléphone est dans l'air du temps des années 90, mais la technologie n'est pas encore mature.
- IBM, GRID et Samsung vont proposer des téléphones comprenant un modem; à noter que l'IBM Simon est déjà une machine à écran tactile, quinze ans avant l'iPhone (mais déjà vingt ans après que la technologie ait été inventée).
- La norme GSM change la donne en Europe dès 1992. Nokia se lance dans ce créneau; le PDG de Nokia sera traité d'optimiste délirant quand il annoncera viser la vente de dix millions d'appareils à l'horizon 2000; la réalité sera plus proche du milliard !
- Apple est au bord du gouffre; Bill Gates intervient pendant le MacWorld pour empêcher la faillite du groupe. Beaucoup d'aficionados de la firme Apple considéreront qu'ils ont été trahis par Steve Jobs; il en ira de même dans les années 2000, lorsque Apple adoptera des processeurs de la marque Intel, traditionnellement utilisés pour les PC.

## Les téléphones «intelligents»



- Nokia commercialise le premier véritable smartphone en 2006, le N95
- Apple commercialise l'iPhone en 2007
- Il y a 747 millions de machines connectées à Internet

- En 2006, Nokia est à l'apogée de son essor; le N95 représente le summum de la technologie du moment.
- Une année plus tard, Apple commercialise l'iPhone; un écran tactile et surtout des applications téléchargeables et un marketing d'enfer vont causer la perte du constructeur finlandais, dernier européen actif sur ce marché. Et pourtant, le N 95 fonctionnait une semaine avec une recharge, alors que l'iPhone peine à finir la journée... Chacun a ses propres critères de choix.
- La combinaison avec un appareil photo rend le smartphone pratiquement universel; j'étais il y a deux mois à Niagara Falls, et j'ai observé de manière plus ou moins aléatoire quelques groupes d'une dizaine de personnes. L'une regardait les chutes, une autre faisait une photo avec son smartphone, et les huit autres regardaient leur smartphone, sans doute pour admirer les photos qu'ils venaient de faire ?On pourrait en conclure que le smartphone est devenu plus important que l'univers réel; mais c'est une spéculation...
- Actuellement, le smartphone est devenu le couteau suisse du monde technologique; accessoirement, une mine d'or pour quelques constructeurs ayant parfaitement compris le sens de l'expression «obsolescence programmée».
- Le smartphone est de nos jours le principal outil informatique de la population mondiale. Il y a actuellement plus de trois milliards de smartphones dans le monde; aucun produit n'a jamais suscité un tel engouement; aucun produit n'a jamais atteint autant de ventes en si peu de temps: la poupée Barbie a semble-t-il fait mieux, mais

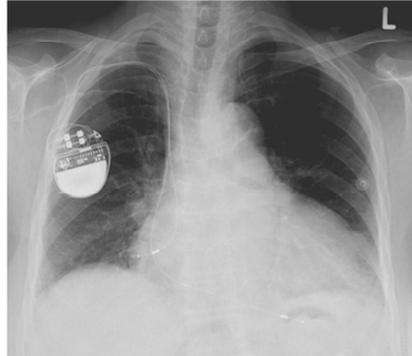
sur un laps de temps plus long. La brique Lego est aussi mieux placée, mais il ne s'agit pas de la même catégorie d'objet.



## Proche horizon : transports, énergie

- Les transports autonomes permettent de fluidifier le trafic et de rendre les déplacements plus sûrs (et plus écologiques, peut-être ?)
  - Des algorithmes permettent l'optimisation de la consommation d'énergie dans de nombreux cas
- 
- On parle beaucoup de l'automobile autonome; c'est oublier que le train existe en version autonome depuis pas mal de temps déjà (et les tondeuses à gazon depuis davantage de temps encore !) : après tout, on a célébré le dixième anniversaire du M2 en septembre de cette année, et il n'était pas le premier métro automatique. Les obstacles pour l'automobile et l'avion autonomes sont d'abord juridiques, mais aussi encore techniques : mêler des utilisateurs humains et informatisés dans un même flux de trafic pose des problèmes fort complexes. Ensuite, il y a divers problèmes éthiques qui ne sont de loin pas résolus.
  - L'informatique peut (devrait) aussi participer à améliorer le bilan écologique des transports; mais à l'heure actuelle, le bilan est plutôt mitigé : on a récemment beaucoup parlé de logiciel en rapport avec des automobiles à moteur diesel, mais il n'est pas certain que ce soit une bonne chose...

## Proche horizon : médecine



- L'informatique est déjà indispensable dans presque tous les domaines de la médecine : diagnostic, robots de soins, imagerie, prothèses, ...
- Cette tendance va s'accroître de manière exponentielle dans les prochaines années

- Cela fait déjà plus de vingt ans que des personnes ne survivent que grâce à un implant électronique, plus ou moins informatisé : l'implantation de prothèses informatisées déborde actuellement largement le domaine des prothèses cardiaques. Les implants neurologiques, les pompes à insuline, entre autres sont également devenus d'un usage courant; notre école est également partie prenante avec le développement de divers dispositifs médicaux implantables, dont par exemple une micro-vanne pour combattre l'incontinence urinaire. Cela pourrait se commander avec un smartphone, par exemple; mais il faut éviter de se tromper...
- La semaine passée, une publication originaire de l'EPFL et du CHUV dans Nature a redonné espoir à de nombreuses personnes paralysées qui pourraient peut-être recouvrer une certaine mobilité grâce à des implants dans la moelle épinière.
- Les robots chirurgicaux sont moins fréquemment évoqués, mais ils sont devenus indispensables pour nombre d'opérations. En général, ce ne sont que des télécommandes avec plus ou moins d'assistance informatique, mais on envisage déjà des opérations entièrement robotisées, où le chirurgien ne fait que superviser le travail (ou pas ?)
- Le diagnostic est, dans un proche avenir, probablement le domaine qui sera le plus bouleversé par l'informatique. Actuellement déjà, de nombreux utilisateurs pratiquent l'automédication en se basant sur des sites spécialisés. C'est certainement en l'état une pratique à déconseiller formellement, mais il y a fort à parier que dans quelques années, votre généraliste, après l'anamnèse, consultera un assistant

informatisé ayant accès à votre dossier médical qui lui fournira un diagnostic impossible à produire pour un être humain n'ayant pas accès à des millions de cas similaires. Il ne s'agit pas ici d'intelligence artificielle à proprement parler, simplement de brassage de montagnes de données...

- Il y a une chose que l'on voudrait demander à l'informatique dans le cadre médical : c'est de faire baisser les primes d'assurance-maladie. Un sujet de projet de master, peut-être ? Ou une incongruité politique ?



## Contribution écologique

- Les *spams* et le *cloud computing* contribuent à une consommation délirante d'énergie pour des objectifs parfois peu pertinents
- A quand une plate-forme de télétravail réellement confortable et utilisable ?
- L'obsolescence programmée et une récupération parfois inadéquate représentent une charge conséquente en métaux lourds pour l'environnement

- Dans divers secteurs, l'informatique permet d'améliorer le bilan énergétique : maisons informatisées truffées de capteurs, distribution d'énergie, mobilité douce, partage de ressources pour les déplacements, etc... Mais en général, on peut tout de même reprocher à l'informatique de ne pas en faire assez dans le domaine.
- Des *data center* monumentaux consomment une énergie fantastique pour stocker des exabytes de données plusieurs fois redondantes et des messages essentiellement constitués de spams. L'énergie est encore souvent fournie par des centrales à charbon !
- Au nom du Cloud Computing, chaque utilisateur se voit gratifié d'un volume de stockage prétendument gratuit dont il ne sait que faire, et dont il oubliera jusqu'à l'existence dans les mois qui suivront.
- A l'inverse, aucun effort n'est consenti pour des objectifs réellement écologiques. Des puces d'une puissance incroyable sont développées, de quoi faire pâlir Seymour Cray s'il était encore de ce monde. Mais elles sont placées dans des téléphones portables pour jouer majoritairement à Candy Crush, alors qu'il manque toujours cruellement une plate-forme logicielle permettant de réaliser simplement et efficacement un espace virtuel de télétravail (de nombreuses solutions existent, mais elle sont au mieux peu pratiques et souvent complexes, voire coûteuses à mettre en œuvre, pour ne rien dire du peu de sécurité qu'elles offrent)
- La récupération existe et est souvent effectuée de manière conséquente dans nos régions; mais ce n'est de loin pas le cas partout. L'obsolescence programmée incite à

jeter des appareils réputés vétustes avant qu'ils ne soient réellement devenus inutilisables.

- L'exploitation de minerais relativement rares induit des désastres écologiques dans plusieurs endroits de la planète (Ex.: Lithium en Amérique du Sud).

## Sécurité informatique

Username

Password

Keep me logged in

- Sécurité d'accès = Mot de passe
- Les informaticiens demandent aux utilisateurs de se plier à des règles parfois absurdes eu égard aux métiers concernés
- L'utilisateur est rendu responsable de la sécurité d'accès, alors que ce n'est en principe pas son rôle dans le métier qu'il exerce

- L'authentification est basée sur des mots de passe depuis les débuts de l'informatique. On a de ce fait délégué la responsabilité de la sécurité à l'utilisateur.
- Si le mot de passe est craqué, ce sera parce que l'utilisateur en a choisi un mauvais, ou n'a pas pris suffisamment de précautions.
- Dans certains hôpitaux, le personnel soignant doit s'authentifier avec sa carte personnelle sur chaque PC utilisé pour consulter un document de patient, ce qui représente un inconfort considérable; il cherchera donc à éviter cet inconfort en gardant des sessions ouvertes, ou en ne consultant pas le dossier pour des cas qu'il pense maîtriser. Dans certains cas, il conservera sur son smartphone des copies de données pour éviter l'ennui d'une authentification complexe et chronophage.
- Ce n'est en l'occurrence pas le rôle du médecin de se préoccuper de la sécurité d'accès au système informatique, ce serait le rôle de l'informaticien qui gère le système. Dans ce sens, les tentatives de Apple (FaceID) et d'autres sont intéressantes, mais leur réalisation tient actuellement plus de l'argument publicitaire que d'une véritable réflexion sécuritaire : la reconnaissance faciale est peu efficace lorsque l'on porte un masque à poussière, ou en salle d'opérations, voire en cas d'épidémie de grippe... Il en va de même pour les empreintes digitales difficiles à lire avec des gants de protection.

## Sécurité informatique



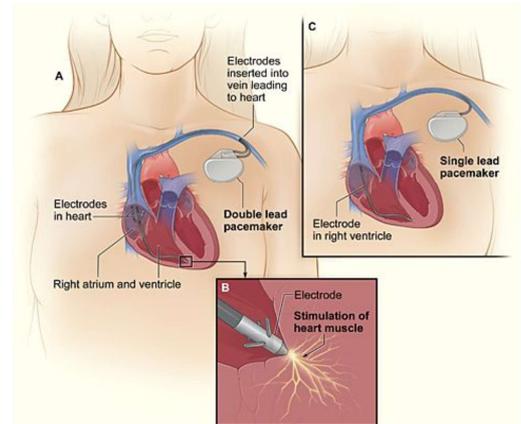
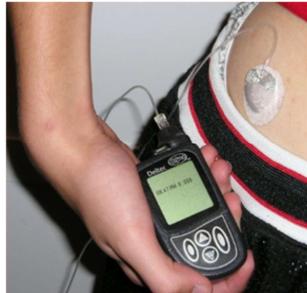
- Google, Apple, Facebook, Amazon, Microsoft (GAFAM) sont-elles les autorités adéquates pour définir ce qui est bon ou non dans la sécurité informatique ?
- Plus généralement, qui devrait définir ce qui est tolérable et ce qui ne l'est pas ?

- La sécurité des systèmes informatiques est contrôlée et régie par des entreprises (GAFAM). Ce sont elles en effet qui ont la main-mise sur les infrastructures utilisées
- Une entreprise, par définition, cherche avant tout à maximiser ses profits; or la sécurité coûte cher, et ne rapporte pas forcément grand-chose.
- Donc, il faut que les utilisateurs détectent un problème majeur pour que les entreprises se donnent la peine de réagir (voir Facebook, par exemple, qui a dû réagir pour ne pas subir un dégât d'image trop conséquent); mais quant à savoir ce qui est exactement entrepris et jusqu'à quel point la réaction est efficace n'est pas évident à déterminer, secret de fabrication oblige.
- Ironie, Windows et Facebook annoncent qu'ils vont s'attaquer à la sécurité informatique; ce sont les 2 principaux vecteurs de malwares, pourquoi ne pas l'avoir fait avant ? Par ailleurs, à qui demander de définir les règles nécessaires à la sécurisation d'un système informatique ?
- En l'espèce, la principale réponse réside dans les anti-virus et les détecteurs de malwares, ce que font McAfee ou Kaspersky depuis des décennies; mais est-ce suffisant ? Les programmes de sécurité sont notoirement impuissants contre les nouveaux virus que concoctent d'excellents programmeurs dans des pays pas si lointains... L'anti-virus est de toutes façons limité, car il ne peut agir qu'en tant qu'extension de l'OS. Et il faut l'installer, et garantir sa mise à jour...
- Ironie, des produits existent, certains ont été développés dans cette école et sont commercialisés dans la région, à Y-Parc par exemple; le domaine bancaire est un bon

client de ce genre d'infrastructure et de produit.

- Dans de nombreux cas, la protection de dispositifs est rendue difficile par l'obsolescence des produits: ainsi, un fabricant célèbre de dispositifs d'échographie utilise comme OS Windows XP, et ses appareils sont connectés à l'Intranet de grands hôpitaux comme le CHUV ou les HUG; or XP n'est plus supporté et est bourré de failles. Il est malaisé de mettre à jour ces appareils, car ils ne sont guère équipés des ressources matérielles nécessaires et de surcroît plus supportés par l'éditeur du logiciel; de plus, en tant que dispositifs médicaux, ils échappent souvent à la vigilance des services informatiques responsables de la sécurité

## Sécurité des objets connectés

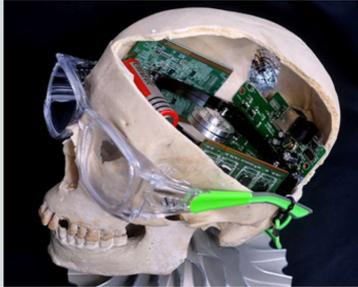


- Peu, voire aucune préoccupation sécuritaire!
- Composants critiques (*life critical*)
- Fonctionnalité médicale, consommation, fiabilité privilégiées

- Les problèmes de sécurité sont particulièrement préoccupants dans le cadre des objets connectés.
- Les ressources de ces objets sont généralement assez limitées, et la protection de ces objets n'est pas toujours au cœur des préoccupations du constructeur.
- De nombreux «objets connectés» jouent un rôle relativement crucial dans une maison ou une entreprise, voire en tant que composant auxiliaire dans un corps humain.
- Ainsi, on a pu démontrer la vulnérabilité assez inquiétante de pacemakers; et une vulnérabilité similaire pour les défibrillateurs implantés ou les pompes à insuline.
- Bien sûr, il est possible de faire des mises à jour : Le ministère américain de la santé a donné son aval au rappel de 465.000 pacemakers en 2018, quant on sait ce que représente le «rappel» d'un pacemaker, soit une intervention en ambulatoire de 1 heure et une hospitalisation de 5 à 6 heures, on peut estimer le coût de l'opération, avec un cardiologue, un ingénieur et 2 ou 3 infirmières engagées, sans compter le manque à gagner causé par l'intervention sur le patient et sa convalescence.
- Des experts en sécurité de WhiteScope assurent avoir découvert plus de 8000 failles dans les programmeurs de pacemakers dont certaines permettant d'agir sur ce dispositif médical d'importance vitale.
- Il se trouve que la préoccupation des fabricants est le bon fonctionnement des fonctions d'assistance à la vie des dispositifs, et non pas la sécurité informatique.
- Renversons le paradigme : proposons un OS de très haut niveau sécuritaire, avec

toutes les primitives nécessaires, et adapté (taille, vitesse, consommation) aux exigences des objets connectés, et laissons ensuite les spécialistes des objets connectés construire leur application par-dessus. Certains développements au cœur même de cette école pourraient en bénéficier !

- A noter que la sécurité des objets connectés médicaux fera l'objet d'une rencontre à Y-Parc très prochainement.



## Intelligence (?) artificielle

- L'intelligence artificielle dont seront dotés divers systèmes comprenant des objets «connectés» n'est pas à l'abri de problèmes sécuritaires
  - Une maison entièrement robotisée attaquée par un logiciel malveillant peut conduire à des situations préoccupantes
  - Certains objets «intelligents» sont susceptibles de prendre des décisions pouvant impacter la vie de personnes
- 
- Les objets connectés seront intégrés dans des processus dotés d'intelligence artificielle; ainsi, on a déjà des métros autonomes (le M2, par exemple), on aura bientôt des voitures autonomes, des navires, des trains et des avions. Tous les domaines de la vie publique pourraient à terme être impactés par l'intervention d'algorithmes et de machines dotées de capacités d'apprentissage. Une capacité d'apprentissage implique une fonction d'évaluation du résultat, afin de déterminer si il y a progrès. Mais qui définit ce qu'est un «progrès» ?
  - Pourquoi ces algorithmes seraient-ils moins vulnérables aux attaques que les PC, s'ils utilisent des OS identiques, ou basés sur des noyaux similaires ?
  - La maison robotisée (déjà d'actualité dans de nombreux cas) va ouvrir les portes, déclencher des alarmes, contrôler le chauffage, la climatisation, etc... de manière largement autonome... Mais que se passe-t-il si un malware s'introduit dans le système ?
  - Plus préoccupant, l'AI va probablement bientôt introduire des fonctionnalités impliquant des décisions pas toujours innocentes. Les armes intelligentes actuelles le font déjà, mais une arme n'a pas d'état d'âme. L'AI n'a actuellement aucun code éthique de quelque sorte que ce soit. Elle n'a même pas les trois lois de Asimov, notoirement insuffisantes si l'on lit les romans de cet auteur... Pourra-t-on faire l'impasse sur une telle réflexion au moment de lancer sur le marché des outils qui peuvent potentiellement prendre des décisions, bonnes ou mauvaises, impactant la

vie ? **Plus philosophiquement, peut-on parler d'intelligence en l'absence de conscience ?**

- Malgré ces doutes, je suis impatient de m'asseoir dans une voiture et lui dire «Proposes-moi un bon film pendant que tu m'emmènes au sud de la France». Mais ne suis-je pas optimiste ?

## Des logiciels vétustes



- Les systèmes d'exploitation descendent presque tous de systèmes développés dans les années 70 : UNIX, ou VMS majoritairement. Même Linux a ses origines dans UNIX
- Les logiciels les plus utilisés sont des dinosaures, énormes et difficilement gérables car encombrés de fonctionnalités peu utilisées.
- Les éditeurs et distributeurs de logiciel sont essentiellement des entreprises nord-américaines
- IP et TCP eux-mêmes sont des protocoles peu évolutifs, malgré l'évolution vers IPv6 (évolution pour le moins laborieuse d'ailleurs !)

- Les programmes que nous utilisons sont un peu comme moi : ils essaient de se pomponner pour avoir l'air jeune, mais cela devient de moins en moins crédible. En réalité, il s'agit de dinosaures qui ne subsistent que par la grâce des progrès de la microélectronique. Même les protocoles de communication sont vieilllots: après tout, la suite TCP-IP a été adoptée en 1983, même si IP a reçu un lifting qui a eu beaucoup de peine à s'imposer.
- Le logiciel est essentiellement géré par quelques entreprises nord-américaines; les systèmes d'exploitation, entre autres, sont de lointains descendants d'OS pensés dans les années 1970, soit il y a quarante-cinquante ans. La mobilité et Internet étaient de la science-fiction, à cette époque. Mais nous utilisons ces produits... A l'époque, on parlait de fichiers; malgré toutes les couches cosmétiques ajoutées par les Windows et autres MacOS, il n'y a pas grand-chose qui ait évolué en près de cinquante ans...
- Les entreprises concernées n'ont guère intérêt à développer un nouvel OS, car cela coûte cher et rapporte fort peu.
- Ces OS sont vulnérables (Linux, MacOS, Windows); et surtout, sont majoritairement gérés et distribués par des entreprises américaines; ceci pose divers problèmes, notamment de mainmise économique sur les technologies de l'information, et aussi de sécurité politique.
- Les Etats-Unis sont une démocratie, et il est peu probable que cette démocratie vienne un jour à élire un gouvernement présidé par un psychopathe ou une lunatique (?); mais comme l'a dit un célèbre personnage romand «Seul l'avenir peut nous dire

de quoi le futur sera fait». Alors, si cela devient le cas, ne risque-t-on pas de voir ce président faire pression sur les firmes concernées pour rendre les systèmes inopérants, ou malicieux chez les «ennemis» ou ceux considérés comme tels ? Une simple mise à jour suffirait, après tout !

- Si ces entreprises cèdent aux pressions, ne risque-t-on pas de voir dès la prochaine mise à jour tous nos smartphones et nos PC ou serveurs Linux s'arrêter tout simplement, ou pire, essayer de nous manipuler insidieusement ?
- Par ailleurs, pour vraiment s'attaquer valablement aux problèmes de sécurité, il semble raisonnable de recréer un nouvel OS avec les exigences de sécurité placées au cœur du développement
- Un grand challenge pourrait être un OS pour les systèmes embarqués connectés : performant, de faible taille, peu gourmand en ressources, peu gourmand en énergie, et possédant les caractéristiques permettant de le sécuriser aisément. De plus, aisément susceptible d'être utilisé comme noyau de systèmes plus ambitieux (scalability). Et proposant une authentique virtualisation des ressources.
- Utilisable dans les dispositifs médicaux, les life-critical devices, dans une montre, dans des téléphones.... Mais aussi pourquoi pas dans des PC, où il pourrait exécuter les programmes Windows ou Mac OS dans des boîtes à sable...
- Un bel objectif pour les universités européennes... et les HES !



## L'information, clef de la démocratie (Alfred Sauvy, 1951)

- Une population bien informée est le garant d'une démocratie de qualité
- Encore faut-il que la qualité de l'information soit au rendez-vous
- L'information est librement disponible; mais quelle information ?
- Les biens de consommation deviennent «traçables»; mais l'information ?

- Alfred Sauvy (dont je ne partage pas les convictions, ce qui n'empêche pas qu'il ait pu émettre des opinions pertinentes) avait, en 1951, bien compris le lien très fort entre la diffusion de l'information et une démocratie bien comprise; le credo des pionniers de l'informatique et d'Internet était en conséquence qu'une information libre et universellement disponible garantissait une démocratie équitable et éclairée, chacun pouvant se faire une opinion sur la base de faits avérés.
- Le grand rêve des pionniers d'Internet (une information gratuite va œuvrer pour la démocratie) s'est avéré une illusion, ou tout au moins entaché d'un vaste côté obscur. Ils avaient en partie seulement raison; encore faut-il que l'information soit de qualité et non biaisée. Actuellement, chacun a accès à une quantité quasi infinie d'informations, mais ces informations sont au mieux approximatives ou contradictoires, au pire falsifiées ou manipulées.
- La traçabilité des biens de consommation ne résout pas tout, mais est globalement très bénéfique. Ne devrait-on pas garantir la même chose pour l'information ? Après tout, nous consommons de l'information au même titre que des fruits et légumes, même si ce n'est pas les mêmes orifices qui sont concernés...



- Je conclurai ici mon propos; avec la conscience que nos générations ont développé un environnement remarquable à de nombreux égards, mais aussi très imparfait à d'autres. Les problèmes climatiques sont bien évidemment en tête de liste des préoccupations actuelles, et vont sans doute le rester encore longtemps, mais les problèmes, souvent liés, de civilisations et de sociétés vont également être très présents. Les technologies de l'information, comme vecteur incontournable, vont jouer un rôle prépondérant dans les interactions entre toutes ces problématiques, et les jeunes ingénieurs auront la responsabilité de développer des outils adéquats pour maîtriser les défis posés par le traitement et la diffusion des informations. Bon courage à eux !.
- Lorsque j'ai pris la décision, à 45 ans, après 15 ans très enrichissants et plein de satisfactions dans le monde industriel, de venir dans l'enseignement, j'avais beaucoup d'appréhension. A juste titre d'ailleurs... Mais les difficultés sont faites pour être surmontées, et grâce à de très nombreuses personnes, je n'ai pas regretté cette transition. Je voudrais donc remercier encore une fois ici tous ceux qui ont accompagné ces vingt ans de carrière dans l'enseignement, à savoir mes proches bien sûr, mes collègues et collaborateurs, le personnel administratif et technique de l'école et du canton, le staff de direction, tous les divers partenaires du monde industriel, administratif ou académique avec qui nous avons envisagé et réalisé des projets

passionnants et bien évidemment les principaux acteurs d'une école que sont les étudiants. A tous, mille mercis, et meilleurs vœux pour la suite, que vous comptiez parmi les actifs ou les retraités !

- Je suppose que comme moi, vous avez soif. Mais il me semble que l'apéro n'est pas trop éloigné...