Serge Bordères

Centre d'Etudes Nucléaires
de Bordeaux-Gradignan

Observatoire des Technologies Nomades et de
l'Internet pour la Recherche

OBTENIR

RESINFO

cnrs

DevLog

Qu'est-ce qu'un mobile ?

Dans cet exposé, on entend par mobile les smartphones et tablettes

Avertissement

Cet exposé n'a pas pour vocation de se substituer à votre support informatique

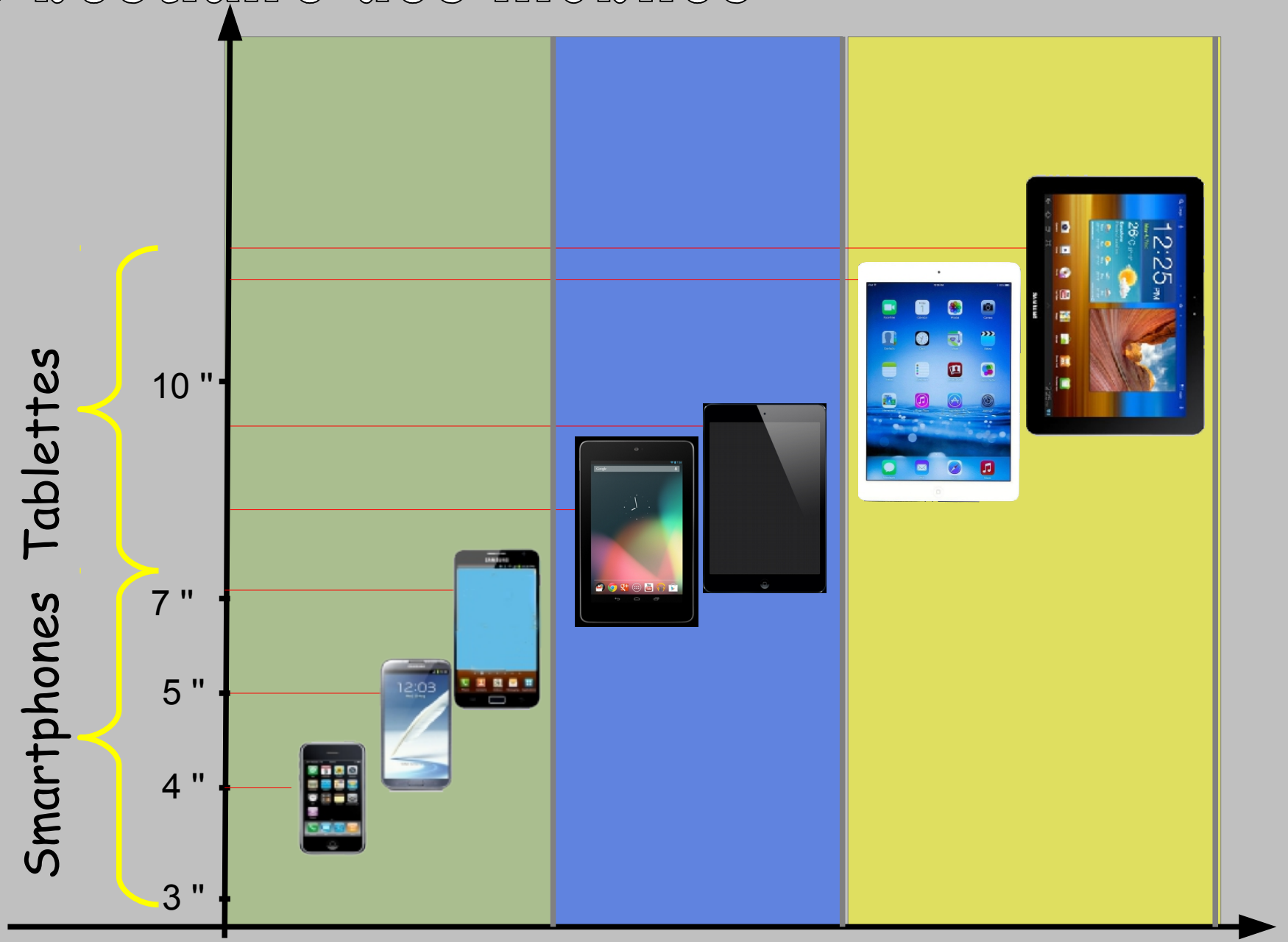
Les mobiles ne sont plus des gadgets

- Dans les années 80 on n'imaginait pas ce qu'on ferait faire à des ordinateurs 30 ans après !
- Nous n'imaginons pas ce que nous ferons dans 10 ans avec nos smartphones, nos tablettes...et nos objets connectés.

- Il est indubitable qu'ils seront partout dans nos vies privées...et dans nos activités professionnelles
- Ce qui posera un certain nombre de défis...

Tour d'horizon du monde des mobiles

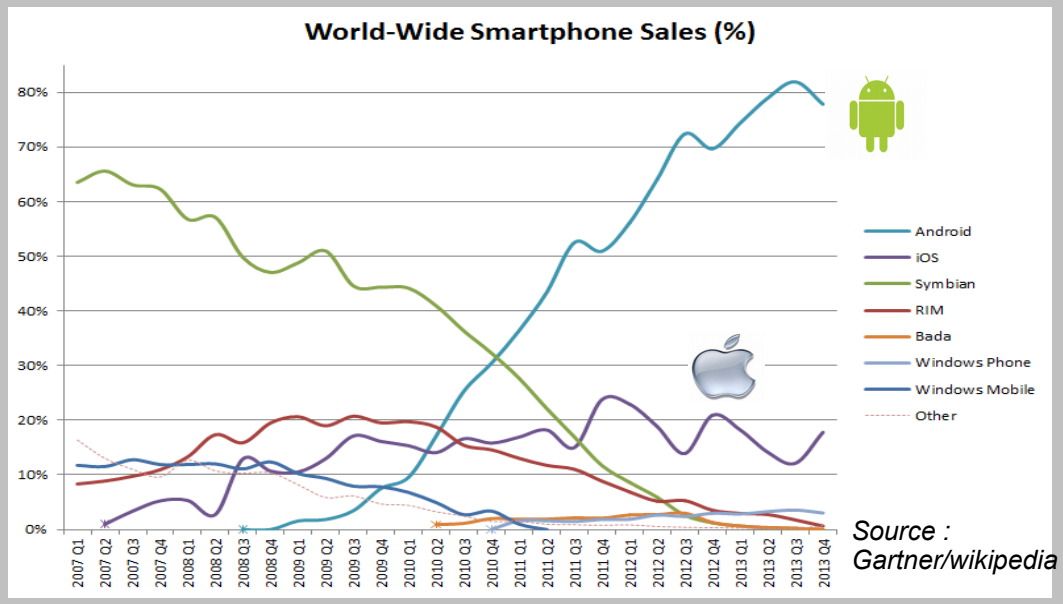
Le bestiaire des mobiles



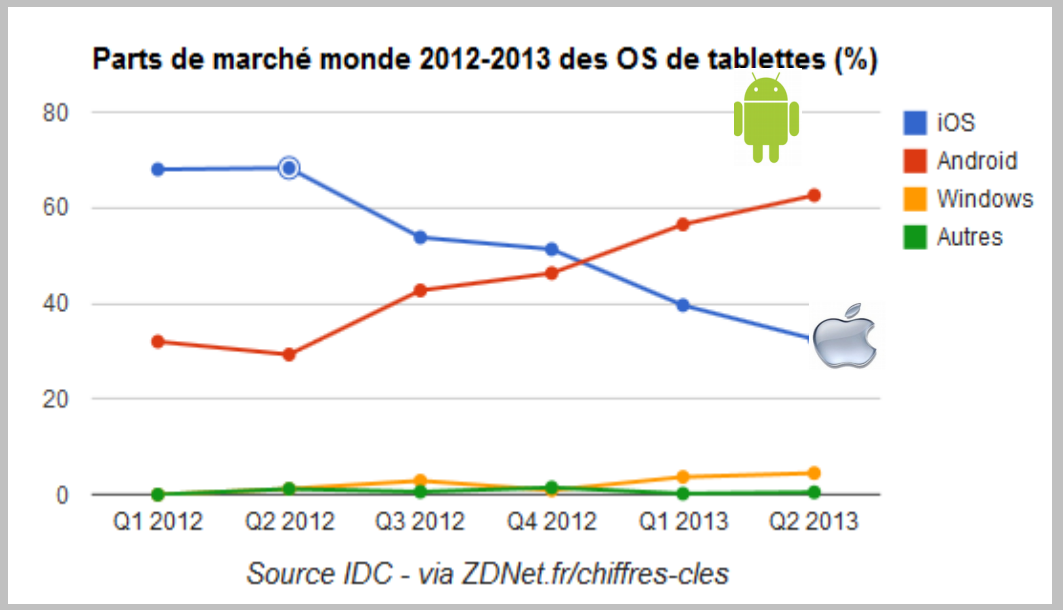
De nombreux acteurs

Editeurs	IOS	Google ANDROID	BlackBerry	Windows 8, TIZEN, Firefox OS
Fabricants		SAMSUNG, SONY, htc, LG, MOTOROLA, ZTE中兴, etc ■ ■ ■ ■	BlackBerry	Divers et variés
Opérateurs	orange™, free, SFR, Bouygues Telecom			
Store	Apple Store	Google play, amazon, android	BlackBerry App World	Windows Store

Part de marché des systèmes d'exploitation



Source : Gartner/wikipedia



Caractéristiques techniques

De quelques constructeurs

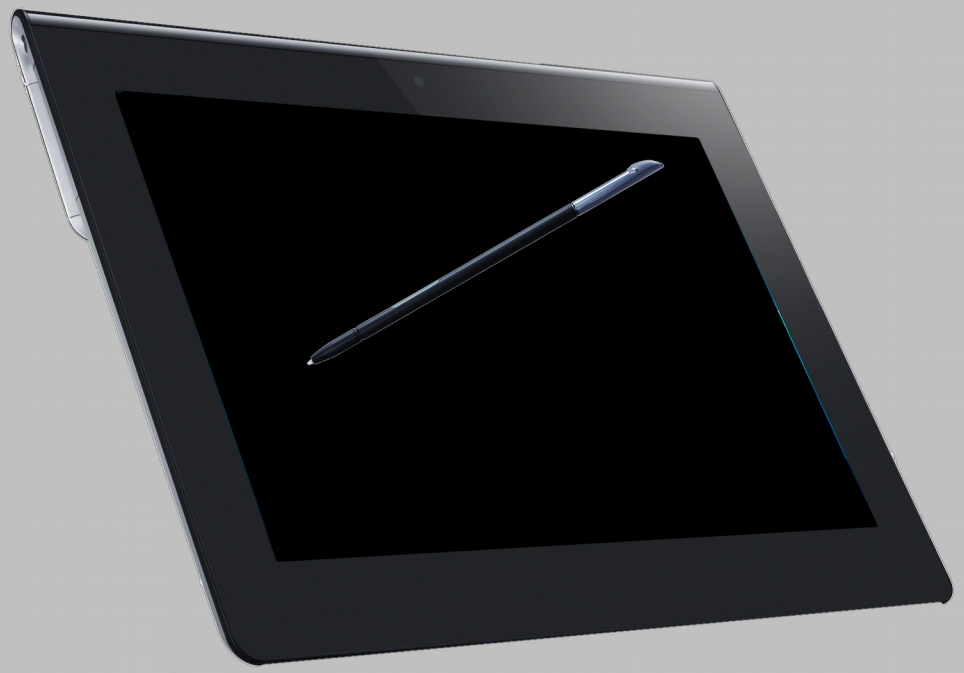
	TABLETTES			SMARTPHONES		
	Apple iPAD air	**Samsung GALAXY NOTE 10.1 2014**	**Google (Asus) Nexus 7**	**Apple iPhone 6 plus**	**Samsung Galaxy S5**	**Google (LG) Nexus 5**
Processeur	2 cœurs 1,4 Ghz	4 cœurs 2,3 Ghz (8=>1,9)	4 cœurs 1,51 Ghz	2 cœurs 1,4 Ghz	4 cœurs 2,5 Ghz (8)	4 cœurs 2,26 Ghz
Mémoire	1Go	3 Go	2 Go	1Go	2 Go	2Go
Stockage	16 à 128 Go Non extensible	16 à 64 Go Extensible 64Go	16 à 32 Go Non extensible	16 à 64 Go Non extensible	16 ou 32 Go + jusqu'à 128Go	16 ou 32 Go Non extensible
Ecran	9,7 pouces 2048x1536 264ppi	10.1 pouces 2560x1600 298ppi	7 pouces 1920x1200 323ppi	5.5 pouces 1920x1080 326ppi	5,1 pouces 1 920×1 080 432ppi	4,95 pouces 1920x1080 445ppi
Poids	469g	536g	340g	172g	145g	130g
DAS				0,907 W/kg	0,562 W/kg	0,407 W/kg

Des ordinateurs comme les autres

- Un système d'exploitation (Androïd, IOS...)
- Des fonctions réseau (Wifi)
- Des applications
- Des failles de sécurité
- Nécessité de faire des mises à jour
- Des utilisateurs

Des ordinateurs PAS comme les autres

- Ecran tactile
- Gyroscope/Accéléromètre
- Capteur de lumière
- Caméra/photos/micro
- Vibreur
- GPS
- Bio-capteurs
- Téléphone
- 3G/4G
- NFC



Des ordinateurs PAS comme les autres

- De très nombreuses applications
- Regroupées dans des « magasins » (stores)
- Pas chères ou gratuites
- Très faciles à installer
- Des technologies qui évoluent très rapidement
- Taux de renouvellement très élevé

Des ordinateurs PAS comme les autres

- Pénétration rapide dans la société
- Frottements avec l'environnement professionnel
- Introduction de matériels personnels dans le milieu professionnel ...sans contrôles ou limites
- Des problèmes de sécurité fortement exacerbés

Le mélange des sphères privées - professionnelles

Le mélange des sphères privées - professionnelles

- Pour la première dans l'histoire de l'informatique des technologies ont pénétré la sphère privée avant la sphère professionnelle

- Les mobiles ont pénétré plus ou moins sauvagement les entreprises et nos établissements.

- Certains se sont adaptées et pratiquent le B.Y.O.D = Bring Your Own Device

Le mélange des sphères privées - professionnelles

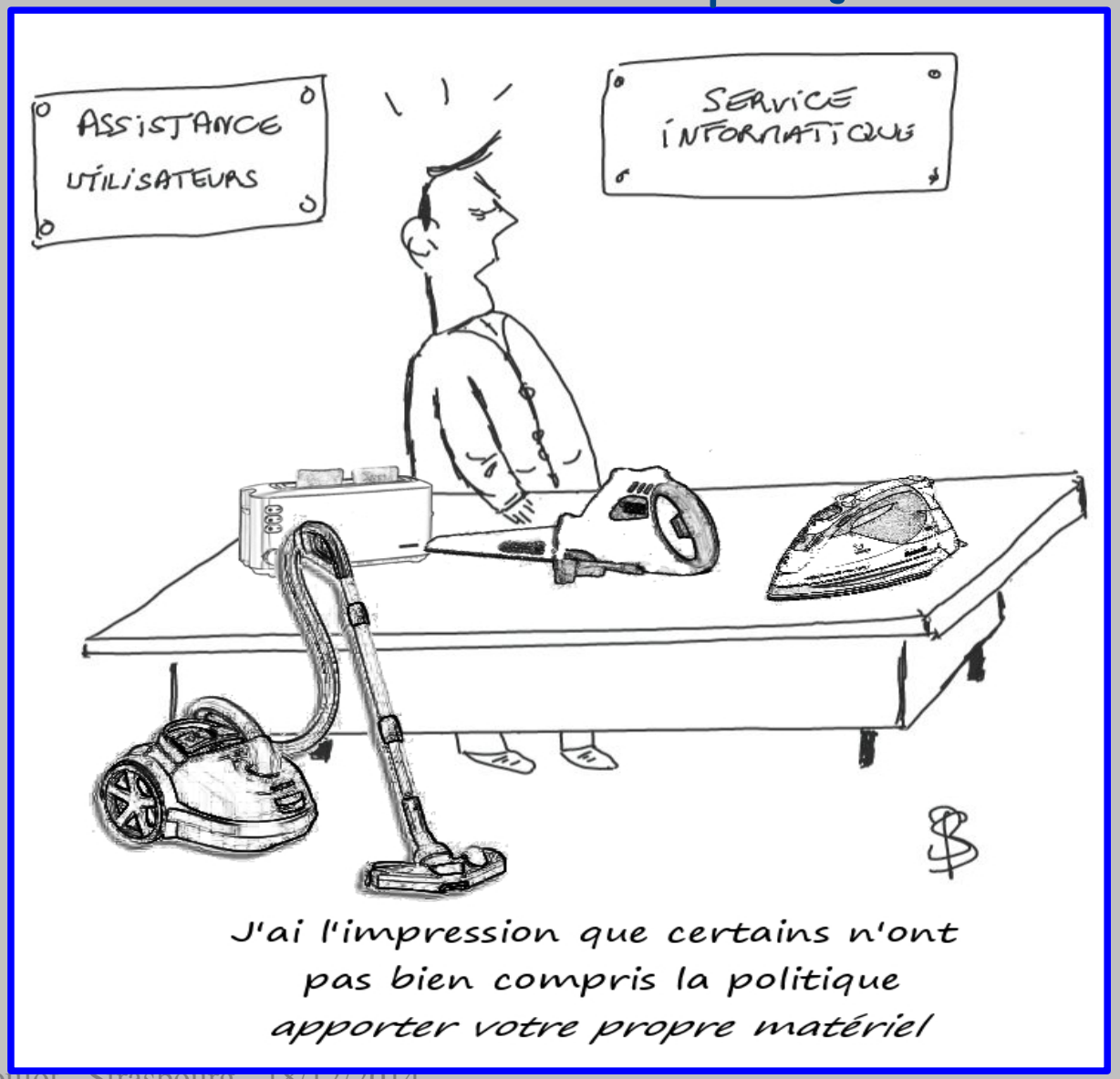
- Le BYOD est une politique élaborée par un établissement pour encadrer l'usage des mobiles dans le Système d'Information et en définir les limites

- Ce n'est pas « chacun fait ce qu'il veut. »

- Dans tous les cas, ne JAMAIS introduire de mobiles dans le S.I sans l'avis/autorisation/procédure du support informatique

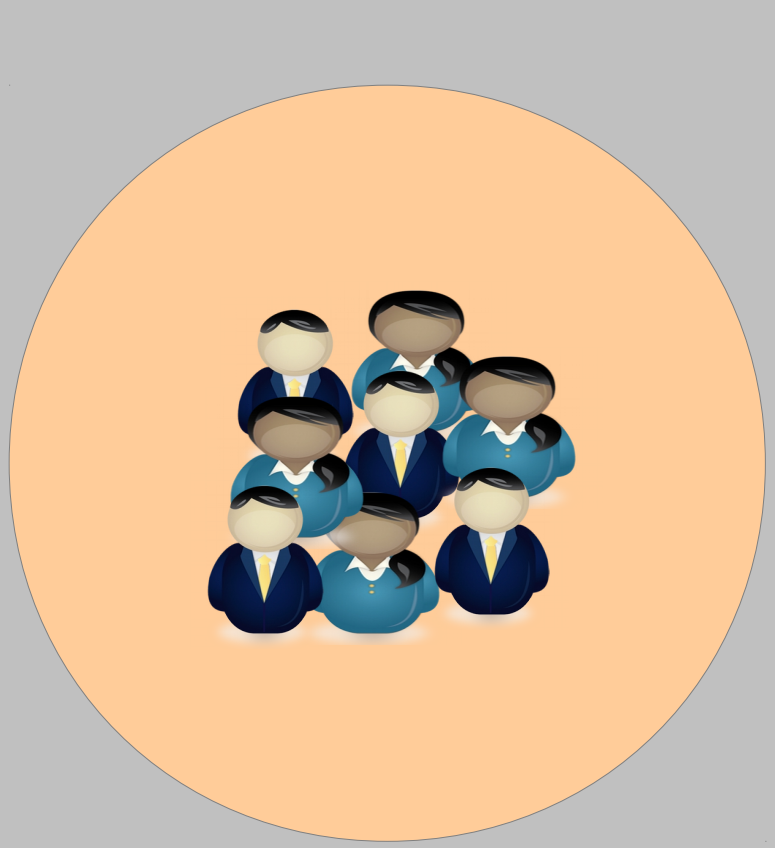
Le mélange des sphères privées - professionnelles

BYOD ce n'est pas ça...

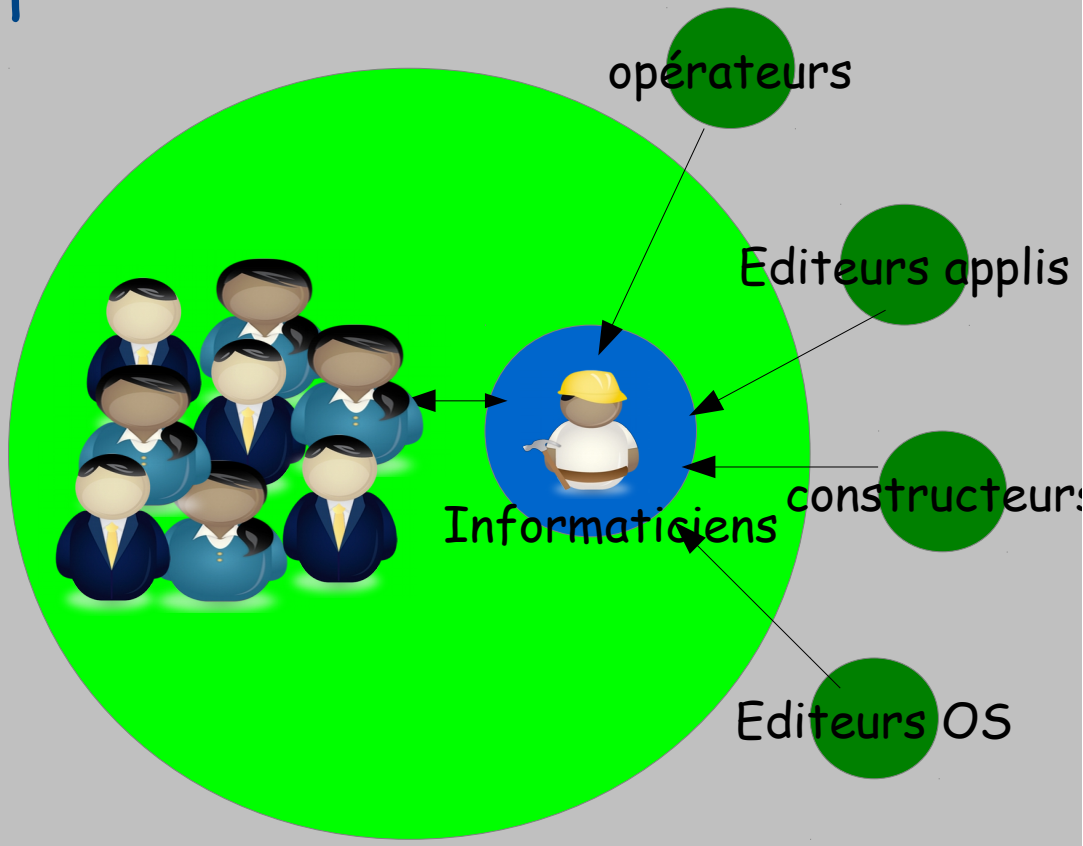


Où cela nous mène ?

AVANT

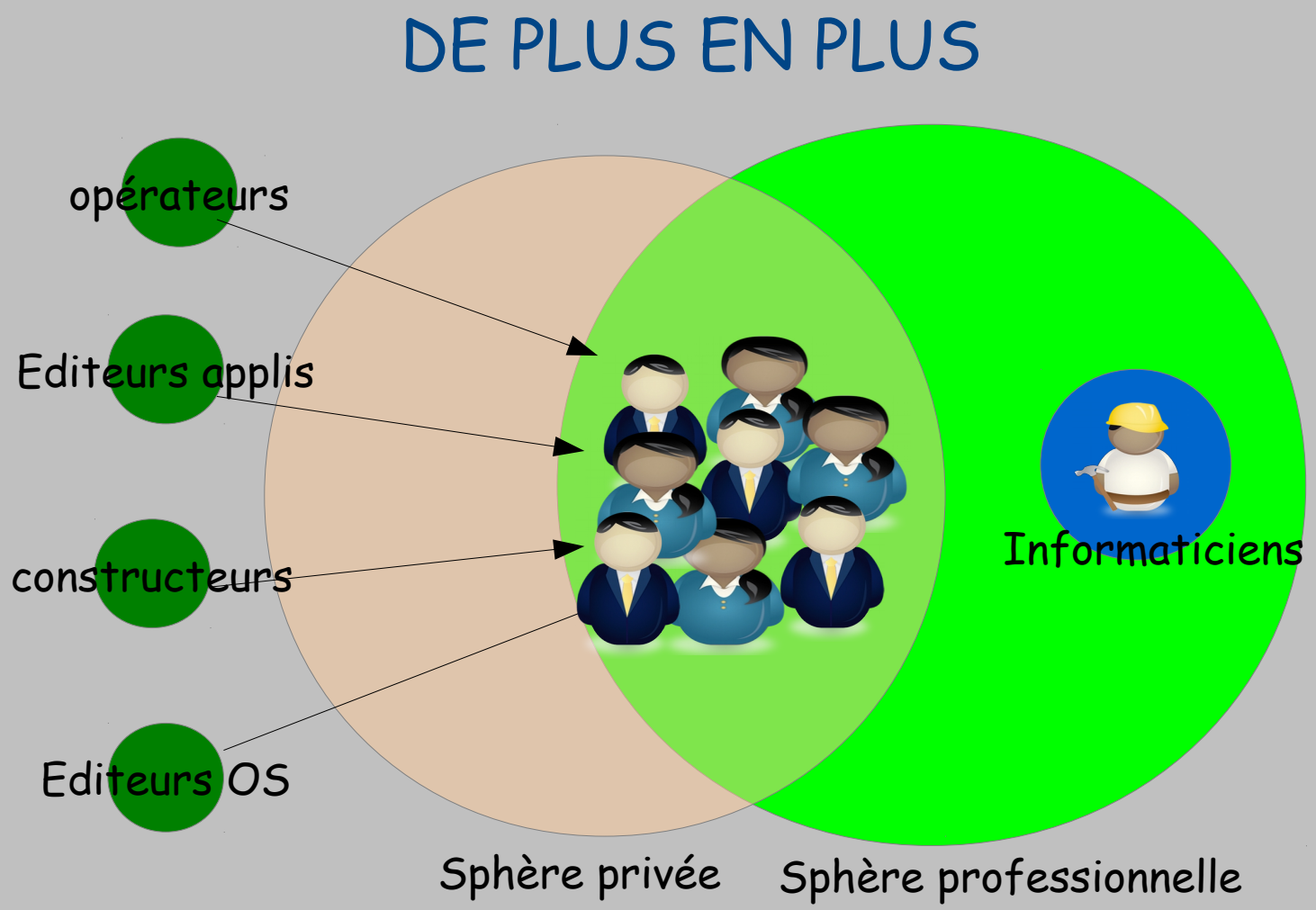


Sphère privée

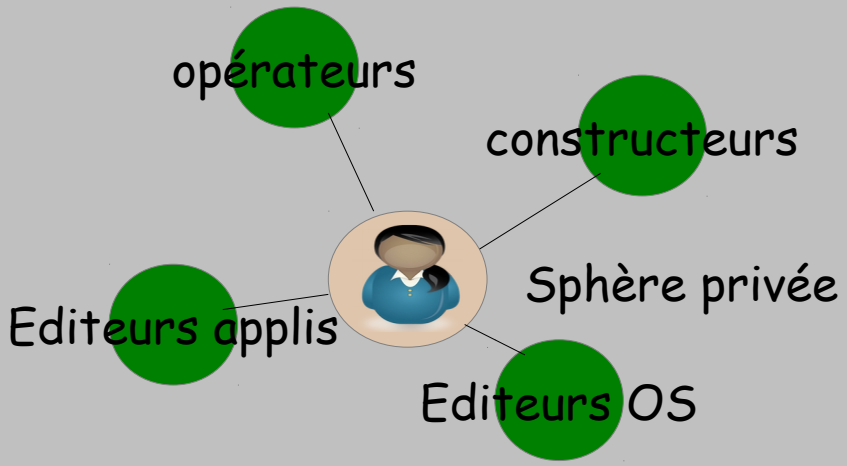


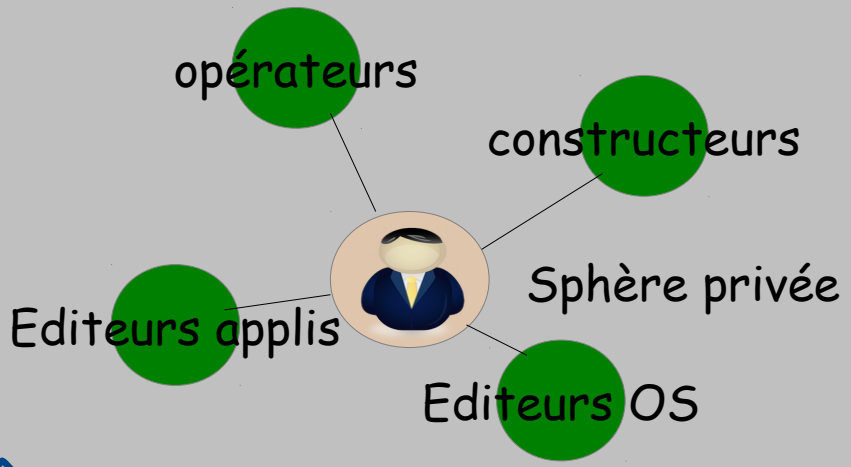
Sphère professionnelle

Où cela nous mène ?

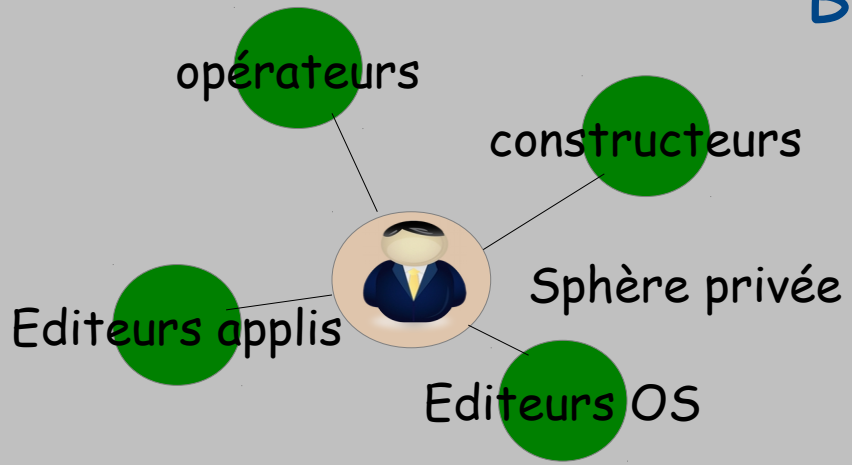


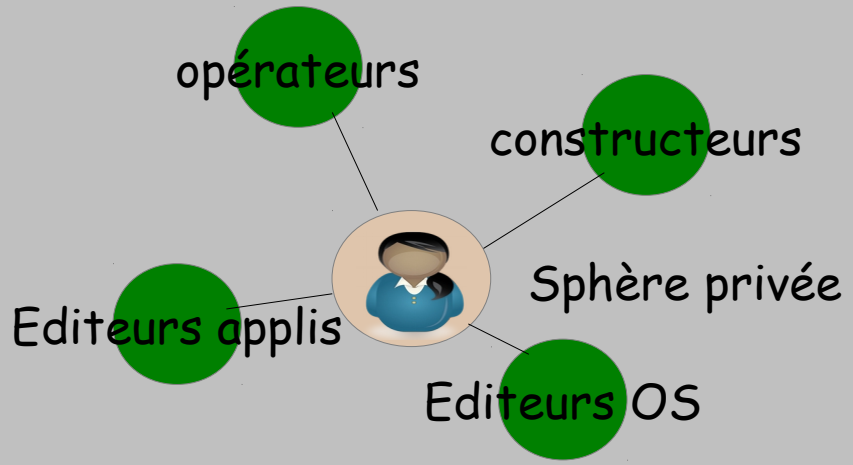
Où cela nous mène ?





BIENTÔT ?



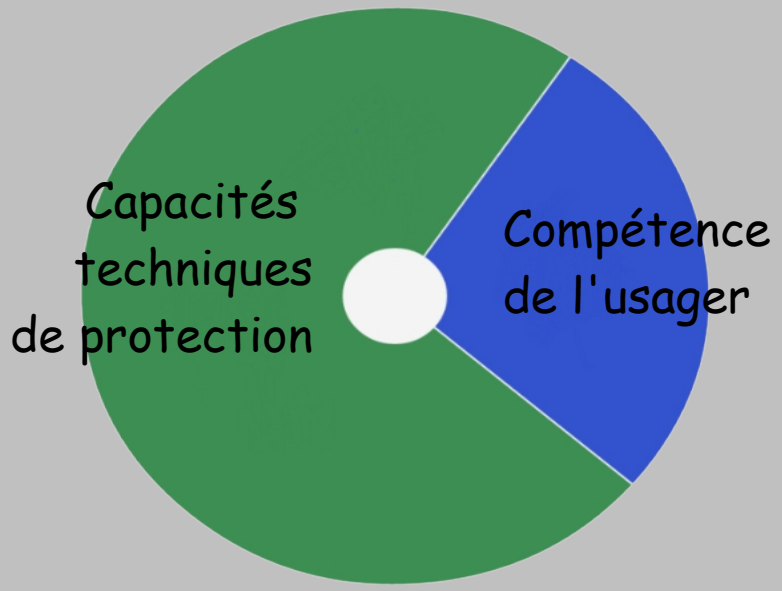


Qui influence la politique de sécurité ?

L'usage de matériels personnels change les critères qui influencent le niveau de sécurité du système d'information

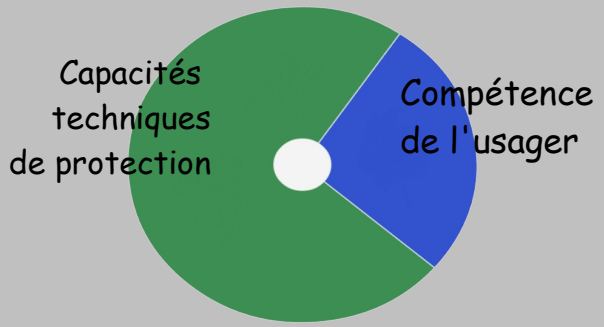
Qui influence la politique de sécurité ?

- Terminaux gérés
  (nomades ou pas)

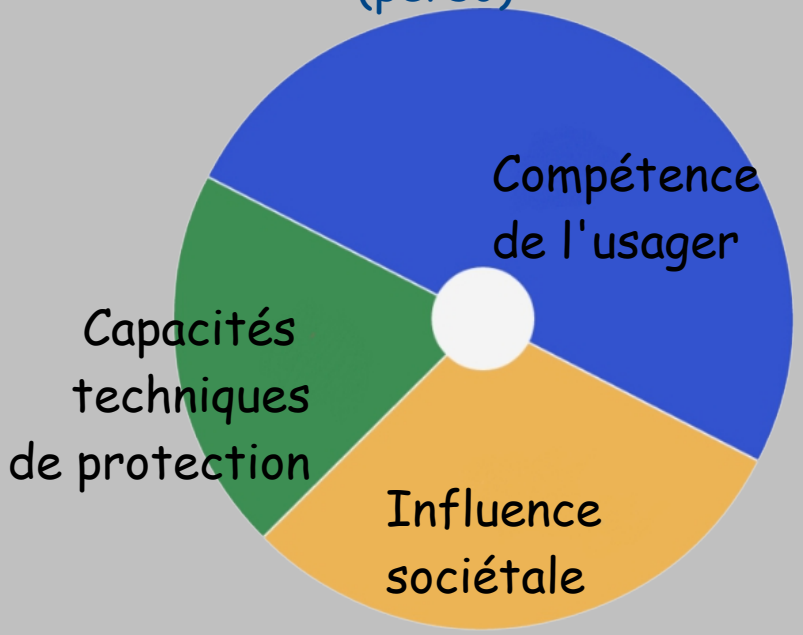


Qui influence la politique de sécurité ?

- Terminaux gérés

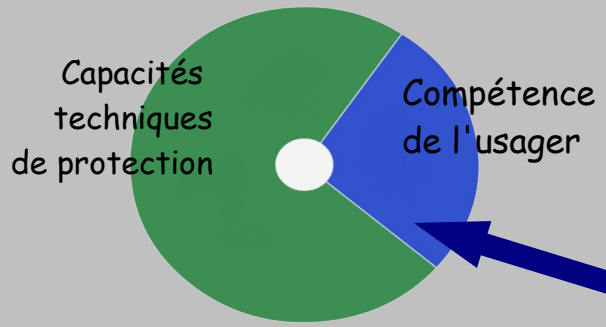


- Mobiles pas gérés (perso)

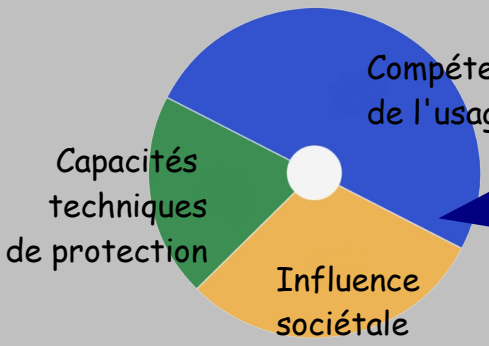


Qui influence la politique de sécurité ?

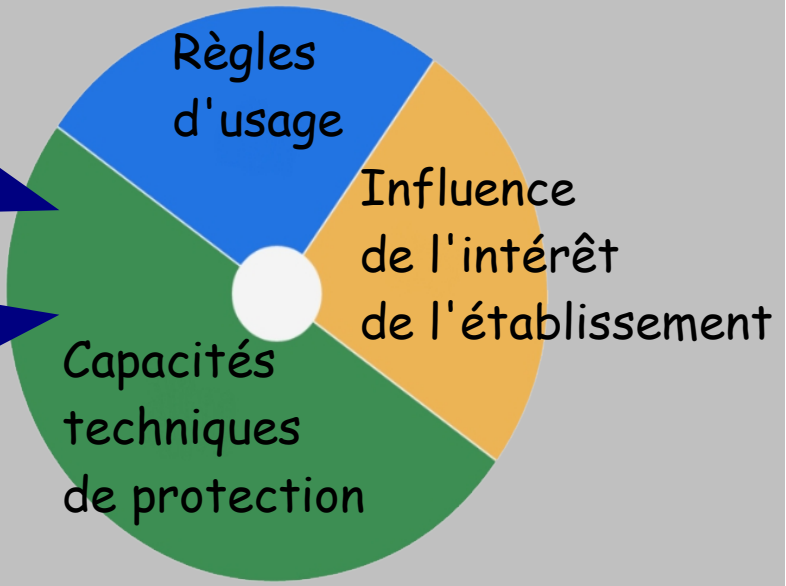
- Terminaux gérés



- Mobiles pas gérés



- Système d'information
  (serveurs, services, données, postes de travail...)



Quels problèmes posent les mobiles ?

- Toutes les applications enregistrent les mots de passe de façon hétérogène avec de faibles protections voire aucune…

- Un mobile non protégé ou mal protégé donne très facilement accès à toutes sortes d'informations privées ou professionnelles=> risques personnels + risques pour l'établissement.

- Un mobile est très « volatile » et peut facilement être perdu ou volé

Qu'y a-t-il dans un mobile ?

Qu'y a-t-il dans un mobile ?

Beaucoup pensent (et disent) : Je ne détiens pas d'informations importantes ou elles n'intéressent personne.

- C'est peut-être vrai
- C'est peut-être faux
- C'est peut-être vrai aujourd'hui , faux à moyen terme
- De toute façon les identifiants (mot de passe) sont sensibles car ils peuvent servir à :
  - Vous attaquer
  - Infiltrer le système d'information de votre établissement
  - Accéder à beaucoup plus d'informations
  - Attaquer des tierces personnes
  - Etc , etc

Que devient un mobile ?

Zone de fuite d'informations

Physiquement détruit

Réinitialisé (config usine) Puis cédé à un tiers

Cédé à un tiers sans ré-initialisation

Retour à L'opérateur sans ré-initialisation

Décheterie Sans ré-initialisation

Perdu/volé

D'un point de vue plus pratique

La tentation du jailbreak/root

Qu'est-ce-que c'est ?

- Cela consiste à débrider un mobile pour accéder à des fonctions interdites.
- Cela fait sauter les principaux verrous de sécurité
- Un mobile jailbreaké/rooté n'a plus de sécurité

- Si rooter ou jailbreaker n'est pas illégal, l'usage qu'on peut en faire peut l'être.

- Par exemple : Installer des applications payantes, proposées gratuitement sur des sites pirates.
  C'est une violation de la licence et du droit d'auteur.

Verrouillage d'écran

Protection minimale : passcode de déverrouillage

Il n'est pas raisonnable de laisser un smartphone
ou une tablette sans verrouillage d'écran

- Ne pas confondre avec le pincode de la carte SIM qui ne protège pas du tout un smartphone

- Sans passcode de déverrouillage un mobile n'est absolument pas protégé

Un mobile en relation avec le réseau et les applications professionnels doit toujours avoir un passcode
Même si ce n'est pas une protection absolue,
c'est une protection minimale

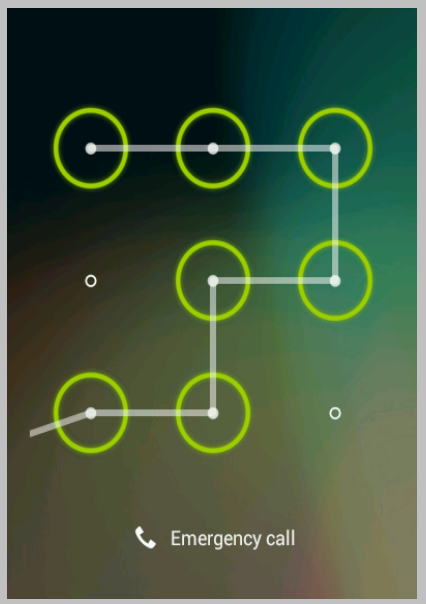
Déverrouillage par modèle

- **Consiste à dessiner un motif entre des points contigus**

  - Uniquement sous Androïd
  - La robustesse est proportionnelle à la complexité du motif
  - Déverrouillage très rapide du mobile.

  - Réputé peu robuste car le nombre de combinaisons est faible :

    4 points => 1624 solutions
    5 points => 7152 combinaisons
    6 points => 26016 combinaisons ==> plus de combinaisons qu'un pincode à 4 chiffres
    9 points => 140704 combinaisons



Déverrouillage par pincode

- Verrouillage par une suite de 4 à 16 chiffres 
  - Robustesse proportionnelle au nombre de chiffres.
  - En général 4 chiffres utilisés => 10000 combinaisons seulement

Déverrouillage par mot de passe

- Utilisation d'un « vrai » mot de passe alpha-numérique

  - Méthode la plus robuste
  - Mais la moins pratique
  - Difficile de taper un mot de passe contenant chiffres, lettres, caractères spéciaux sur un smartphone :
    - basculement entre les claviers virtuels (numérique, alpha)
    - gros doigts – petites touches
    - Soleil…

Déverrouillage par empreintes digitales

- Méthode introduite récemment (automne 2013)
- Disponible sur les matériels haut de gamme Apple et Samsung
- Pas invulnérable
- Doit faire ses preuves

Limites du passcode

- Vis à vis d'une activité professionnelle, le passcode est un minimum et on doit être sûr que l'utilisateur a bien positionné un moyen de verrouillage, ou qu'il ne l'a pas supprimé.
- Ne pas utiliser des passcodes triviaux : Ils sont bien connus : 0000, 1234, 2580, 2468 ……
- Paramétrer le verrouillage automatique de façon raisonnable (10 mn par exemple, pas 1 heure)
- Attention au Shoulder Surfing
- La nature même des matériels fait que l'écran est souvent déverrouillé et à des grandes chances d'être volé dans cet état.

Limites du passcode

- Des publications font état des résultats suivants pour cracker le passcode de verrouillage d'écran d'un système Apple (iphone, ipad)

4 chiffres.....18 mn
4 caractères alphanumériques.....19 jours
6 caractères alphanumériques.....196 jours
8 caractères alphanumérique.....755 000 ans
8 caractères complexes.....27 millions d'années

Conseils

A l'achat

- Choisir son système d'exploitation, ne pas laisser le vendeur choisir à votre place.
- Acheter un mobile avec une version récente du système d'exploitation.
- Un smartphone bas de gamme peut ne pas contenir toutes les fonctionnalités, pas de mises à jour.
- Les anciens mobiles ne supportent pas les versions récentes (attention au discours du vendeur)
- Ne pas écouter les Geeks : ils sont de mauvais conseils.
- Dans le cas d'une « possible » utilisation professionnelle, consulter d'abord le support informatique.

Réseau

- Coupez le Wifi et 3G/4G quand vous n'en avez pas besoin.
  - Même en veille le réseau reste actif
  - Économie d'énergie

- Coupez le bluetooth s'il n'est pas utilisé

- Attention aux propositions de stockage dans le Cloud (Google, Apple, Dropbox ou autres)

- Attention sur quoi vous vous connectez : Eduroam chez McDo c'est louche

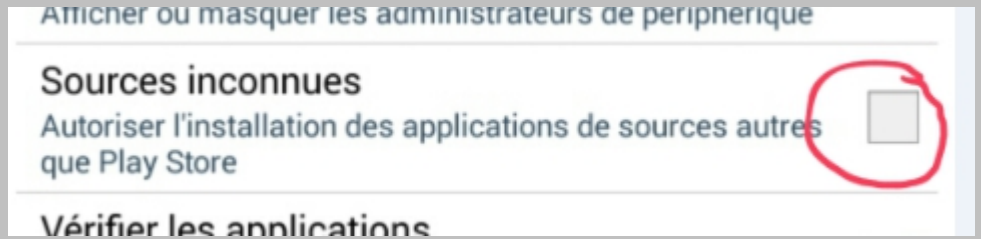
- Configuration de messagerie => toujours chiffré (imapS, smtpS)

Installation d'applications

Monde Androïd

- Les applications sont téléchargeables depuis Google play mais pas uniquement.
- Il existe d'autres stores (constructeurs, Amazon...)
- Les paquetages peuvent être aussi téléchargés depuis des sites non-officiels => C'est la plus grande source de virus
- Le téléchargement depuis des sites non officiels doit être maîtrisé (il faut avoir confiance)

Paramètres/sécurité



Installation d'applications

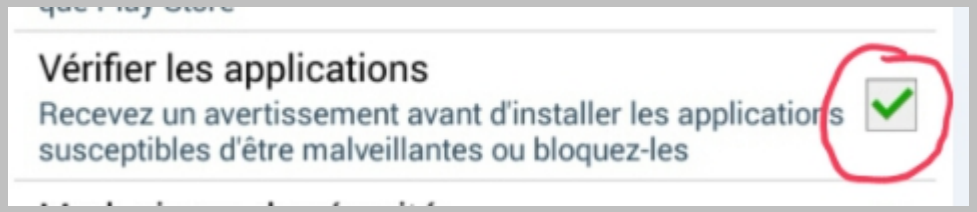
Monde Androïd

- Google effectue des vérifications de sécurité sur les applications disponibles (pas forcément toujours efficaces).

- Le service « Vérifier les applications » peut être activé pour effectuer une vérification d'une application lors de son installation (quelle que soit la source) et envoyer un message d'alerte si un malware est détecté (version >= 4.2.2)

- Ces vérifications ne sont pas forcément imperméables.

Paramètres/sécurité



Installation d'applications

Monde Androïd

- Lors de l'installation, la liste des permissions demandées par l'application s'affiche et l'utilisateur doit accepter ou refuser

- Il est difficile de comprendre la portée de ces permissions mais c'est ce qui détermine le « pouvoir » qu'aura une application dans le système (accès aux fonctions téléphoniques, SMS, caméra....)

- Par exemple : se poser la question pourquoi une application demande à pouvoir passer des appels téléphoniques ?

Installation d'applications

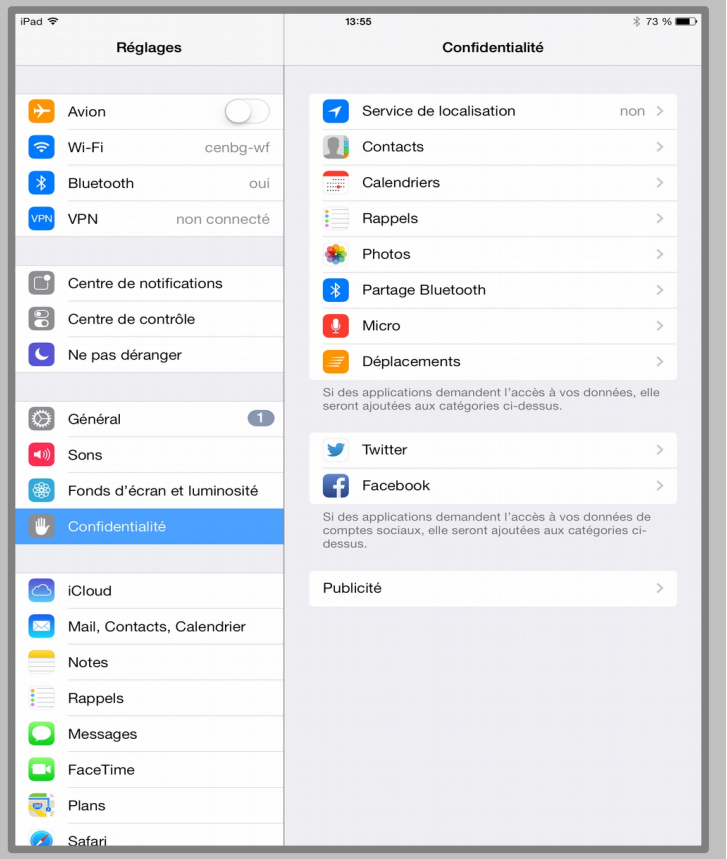
Monde Apple

- Les applications ne sont téléchargeables que depuis l'Appstore (sauf si le mobile est jailbreaké=> danger)
- L'utilisateur ne sait pas quelles ressources l'application va utiliser (accès aux fonctions téléphoniques, SMS, caméra...)
- Apple fait des contrôles sur chaque application et décide si les ressources utilisées sont légitimes ou pas

Installation d'applications

Monde Apple

- Depuis IOS 6.0
  - il est possible de visualiser quelles applis accèdent à quelles ressources
  - Pour certaines ressources, l'utilisateur doit donner son accord au moment de leur usage.



Installation d'applications

- Lire les appréciations des utilisateurs et la réputation de l'appli.
- Installez uniquement des applications utiles / ne pas tout tester
- Un jeu qui demande accès au SMS, c'est louche…
- Ne pas faire confiance au discours de l'éditeur (genre : « sécurité militaire »).

Virus et Malwares

- Comme les mobiles sont des ordinateurs comme les autres...Ils ont des vulnérabilités et ils peuvent être la cible de programmes malveillants....

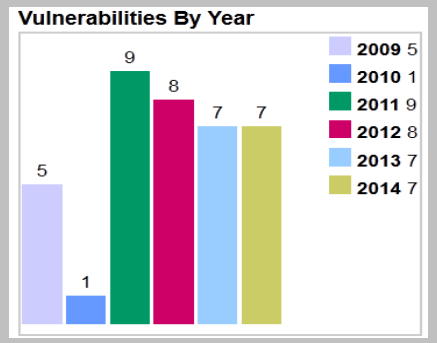
- IOS comme Androïd ont des dispositifs qui limitent fortement les « pouvoirs » d'une application dans le système, donc les possibilités pour un malware....

- ...A condition de conserver des bonnes pratiques : Ne pas rooter Jailbreaker, ne pas installer tout et n'importe quoi, ne pas installer d 'applications piratées

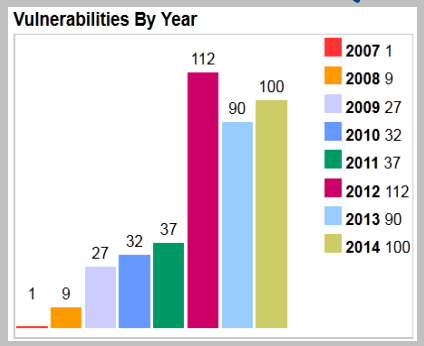
Virus et Malwares

- Les Malwares ciblent plus fortement les systèmes Androïd
  - Parce que les premières versions étaient très problématiques d'un point de vue sécurité. Le niveau de sécurité a fortement augmenté dans les dernières versions
  - Parce qu'Androïd représente 90 % des ventes
  - Parce l'eco-système Androïd est plus ouvert qu'IOS.
  - Souvent sur des systèmes rootés ou des applis piratées
  - Mais, 0,1 % des malwares proviendraient de Google Play

- Plus de vulnérabilités dans IOS que dans Androïd (au niveau système)



Androïd



IOS

Virus et Malwares

- Les problèmes ne sont pas seulement techniques

- Les techniques d'attaques par social engineering (Phishing/ Hameçonnage) sont et seront de plus en plus présentes, sophistiquées et efficaces (associant mails, SMS, Web, téléphone....)

Virus et Malwares

Un anti-virus est-il utile ?

- A ce jour, en respectant des bonnes pratiques, la probabilité d'avoir un virus est faible. Un anti-virus n'est donc pas utile
- Un anti-virus n'a pas pour fonction de compenser des mauvaises pratiques.
- Les applications anti-virus ne sont pas forcément très efficaces (applications cloisonnées) et peuvent être une source de problèmes.

Fin de vie

- Cession d'un mobile
  - Ne cédez pas votre mobile sans ré-initialisation (paramètres d'usine)
- Panne/Fin de vie
  - Avant de rapporter le mobile au centre de recyclage, le ré-initialiser
- Perte / vol /
  - Déclarer l'incident au chargé de sécurité de votre unité, même si c'est du matériel perso !
  - Changer, le plus rapidement possible, tous les mots de passe de vos comptes qui seraient enregistrés dans le mobile (en faire la liste ...avant!)
  - Eventuellement utilisez la fonction de destruction à distance (efficacité incertaine)

Passcode

- Conseils
  - Rendre la frappe des mots de passe sur le clavier invisible

Paramètres/Sécurité/décocher la case « Rendre les mots de passe visibles »

  - Activer le verrouillage automatique après un temps d'inactivité.

Réglages/Général/Verrouillage automatique

Paramètres/Affichage/mise en veille de l'écran

Passcode

- Déblocage du mobile lorsque le passcode est oublié
  - Inutile d'aller voir un marabout
  - Ne pas confondre le pin code de la carte SIM et passcode de déverrouillage du système
  - L'opérateur qui a vendu le mobile peut ré-initialiser le pin code de la carte SIM mais pas le passcode du système
  - Il existe des procédures pour Androïd et Apple
  - En cas d'échec, il faut ré-initialiser le mobile

Passcode

- Déblocage du mobile lorsque le passcode est oublié
  - Sous Androïd, 3 possibilités
    - Soit avec les fonctions de contrôle à distance (voir plus loin)
    - Soit directement sur le mobile
      - Après 5 tentatives infructueuses, Il est possible d'utiliser « Mot de passe oublié ? »
      - Le nom du compte Google et son mot de passe sera alors demandé, puis il sera possible de spécifier un nouveau passcode.
    - Si aucune méthode ne fonctionne il faudra ré-initialiser le mobile en configuration d'usine.

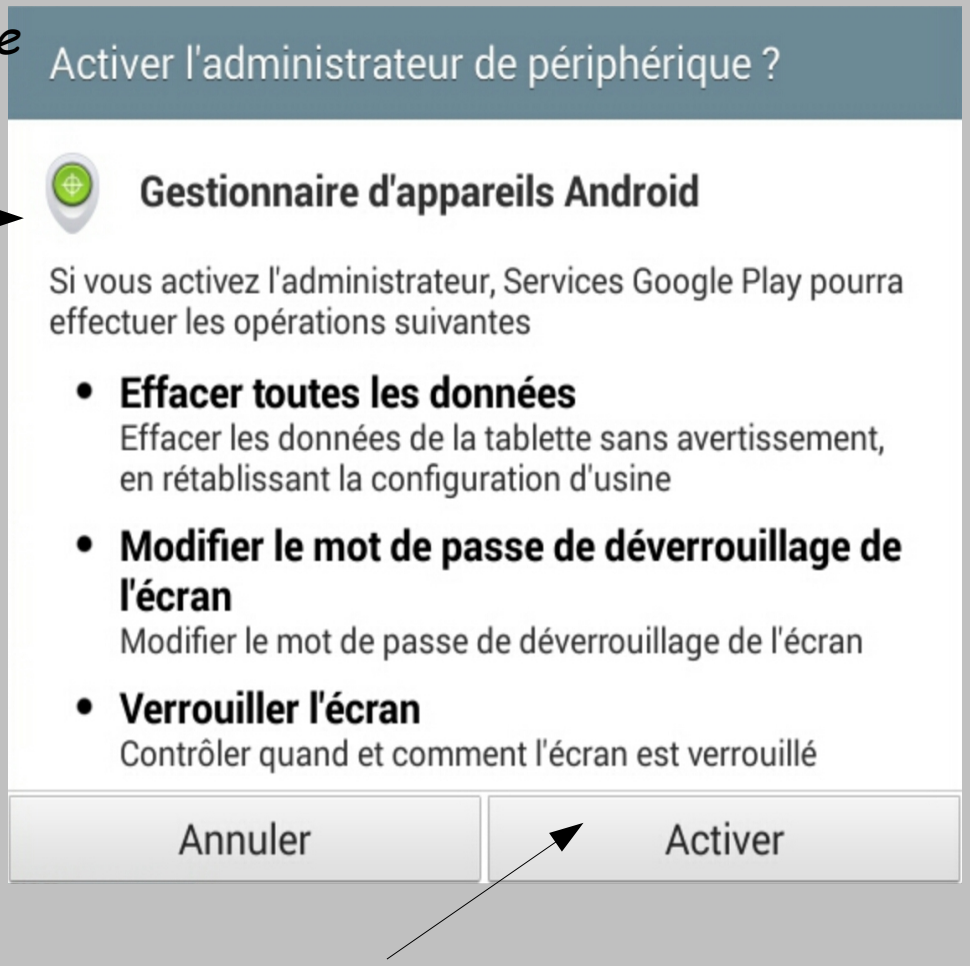
Passcode

- Déblocage du mobile lorsque le passcode est oublié
  - Sous IOS, 2 possibilités
    - Soit une sauvegarde a été réalisée avec iTunes sur un micro-ordinateur et il est possible de la restaurer (un nouveau passcode sera demandé)
    - Soit il n'y a pas eu de sauvegarde, il faut alors ré-initialiser le mobile en configuration d'usine (tout sera perdu)

Fonction de contrôle à distance d'un mobile

Ces fonctions doivent être activées avant de perdre un mobile

Paramètres/sécurité/Admin. de périphérique



Fonction de contrôle à distance d'un mobile

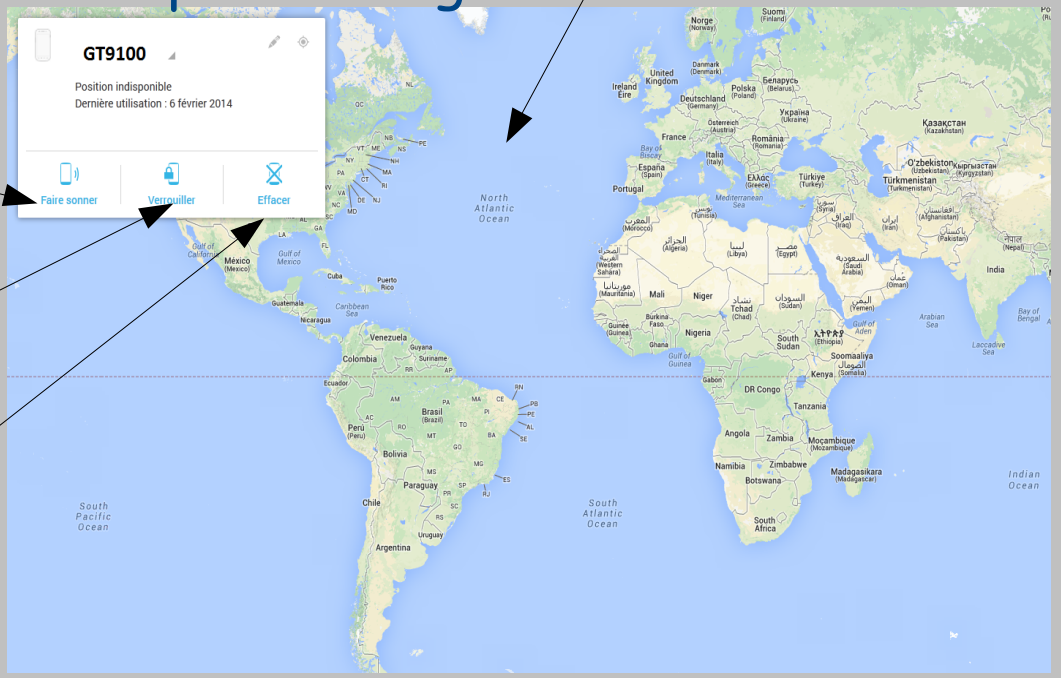
- Le mobile doit être connecté au réseau pour que cela fonctionne (ou cela fonctionnera dès qu'il s'y connectera)
- A partir d'une autre machine se connecter sur *https://www.google.com/android/devicemanager*
  Il faut fournir son compte et mot de passe Google

Localise le mobile (si possible)

Faire sonner le mobile

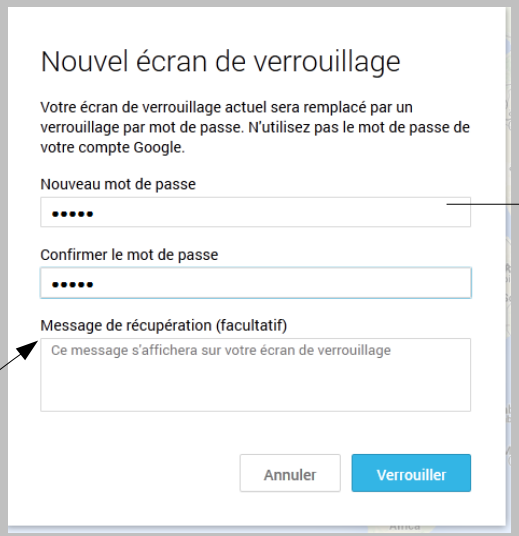
Positionner un nouveau mot de passe de verrouillage d'écran

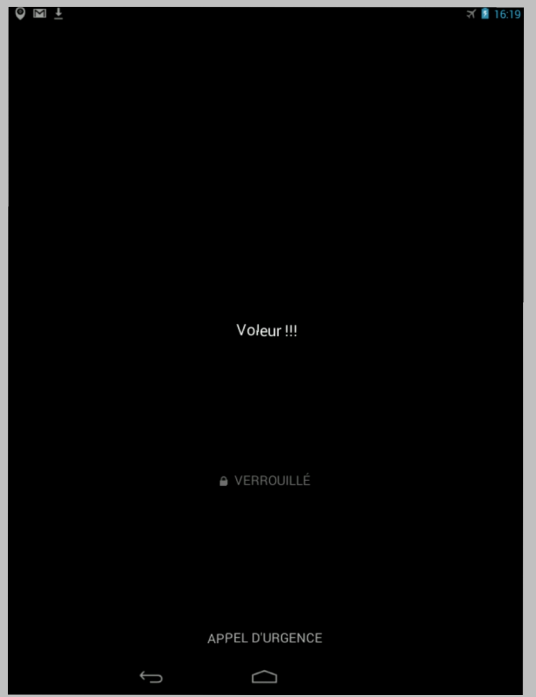
Supprimer les données



Fonction de contrôle à distance d'un mobile

- Verrouillage à distance ou passcode oublié
  - Permet de positionner à distance un nouveau mot de passe de verrouillage
  - Utile aussi quand on a perdu son mot de passe.
  - Il faut simplement indiquer un nouveau mot de passe et, éventuellement, un message qui s'affichera sur l'écran.





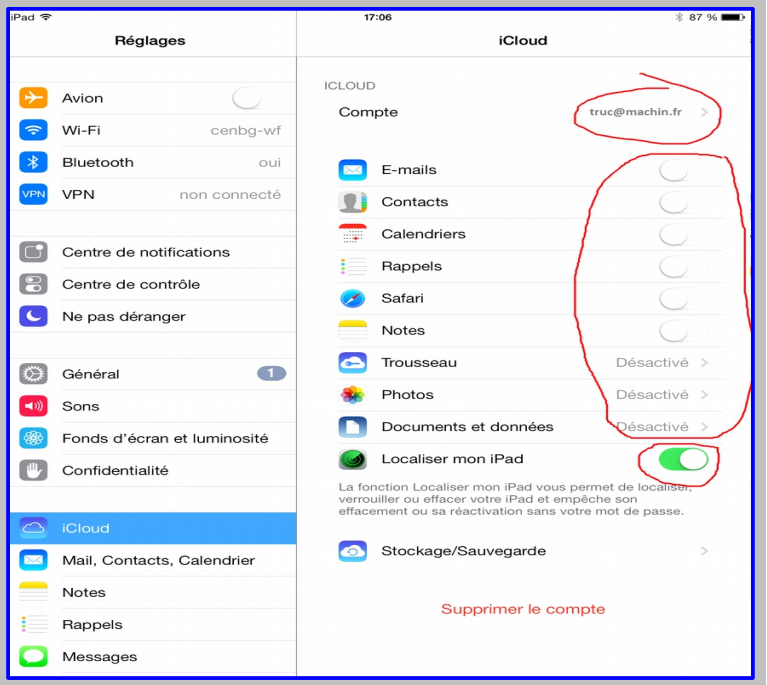
Fonction de contrôle à distance d'un mobile

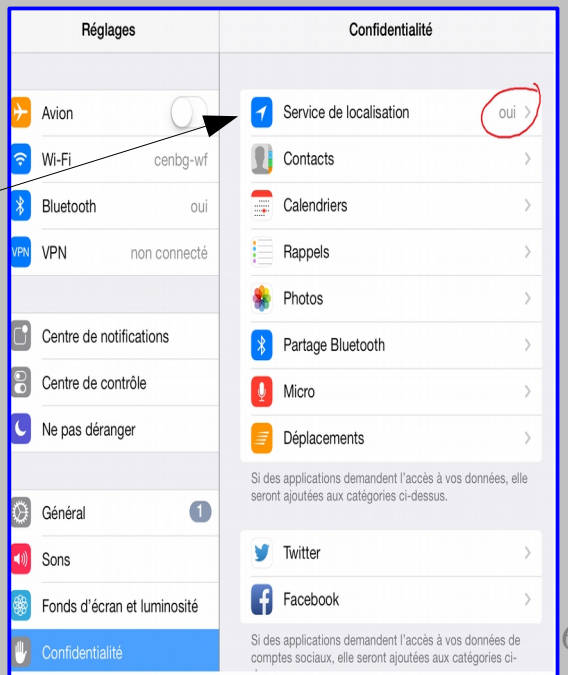
- Destruction des données à distance

  Re-initialise le mobile en configuration d'usine

Fonction de contrôle à distance d'un mobile

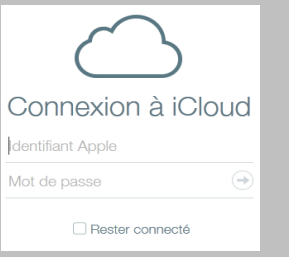
- Nécessite d'activer (avant la perte) un compte iCloud (avec AppleId)
- Attention iCoud permet de faire d'autres choses que du contrôle à distance.
  Notamment des synchronisations dans le Cloud Apple
- Ce qui veut dire, que si ces fonctions ne sont pas désactivées toutes les données sur le mobile seront copiées chez Apple
- Désactivez tout si pas nécessaire, surtout s'il y a des données professionnelles
- Activez uniquement « Localiser mon Ipad »
- Activez aussi le service de localisation.



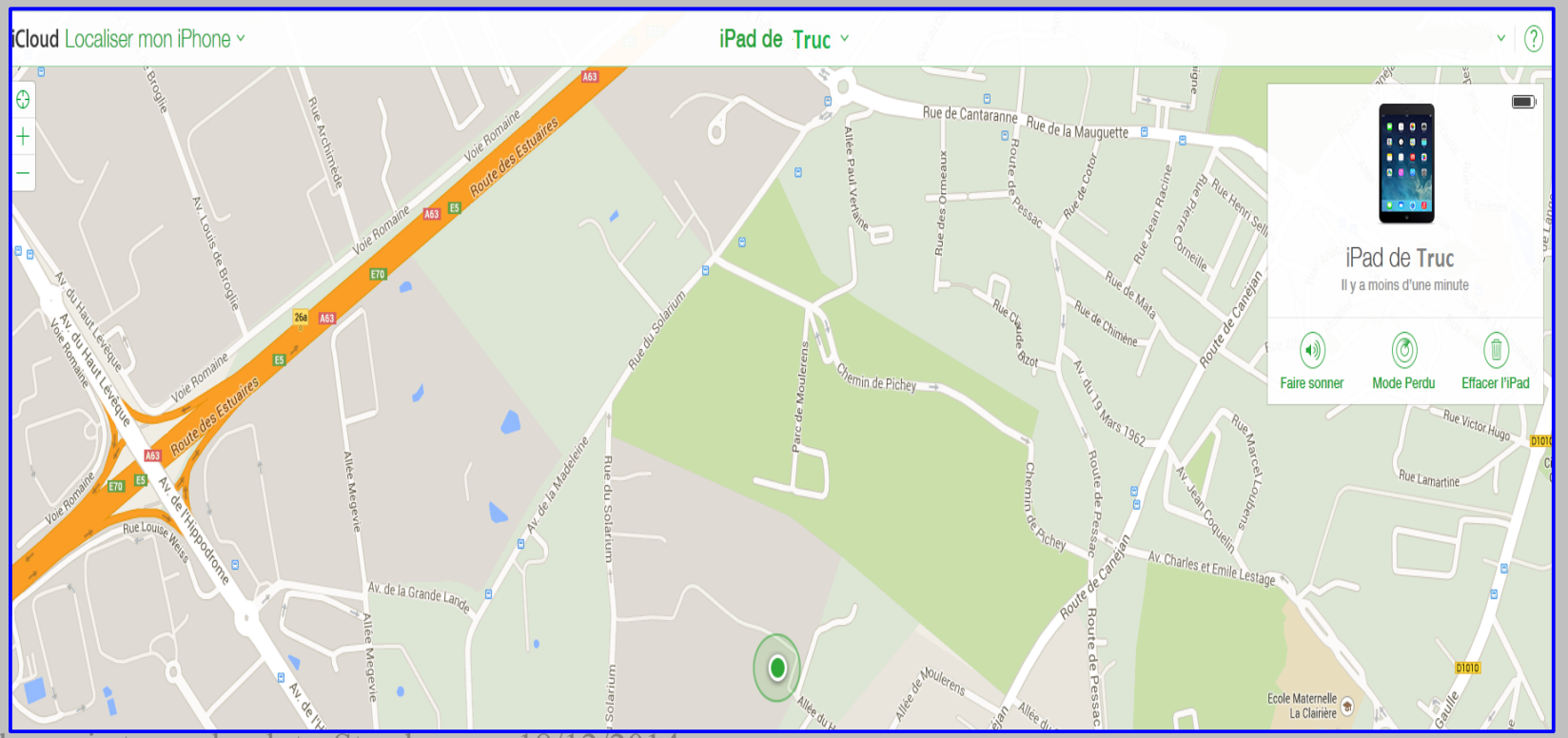


Fonction de contrôle à distance d'un mobile

- Les fonctions à distance permettent de faire sonner le mobile, le bloquer ou l'effacer...pas de changer le code de verrouillage.



- Il faut se connecter depuis une autre machine sur iCloud (https://www.icloud.com) avec son compte Apple



Partage entre plusieurs utilisateurs

- Sur Androïd (uniquement) utilisez la fonction multi-utilisateur (>=4.3)
- Possibilité de créer plusieurs comptes utilisateurs indépendants
- Chaque compte a son propre environnement
- Pratique en environnement familial.
- Possibilité de restreindre les possibilités d'un compte
  (par exemple, autoriser explicitement une liste d'applications.
  Interdire l'accès à Play Store....)
- Pratique aussi pour créer un compte professionnel protégé.

Chiffrement

- Chiffrement

  - Les iPAD, iPhone disposent d'un processeur cryptographique qui chiffre en permanence le contenu de la mémoire flash. Il n'y a rien à faire pour l'activer.
  - Ce chiffrement ne sert à rien s'il n'y a pas de passcode.
    Note : avec IOS 8 le passcode semble désormais obligatoire

  - Les matériels Androïd doivent être chiffrés volontairement
    Paramètres/sécurité/Crypter l'appareil.
    Note : Avec Androïd 5, le chiffrement sera activé à l'initialisation du mobile.

  - Le fait de chiffrer impose de positionner un passcode.

Questions ?

http://obtenir.cnrs.fr