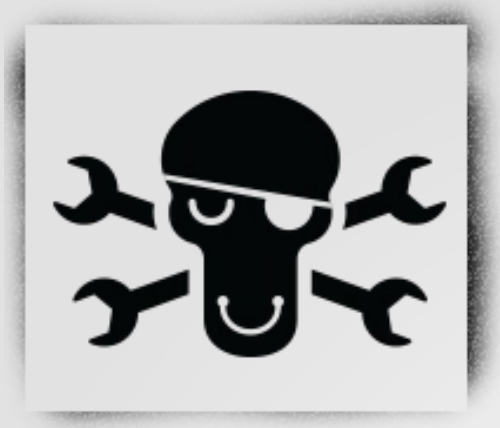


OPEN BIDOUILLE CAMP 33 #2

Crypto—Party :

Sécurité, vie privée et appareils mobiles

(connectés aux réseaux de téléphonie mobile)

17 — 18 mai 2014

Paul Kocialkowski
paulk@replicant.us

Appareils mobiles ?

Famille d'appareils électroniques :

- Téléphones simples
- Smartphones/ordiphones/téléphones intelligents
- Tablettes connectées (3G/LTE)

Caractéristiques :

- Connectés aux réseaux de téléphonie mobile (modem)
- Transport de voix (appels)
- Transport de messages (SMS)
- Transport de données (GPRS/EDGE/UMTS/HSPA/LTE)

Appareils utilisés au quotidien et transportés partout !

Sécurité, vie privée ?

Sécurité et vie privée : même combat !

Pour quoi, pour qui, contre quoi, contre qui ?

- Ne rendre accessible que ce-que l'on souhaite
- Seulement aux gens que l'on souhaite
- Anonymat

Définition générale, s'applique à de nombreux domaines de la vie !

Sécurité, vie privée ?

Réclamer le droit à la vie privée, c'est avoir des choses à cacher ?

- Modèle de société : contrôle ou liberté ? 1984
- Liberté fondamentale
- Contre-pouvoir, opposition
- Journalisme
- Activisme politique

C'est souvent se protéger de l'État avant tout !

- Pays dictatoriaux
- Respect des libertés
- Sanctions et peines

Sécurité, vie privée ?

Quel intérêt si on n'est pas engagé politique ou journaliste controversé ?

- Sommes-nous jamais à l'abri d'une dictature ?
- Engagement futur
- Relations entre les individus

Mais pourtant, avec la collecte des données :
C'est déjà trop tard !

Sécurité, vie privée ?

Quel intérêt si on n'est pas engagé politique ou journaliste controversé ?

- Sommes-nous jamais à l'abri d'une dictature ?
- Engagement futur
- Relations entre les individus

Mais pourtant, avec la collecte des données :
C'est déjà trop tard !

Enjeux :
- Se faire vider son compte en banque ?
- Besoin fondamentalement politique
- Respect de l'individu, nuisance (publicité, revente, etc)

Quelles sont les vulnérabilités ?

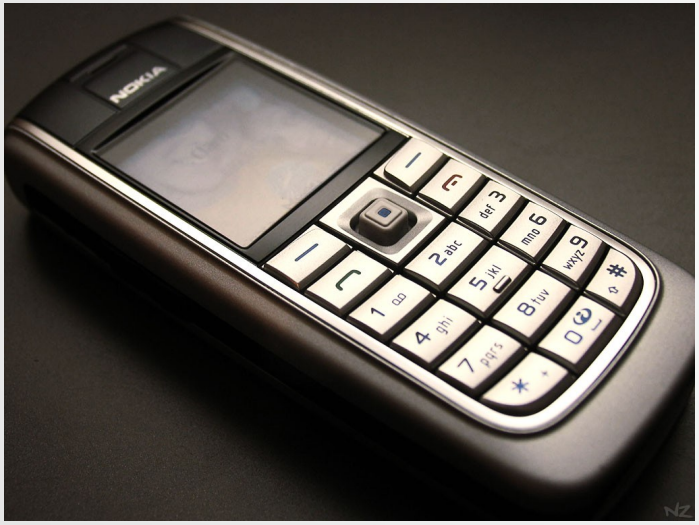
- Communications : voix, messages : pas sûrs
- Données mobiles : pas sûr
- Données du téléphone (contacts, messages envoyés et reçus, photos, documents)
- Accès aux capteurs du téléphone (microphone, GPS, camera) qui en disent sur l'état actuel de la personne (localisation, gens avec qui on discute, qu'est-ce qu'on dit)

Quelles solutions possibles ?

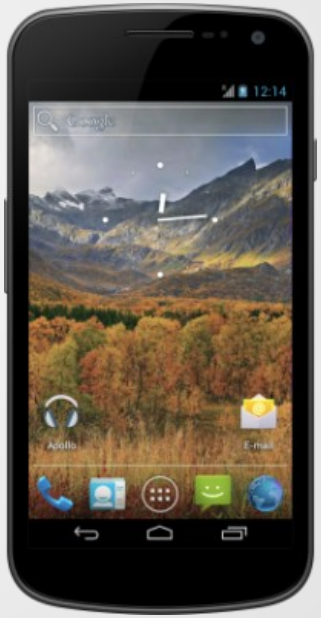
- Communications : encrypter de pair à pair
- Données mobiles : encrypter de pair à pair
- Données du téléphone : encrypter les données, éviter les logiciels propriétaires (Backdoor)
- Accès aux capteurs du téléphone : choisir un téléphone qui donne peu d'accès au matériel pour les logiciels propriétaires restants

Quelles solutions pratiques ?

- Quels téléphones utiliser ?



- Téléphone simpliste

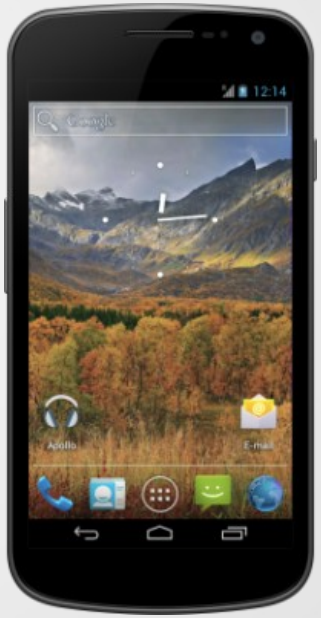


- Smartphone
- Ordiphone
- Téléphone intelligent

Quelles solutions pratiques ?

- Quels téléphones utiliser ?

- Téléphone simpliste



- Smartphone
- Ordiphone
- Téléphone intelligent

Quelles solutions pratiques ?

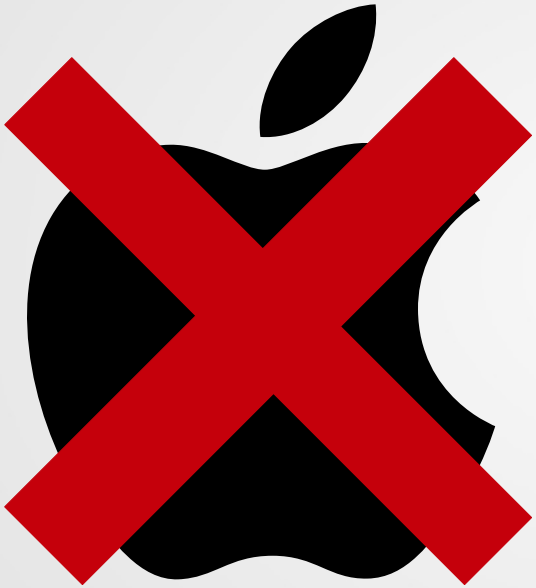
- Quels systèmes d'exploitation ?

- Apple

- Android et dérivés

Quelles solutions pratiques ?

- Quels systèmes d'exploitation ?



- Apple

- Android et dérivés

Quelles solutions pratiques ?

Appareils les mieux pris en charge par les logiciels libres :

- Google Nexus (S/Galaxy Nexus)
- Samsung Galaxy

Systèmes d'exploitation les plus libres :

- Android (mieux que Apple ou autres)
- CyanogenMod, OmniROM
- Replicant

Quelles solutions pratiques ?

Logiciels de communication encryptés :

- RedPhone
- TextSecure
- Chatsecure (XMPP)
- CsipSimple (SIP)
- K9 + AGP
- Tor : Orbot, Orweb

Bonnes pratiques :

- N'installer que des logiciels libres (F-Droid)
- Encrypter les données
- Utiliser https dès que possible

Texte :

- © 2014 Paul Kocialkowski
  Licence Creative Commons BY-SA 3.0

Images :

- **Replicant robot**, © Mirella Vedovetto, Paul Kocialkowski,
  Licence Creative Commons BY-SA 3.0