EthACK

The Swiss Privacy Basecamp

EthACK ?

- Éthique
- État
- ACKnowledgement (reconnaissance)
- Hacking (éthique, évidemment)
- ...

Pourquoi ?

- Notre gouvernement ne s’intéresse pas (ou peu) au sujet
- Les sociétés privées nous fichent à notre insu
- Personne ne sait où sont leurs données, qui les traitent, à quoi elles servent

Notre mouchard de poche

Cédric Jeanneret (aka @SwissTengu)

EthACK.org

28 octobre 2015

Description de la menace

- Vol de l’appareil
- Applications “indélicates”
- Fournisseurs de services “cloud”
- Écoute au niveau de l’antenne GSM

Smartphones vs Smartusers

- Que sait notre smartphone ?
- Comment mitiger ?
- Applications disponibles
- ROMS alternatives : bien, ou pas bien ?
- Bonnes pratiques

Quelques chiffres

- 1.5 milliards de smartphones dans le monde (2013)
- Plus de 10 millions de cartes SIM en Suisse (OFCOM 2012)
- Plus de 75% des utilisateurs accèdent à Internet via leur smartphone (en Suisse)

Quelques chiffres et faits

- Plus de **16’600 To** de communications Internet depuis le réseau mobile (OFCOM 2012)
- Chiffrement GSM cassé en 2009
- La 2G ne valide pas l’antenne, que le client
- Technologie >= 3G identifie les deux

Xmbplfgrz ? !

GSM

standard “2G” (seconde génération), remplace “1G” (première génération)

3G

Troisième génération du standard

Chiffrement

brouiller le contenu à l’aide d’un “chiffre” (crypter dans les médias)

Le contraire de “chiffrer”

déchiffrer

décrypter

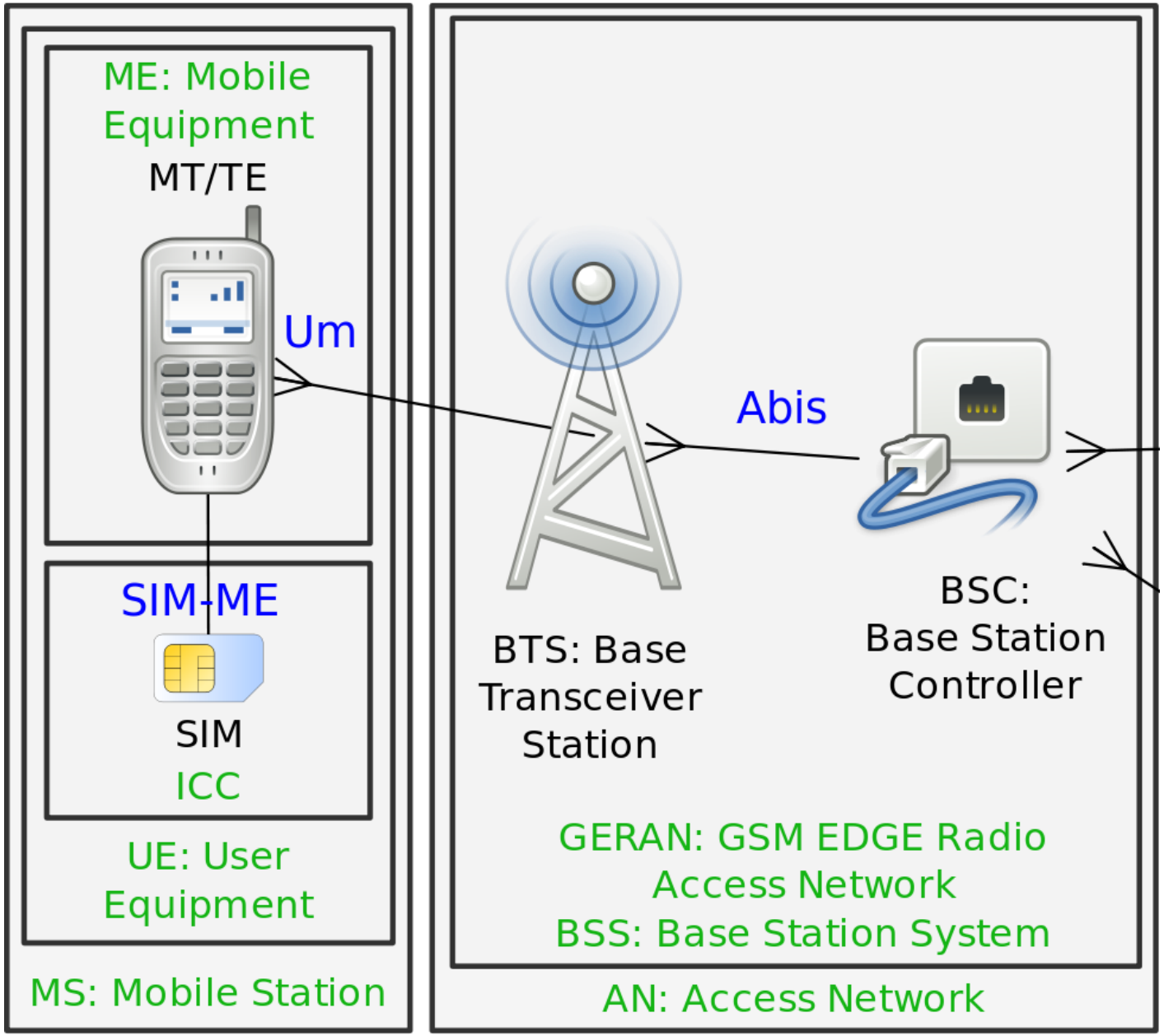
casser le chiffrement sans le chiffre

Mais c’est sécurisé. . . Non ?

Voui, bien sûr ;)

Les communications (SMS/Voix) sont déchiffrées au niveau de l’antenne.

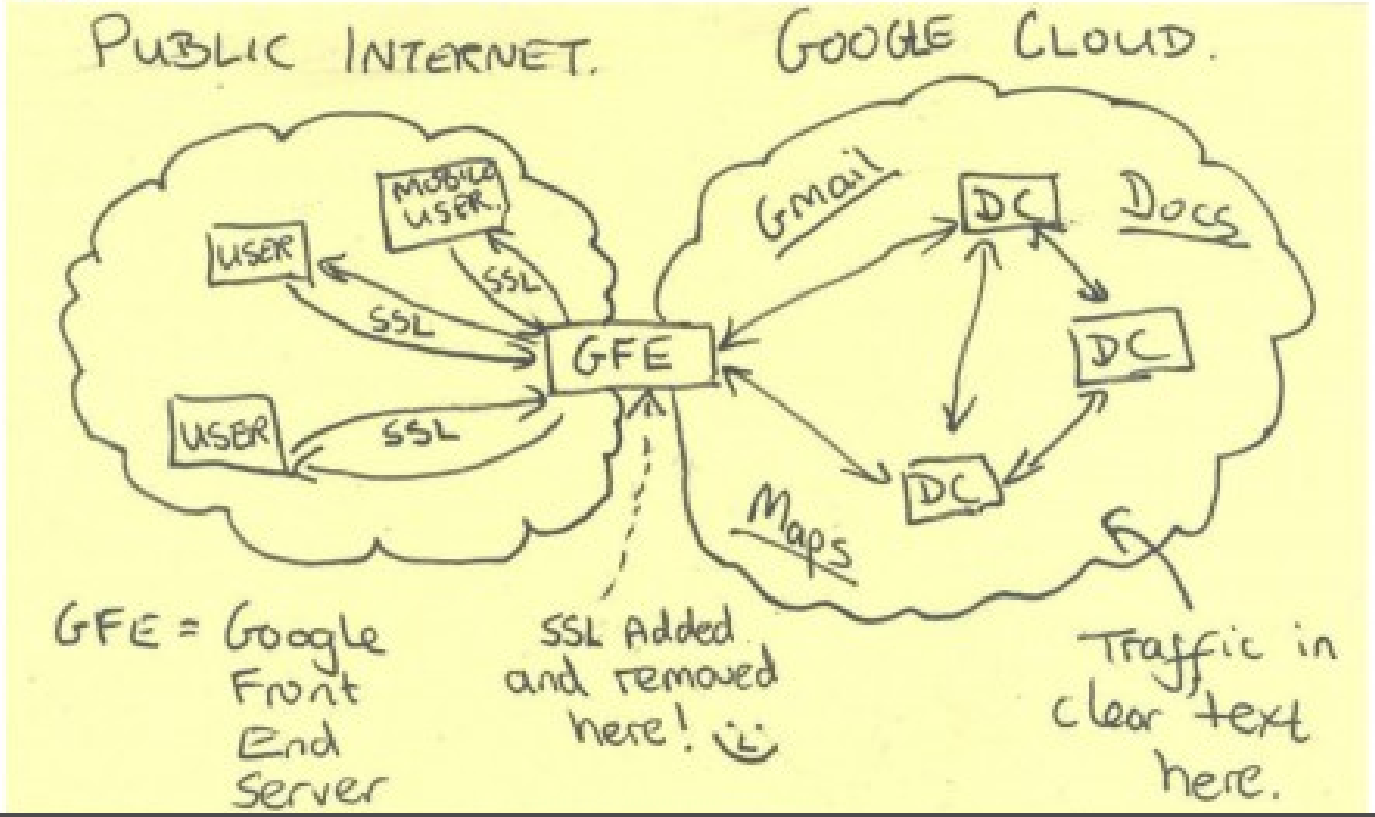
Y compris quand vous êtes à l’étranger


ME: Mobile Equipment
MT/TE
Um
SIM-ME
SIM
ICC
UE: User Equipment
MS: Mobile Station
Abis
BTS: Base Transceiver Station
BSC: Base Station Controller
GERAN: GSM EDGE Radio Access Network
BSS: Base Station System
AN: Access Network

Rappelez-vous ;)

TOP SECRET//SI//NOFORN

Current Efforts - Google



Smart, so smart

- Localisation
- Contacts
- Données biométriques
- Données médicales
- Reconnaissance faciale
- Intéractions numériques et humaines
- *OK Google, OK Glass, Siri*
- Amazon Echo Voice Control System

Capteurs

Gyroscope

Position dans l’espace

Accéléromètre

Direction du mouvement (et déduction vitesse)

Écran tactile

Manière de faire le *swipe* et *tap*

Baromètre

Données sur votre emplacement (altitude, conditions etc)

Empreintes des capteurs

Imprécisions au niveau des capteurs

Permettent d'identifier l'appareil de manière précise et unique (ECE ILLINOIS)

Votre utilisation

Permet de vous identifier de façon unique

Biométrie et santé

Des données qui ne peuvent pas changer

- Sur un appareil qu'on peut perdre
- Sur un appareil qui peut se faire voler
- Sur un appareil configuré par défaut pour envoyer son contenu sur le Net
- Vos empreintes couvrent l'appareil

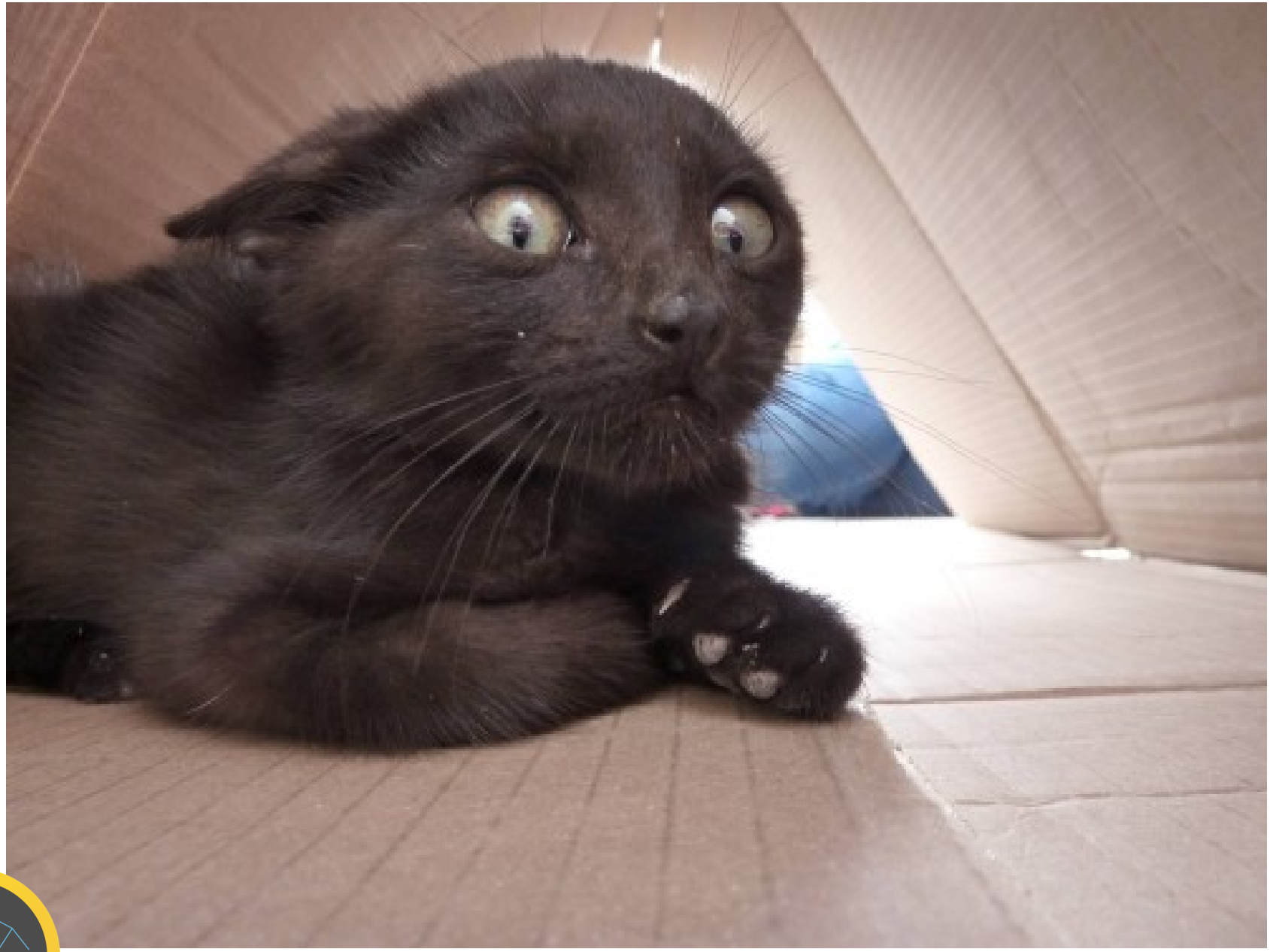
Données médicales

Adieu, secret médical...

Données immuables servant de mot de passe

“Suite à une fuite de données, merci de changer vos empreintes digitales”

Ou votre rétine. . .



On ne va pas se laisser faire tout de même !?

Quelques préliminaires.

Jamais le premier soir

Commencer par trier les applications

- Désactiver/désinstaller les applications inutiles
- Attention aux “packs fournisseurs”

Éviter de s’enregistrer auprès des services “remote”

. . . même si c’est “tellement pratique”

Ni le second

Attention aux permissions !

- Est-ce qu'un jeu a réellement besoin d'accéder aux *contacts* ?
- Est-ce qu'un calendrier a réellement besoin de la *localisation* ?
- Est-ce qu'un lecteur de musique a réellement besoin du *journal des appels* ?

Sortez couverts

Désactivez le GPS

La plupart du temps, le GPS est inutile

Désactivez le NFC

Near Field Contact : “utile” pour paiement sans contact ou transferts, mais 99% du temps inutile

Désactivez Internet

Apprenez à ne plus être connecté 100% du temps. Votre batterie vous dira merci ;)

Désactivez le Bluetooth

Idem que pour le NFC.

Pourquoi désactiver ?

Batterie

L'autonomie est déjà assez mauvaise (une journée) sans en rajouter...

Publicité ciblée

Des magasins utilisent déjà Internet et votre géolocalisation pour vous cibler

NFC

Votre appareil lit et peut être lu, transmettre/recevoir des données à votre insu, etc.

Bluetooth

Identité BT ; bornes dans les magasins

Marketing on NFC

Alex Do (Landor, Fab.com)

> “We could use NFC to push information to customers’ mobiles as they walk through malls”
>
> “[. . .] they could use NFC to advertise digitally - to push deals, VIP invites, and announce new product releases to attract customers to their stores”

Source : WPP

Regardez aussi “nfc marketing usage”. . .

Donc on est fichu

Oui. Et fiché, surtout.

Mais on peut lutter.


SHOW ME YOUR WAR FACE!

Se découpler des services centralisés

Centralisation ?

Une entité possède *toutes* vos données.

Solution

Employer différents services chez différents fournisseurs.
Si possible “locaux” (lois suisses, for juridique en Suisse, etc).

Décentralisation — contacts et calendriers

- **DAVDroid** (opensource, demande un hébergement spécialisé ; compatible OwnCloud, Baïkal, etc)

Décentralisation — fichiers

- **Spider Oak** (propriétaire, US ; chiffrement côté client)
- **OwnCloud** (opensource, US ; hébergement possible sur owncloud.com)
- **Seafile** (opensource, Chine ; hébergement possible sur seafile.com)

. . . et plein d'autres solutions qui se développent tous les jours

Décentralisation — Mails

Alternatives à gmail, hotmail et autres

- **Infomaniak** (Suisse ; à partir de 24CHF/an)
- **Tutanota** (Allemagne ; gratuit, ou offres "business")
- **ProtonMail** (Suisse ; gratuit, mais liste d'attente)
- **EthACK** (Suisse ; oui, on planche dessus (depuis 2014...))

Décentralisation — Messagerie instantanée

Alternatives à GTalk, iChat, iMessages et autres

- **chatSecure** (opensource ; permet d'employer votre compte gmail ou autres XMPP/Jabber)
- **TextSecure/Signal** (opensource ; échange de messages à-la Whatsapp, chiffrés)
- **SMSSecure** (opensource ; envoi de SMS chiffrés)
- **Threema** (propriétaire ; échange de messages à-la Whatsapp, chiffrés)

ROM alternatives

ROM ? (Read Only Memory)
Système d'exploitation installé sur le smartphone

iOS ?

À notre connaissance, possible uniquement pour Android.

Avantages de changer l'OS

Libre

Les ROM alternatives sont libres et ouvertes, avec de solides communautés

Le choix

Il y a une certaine quantité d'alternatives existantes

Vous reprenez votre appareil en main

En choisissant une ROM adaptée à vos besoins
En choisissant d'installer ou non Gapps
En évitant les "packs opérateurs"

Inconvénients

Garantie

Il est possible que la garantie soit annulée

Connaissances

Flasher un appareil demande 2-3 connaissances de base

Limitations du choix de l'appareil

Pas pour tous les appareils Android (secureboot, etc)

Droits

On se retrouve avec des droits avancés — amis Virus, bonjour !

ROM “reconnues”

- CyanogenMod
- ParanoidAndroid
- SlimROMs
- AOKP
- PAC-ROM
- Replicant

To flash or not to flash, that’s the question

Up to you folks ;)


FunnyKittenSite.com

Bonnes pratiques

Bloquer l’écran
: En évitant la biométrie

Chiffrer les données
: Évitez de perdre le mot de passe. . .

Désactiver le superflu
: Applications, services, fonctionnalités

Bonnes pratiques

Contrôler les permissions

Même si on ne peut pas toujours les limiter

Lire les Conditions Générales d'Utilisation

Même si c'est indigeste

Installer le strict nécessaire

Avez-vous réellement besoin de l'application "coussin péteur" ?

Furz Sound Board

Kaufcom Games Apps Widgets

Kostenlos

Fotos/Medien/Dateien
- Zugriff auf geschützten Speicher testen
- USB-Speicherinhalte ändern oder löschen

Kamera/Mikrofon
- Audio aufnehmen

WLAN-Verbindungsinformationen
- WLAN-Verbindungen abrufen

Geräte-ID & Anrufinformationen
- Telefonstatus und Identität abrufen

Bei Updates von Furz Sound Board können in jeder Gruppe automatisch zusätzliche Funktionen hinzugefügt werden.
Weitere Informationen

Schließen

Il existe deux choses qu'on ne peut pas limiter

Qui peut :

- Accéder à toutes vos informations
- Accéder à tous vos SMS
- Accéder à tous vos appels
- Exécute des commandes bas niveau
- Posséder de multiples failles non-corrigées
- Ne peut pas être mis à jour facilement pour appliquer des correctifs

Une idée ?

Réponse

Réponse

Baseband

- Très bas niveau dans l’appareil
- Propriétaire, bardée de brevets
- Déjà plusieurs preuves de vulnérabilités
- Très bas niveau, donc dur à mettre à jour

Réponse

Baseband

- Très bas niveau dans l'appareil
- Propriétaire, bardée de brevets
- Déjà plusieurs preuves de vulnérabilités
- Très bas niveau, donc dur à mettre à jour

L'utilisateur

- Ne réfléchit pas toujours
- Adore cliquer sur tous les liens possibles
- Adore installer tout et n'importe quoi
- Fait rarement les mises à jour de son appareil

En résumé

Ne soyez pas plus bêtes que votre smartphone,
et tout ira bien ;)

Questions ?

https://ethack.org/

@EthACK_org on Twitter

ethack.org on Facebook