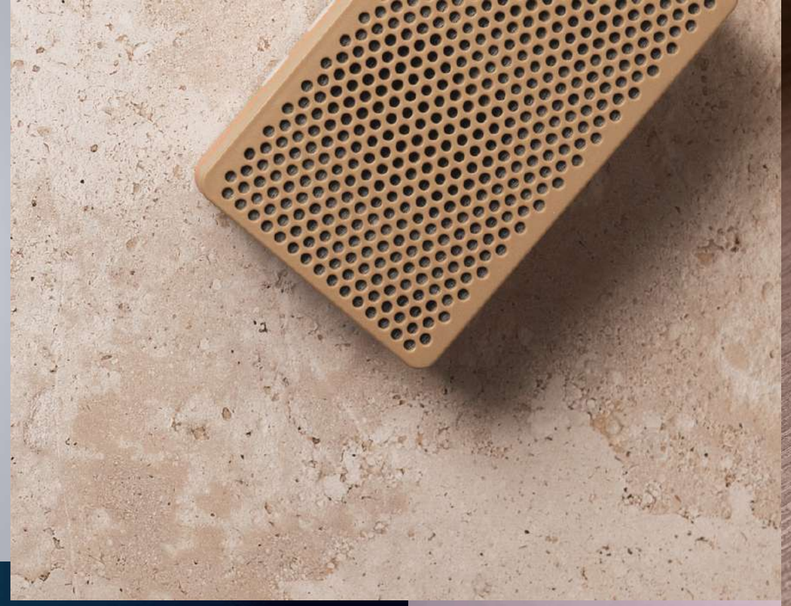
Le Bluetooth

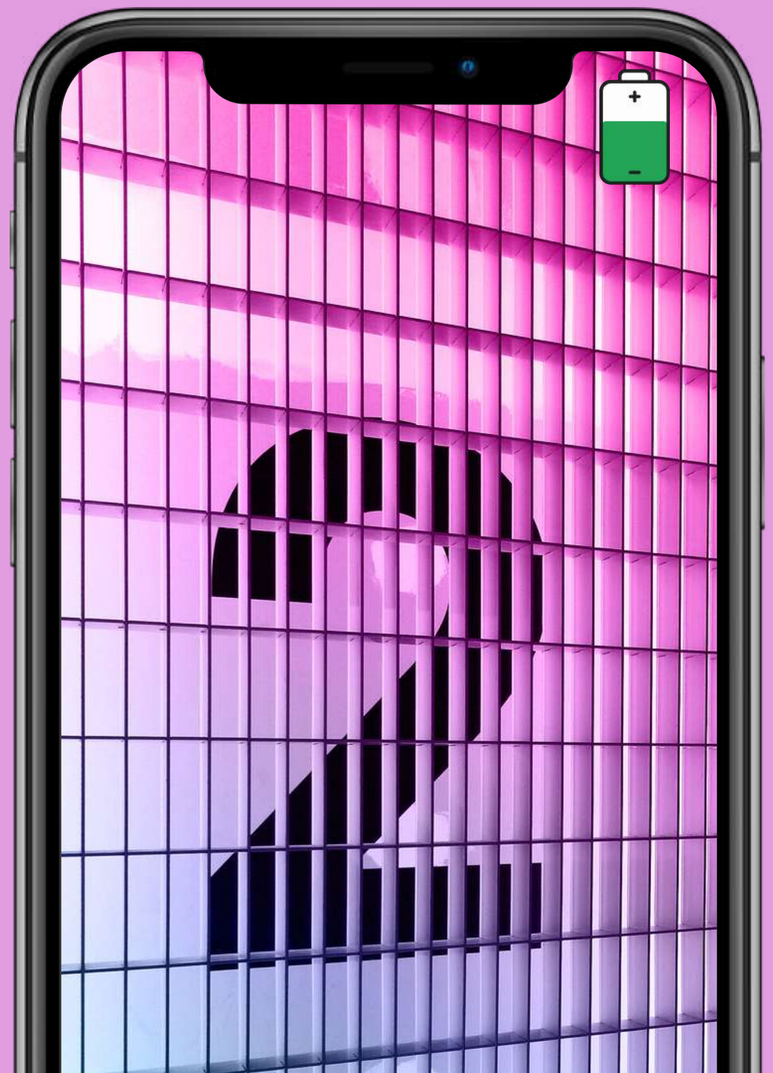


Guillaume D.

Qu'est-ce que le Bluetooth

-Norme de télécommunications

-Ondes radio UHF sur la bande de fréquence de 2,4 GHz



Pourquoi Bluetooth ?

LE ROI VIKING (DANOIS),

HARALD BLUETOOTH

900 A.P *Djayzus Croayyst*

HISTOIRE:

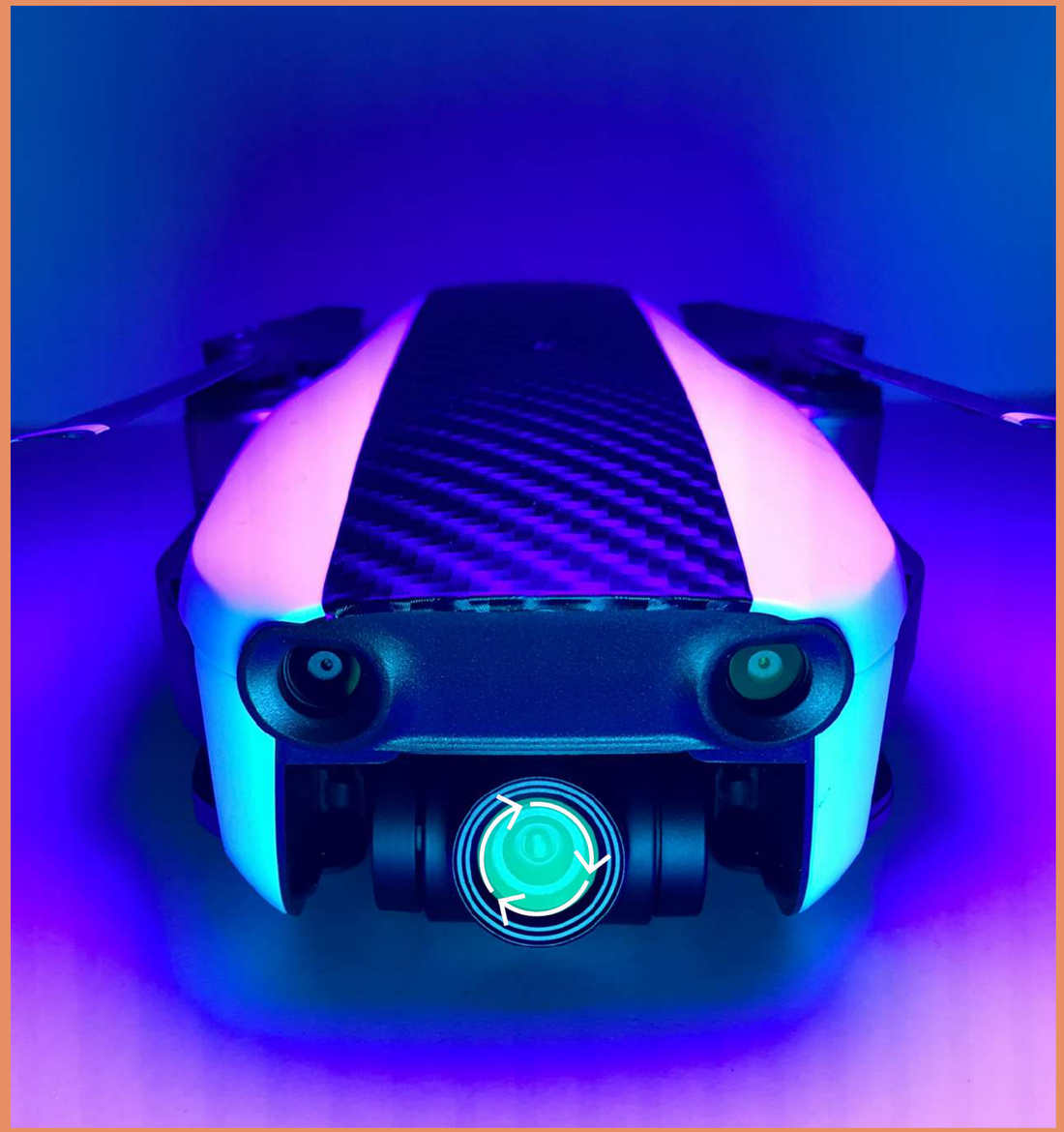
- Créé en 1994. par "Ericsson"

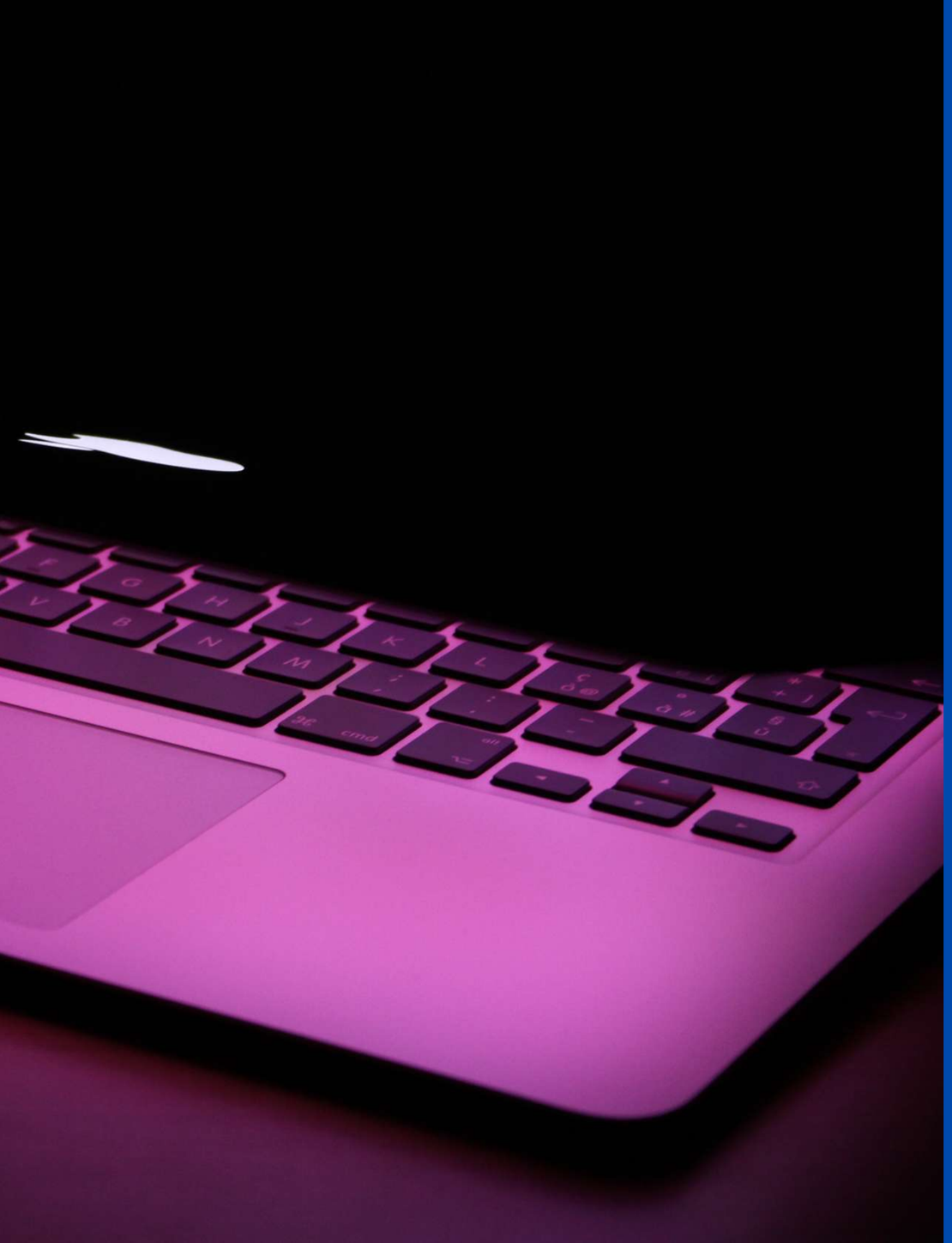
- En 1999, premier téléphone portable (BT 1.0)

- 2006, Version 2.0 (aug. débit de transfère)

- 2009, la 3.0 sera révolutionnaire!

- 2013, 2014, 2016, 2019 sortie des différentes versions





TECHNIQUE :

10 m de portée ... mais jusqu'à 100m !!!

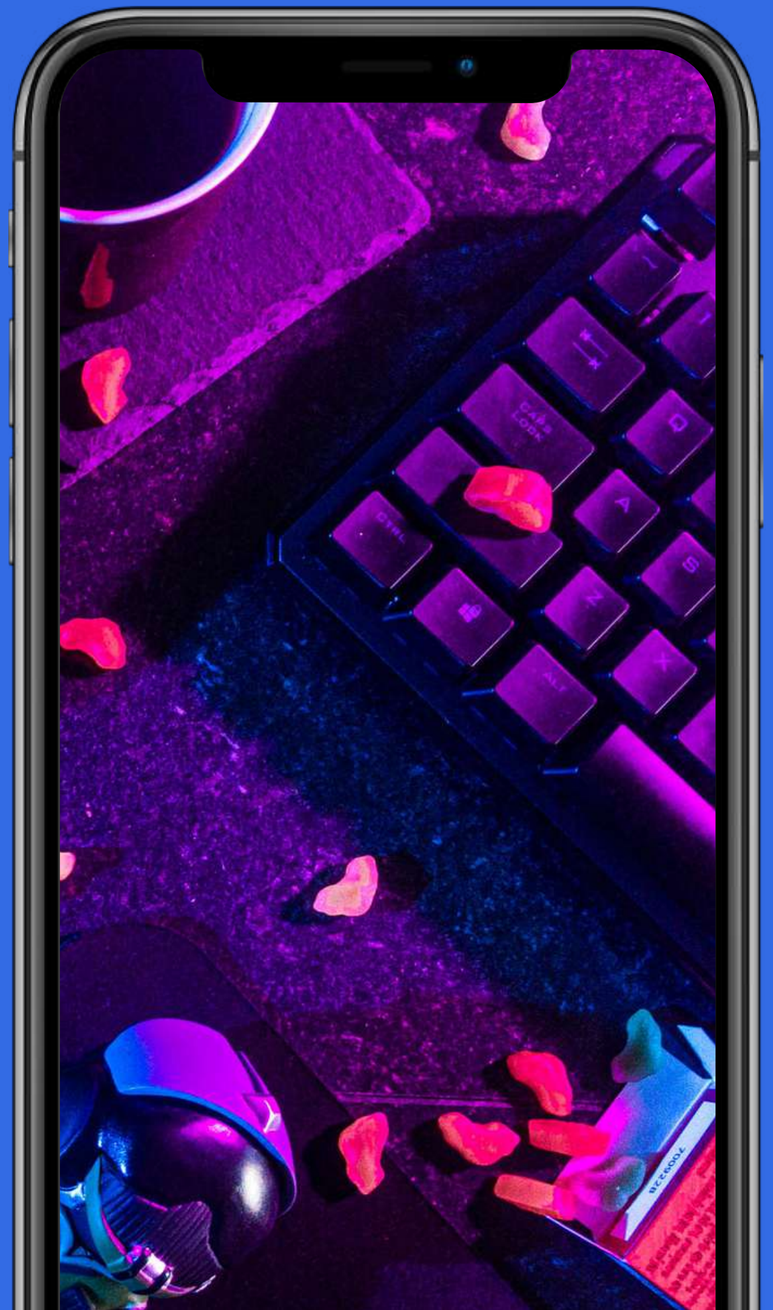
Deux appareils s'échangent une clé secrète appelée "clé de liaison pré-partagée"

un identificateur unique de 48 bits (typeMAC)

PENSEZ SÉCURITÉ !

Le Bluetooth vous facilite la vie..

..ET CELLE DE HACKERS.



QUELQUES EXEMPLES:

2017 la faille Blueborne:
Déployement de codes malicieux
via les privilèges élevés.

2020 la faille BLURtooth:
connexion via bipass de
protocole d'appairage.
4.0 et 5.0

HAUT-PARLEURS

- Shodan
- Shodansploit

-Bluejacking

-Bluesnarfing

-Bluebugging

-Bluesmack

COMMENT S'EN PROTÉGER?

- Se déconnecter
- Passer au filaire
- Une pomme par jour en forme toujours
- Passer sur un OS tiers

HACKING PARTY

Bluelog : Un outil d'étude. Il scanne la zone pour trouver les périphériques découvrables et les enregistre ensuite dans un fichier.

Bluemahoho : Une suite d'outils basée sur une interface graphique pour tester la sécurité des périphériques Bluetooth.

Blueranger : Un script Python simple qui utilise les pings i2cap pour localiser les périphériques Bluetooth et déterminer leurs distances approximatives.

Btscanner : Cet outil basé sur une interface utilisateur graphique recherche les périphériques détectables à portée de main.

Redfang : Cet outil permet de trouver un périphérique Bluetooth caché.

Spooftooph : il s'agit d'un outil de spoofing Bluetooth.

Bettercap : Bettercap est le successeur d'Ettercap et comporte des modules d'attaque pour différents types de technologies radio et réseau, dont le Bluetooth.
Bettercap peut traquer et attaquer des réseaux Wi-Fi, et par défaut, commence à énumérer les périphériques sur n'importe quel réseau.

Sources:

https://www.youtube.com/watch?v=Az-l90RCns8&t=102s&ab_channel=Armis

https://untelephone.com/guide-pirater-un-portable-par-bluetooth/

GENERATION 4.0/5.0(A PARTIR DE 2021)

SAMSUNG GALAXY S10+ (SNAPDRAGON)
SAMSUNG GALAXY S10+ (EXYNOS)
SAMSUNG GALAXY NOTE 9 (SNAPDRAGON)
XIAOMI MI 9
ONEPLUS 6T
HUAWEI MATE 20 PRO
HUAWEI MATE 20 X
GOOGLE PIXEL 3
GOOGLE PIXEL 3 XL
NOKIA 7 PLUS
RAZER PHONE 2