RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

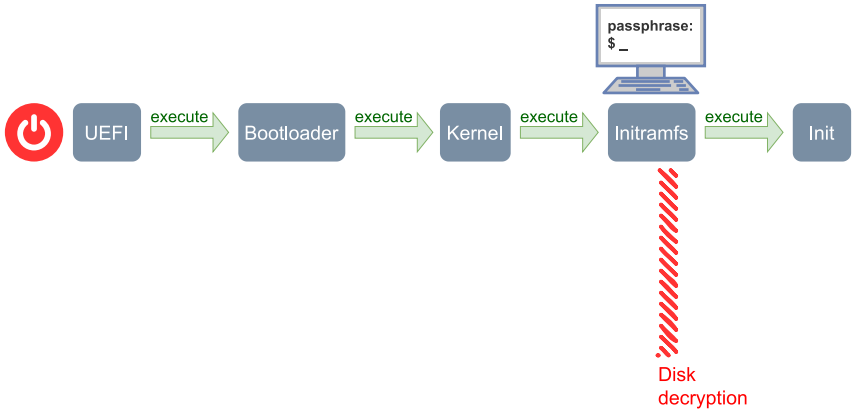
Ultrablue

Attestation distante sur Bluetooth

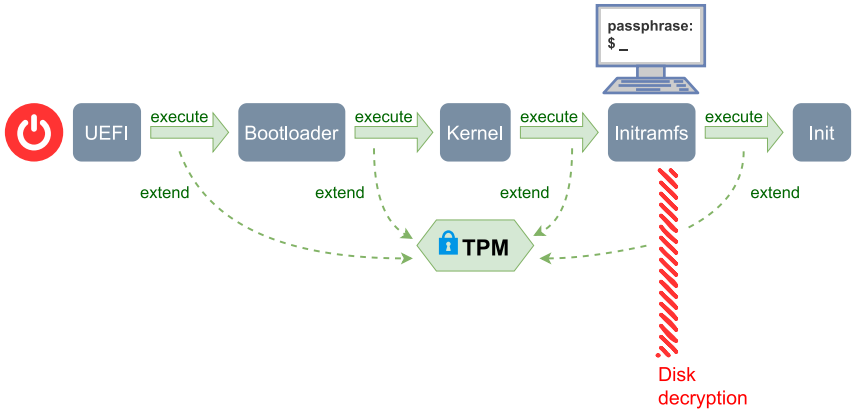
Gabriel Kerneis, Loïc Buckwell, Nicolas Bouchinet
Agence nationale de la sécurité des systèmes d'information

Scénario d'attaque

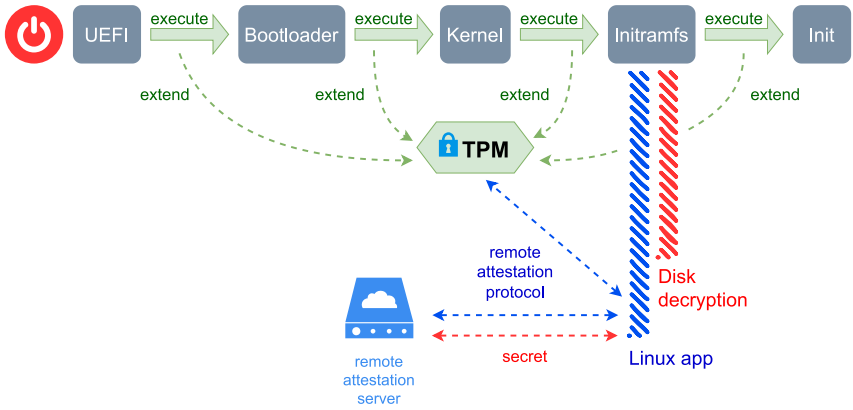
Chaîne de démarrage



Chaîne de démarrage avec TPM



Chaîne de démarrage avec TPM et attestation distante



Problématique

- Nécessitée de monter un serveur d'attestation distante.
- Avoir la capacité de communiquer avec ce serveur.
- Complexité d'administration de l'ensemble.

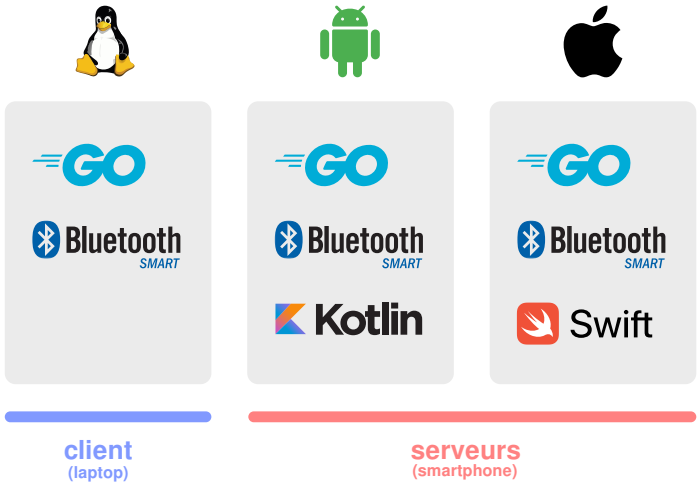
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Ultrablue – User-friendly lightweight TPM remote attestation over Bluetooth

Ultrablue

- Permet une communication en champ proche.
- Plus facile de garder un téléphone avec soit.
- Modèle de sécurité des téléphone relativement résistant par défaut.

La stack Ultrablue



Ultrablue est simple à mettre en place

- S'intègre aux mécanismes de chiffrement de disque existants.
- Exécutable au démarrage ou à n'importe quel instant du flux d'exécution.
- Facile à essayer... avant de l'adopter.

Démo

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Feuille de route

- Amélioration de l'UI de l'application Android.
- Proposer différents protocoles de communication (USB, IP, . . .).
- Authentification mutuelle des deux appareils.
- Envoi des rapports Ultrablue à un serveur de log.
- Implémentation d'un client Windows.
- Vérification d'intégrité à l'exécution avec IMA/EVM ?

https://github.com/ANSSI-FR/ultrablue

Bibliographie

- TPM based attestation - how can we use it for good ? (mjg59)
  https://www.youtube.com/watch?v=FobfM9S9xSI
- Starter pack cambrioleur Playmobil.
  https://www.playmobil.fr/starter-pack-policier-avec-cambrioleur-de-coffre-fort-/70908.html