Projet Icing

Projet Icing

Epitech Innovative Project (EIP)

Alexis Danlos **Ange Duhayon** **Bartosz Michalak** **Florian Griffon**

Stéphane Corbière

I

Contexte & Problématique

Réseau téléphonique = extrêmement faillible

Numéro de téléphone (**messagerie / appel** / sms) = **considéré** comme source d'***authentification fiable***

Profils sensibles (journalistes, politiques, renseignements) :

utilisent des solutions **tierses** (Signal, WhatsApp, etc)

= Internet

I

Comment garantir *sécurité* et *confidentialité* sur le réseau téléphonique *sans internet*, ni tiers?

II

Proposition Icing

II

Protocole Icing

Chiffrement de bout-en-bout sur échange d’audio

Hors-ligne

Protocole ouvert

Cryptographie a courbes elliptiques (P-256)

Multi-support

II *Utilité*

Protège contre:

- Écoute tierse
- Sim Swap (Usurpation physique)
- Usurpation logicielle
- Attaques de messagerie

Permet:

- Indépendance de services
- Adaptable aux lignes fixes / radios
- Utilisateur souverain

Pour:

- Industrie
- Journalistes
- Politiques
- Quidam
- Activistes

II *Proposition*

RFC *Protocole*

Handshakes

ECDH

Compression

Correction d’erreur

Pubkey share

Implémentation Kotlin (*lib*)

Implémentation du protocole dans une library Kotlin open-source, utilisable pour le développement Android

Implémentation Flutter (*dialer*)

Client téléphonique Android open-source
Implémentation de référence du protocole

Chiffrement automatique entre utilisateurs du protocole

II *Dialer*

Application

- Open Source & Libre
- Flutter
- Légèreté

Gestion de clé:

- Sauvegarde simple
- Gestion d’identités
- Stockage sécurisé
- Génération automatique

Partage de clé

- Partage / ajout de contacts par codes QR
- Procédure (protocolaire) d’échange de clé en appel

Appels normaux

- Totale transparence de l’appli
- Tentative de chiffrement par défaut

II

Démonstration

III

Perspectives

III *Objectifs*

Prototype fonctionnel

-

Première version de RFC

-

Politique de tests auto

III *Beta Test Plan*

III *Delivrables*

Merci
Kiitos
Suksma
Thanks