La sécurité et le respect de la vie privée dans les réseaux 5G

MobiS5

Appel : ANR-AAPG-2018

Année : 2018 (début, 2019)

Instrument : PRCE

Contact : maria-cristina.onete@unilim.fr

COORDINATEUR : Maria-Cristina ONETE (XLIM)

PARTENAIRES : Orange, IRISA, LIMOS, Eurecom

Résumé :

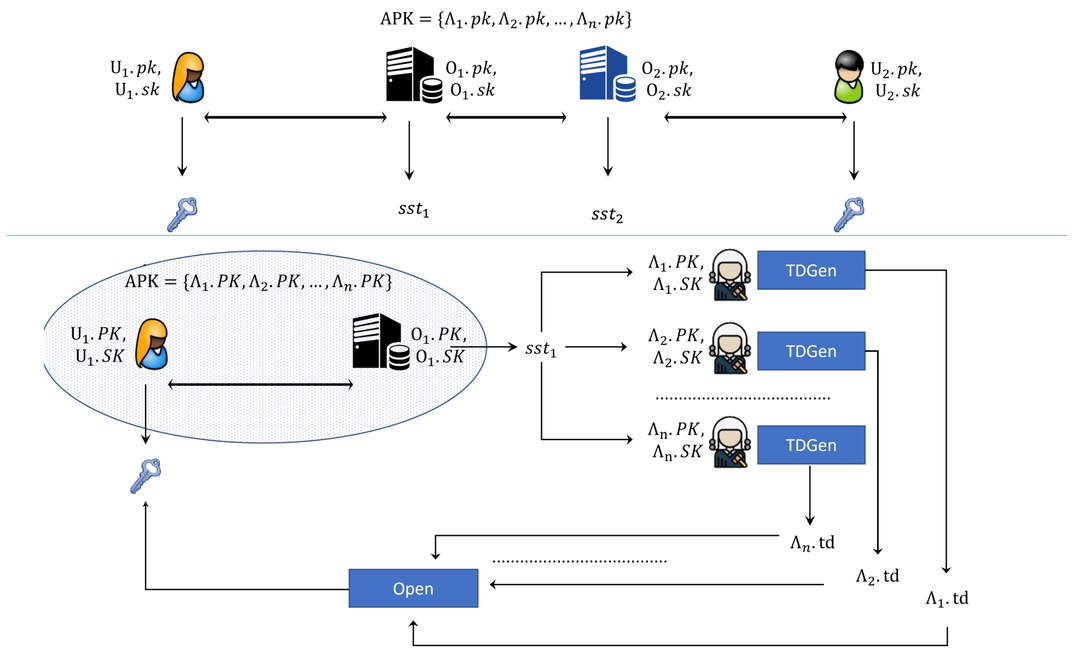
La transition vers la 5ème génération du réseau mobile modifie fondamentalement l'architecture 4G, affectant ainsi la sécurité de milliards d'utilisateurs, tout comme celle des opérateurs. Notre objectif : analyser la sécurité des protocoles 5G et fournir une boîte à outils cryptographiques pour les améliorer.

CONTEXTE ET OBJECTIFS

Le changement d'architecture induit par la 5G se traduit par une virtualisation des réseaux qui change radicalement le modèle de sécurité. En parallèle, les attentes vis-à-vis des protocoles de communication évoluent, mais doivent tenir compte des contraintes matérielles et réglementaires spécifiques aux réseaux mobiles.

MÉTHODOLOGIE ET RÉSULTATS

Quelques-uns de nos résultats marquants visent :



L'interception légale pour un échange de clé à deux parties [ESORICS2021]

- **Protocoles de communication sécurisés**

Le protocole de communication 5G est hérité des précédentes générations, mais souffre de la comparaison avec des protocoles plus modernes. Dans ce contexte nous avons identifié :

- Le besoin de formaliser et de répondre aux nouvelles exigences de sécurité pour les communications
- Le besoin de répondre à des obligations d'interception légale en limitant les conséquences pour la vie privée des utilisateurs.

- **Publications :**
  - ESORICS2021 (XLIM, Orange, IRISA) : L'interception légale avec un meilleur respect de la vie privée
  - SAC 2022 (XLIM) : L'interception légale avec deux systèmes d'interception légale (le cas roaming)
  - SAC2022 (XLIM, IRISA, LIMOS) : Une sécurité post-compromission optimale pour la messagerie asynchrone
  - CT-RSA2020 (Orange) : l'échange de clé symétrique garantissant la sécurité des sessions passées (PFS)
- **Brevets :**
  Brevet associé à la publication ESORICS2021

- **L'attestation dans des réseaux virtualisés**

La virtualisation entraine un changement fondamental au niveau du cœur du réseau, car désormais des fonctions réseau sensibles ne sont plus rattachées à un seul périphérique. Dans ce contexte, nous avons identifié :

- Le besoin d'une formalisation des propriétés demandées dans cette architecture
- Le besoin d'outils cryptographiques qui peuvent assurer la sécurité et le respect de la vie privée dans ce contexte

- **Publications :**
  - ACNS2021 (XLIM, Orange, IRISA, LIMOS) : l'attestation en profondeur
  - PKC2020, PKC 2021 (Orange) : l'attestation anonyme
  - CT-RSA2021 (Orange) : révocation d'attestations anonymes
- **Brevets :**
  Brevets associés aux publications PKC2020, PKC2021
- **Standardisation :**
  Intégration de protocoles dans la norme ISO 20008-2

- **Autres résultats :**

D'autres résultats ont visé :

- les attaques par canal auxiliaire (IRISA, Eurecom),
- les protocoles de délégation de calcul (Orange),
- l'authentification légère (XLIM)