Performance des clés symétriques en réseau de télécommunication

[1]Rakotondramanana R. S. [2]Randriamitantsoa P. A.

Laboratoire de Recherche Télécommunication, d'Automatique, de Signal et d'Images (LR-TASI)

Equipe d'accueil Doctorale de Télécommunication, d'Automatique, de Signal et d'Images (EAD-TASI)

Ecole Doctorale en Sciences et Techniques de l'Ingénierie et de l'Innovation (ED-STII)

Université d'Antananarivo

BP 1500-Antananarivo 101- Madagascar

[1]radiarisainanasitraka@yahoo.fr, [2]rpauguste@gmail.com

Résumé :

Le réseau de télécommunication utilise des clés symétriques pour s'authentifier au réseau et pour chiffrer les données des utilisateurs. Dans cet article, nouveau réseau de télécommunication 646-06 a été exposée. Une téléphonne Samsung, un modem Huawei a pu s'authentifier au réseau quand la clé maitresse dans la carte U-SIM est sembable dans base de données de l'opérateur. Vu que la clé est statique ; des personnes malveillantes possédant la clé de la victime peut créer un faux réseau pour faire les attaques hommes du milieu tel que vol de données, vol d'identité …. Des critères d'évaluation pour la dynamicité de clé sera également analysée : la clé de proximité pour la robustesse contre les attaques par test d'incrémentation et de décrementation, probabilité de proximité pour la robustesse contre les attaques d'incrémentation et de decrémentation par rapport à la clé précédente, probabilité de bit changé pour la résistance contre les modifications des bits et probabilité de l'entropie pour la robustesse contre la répartition des bits.

Mots clés : 646-06 , 5G, clé, U-SIM, opérateur

Abstract :

The mobile network telecommunication uses the symmetric key for the authentication and ciphering of users' data. In this article, the new telecommunication network 646-06 will be exposed. The Samsung phone, the Huawei modem could authenticate to the network when the key at the U-SIM card and the key at the database is the same. Like the key is static, any hacker could create fake and malicious network to capture users and make Man In The Middle Attack : capture traffic,hijacking … The criteria of evaluation of dynamic key will be analyzed : probability of the extremity to make the key robust of attacks of increases and decreases, the probability of proximity make the key robust to the attack of the extremity and proximity compared to the last key, the probability of a bit changed to make the robust of the change of bits and the probability of entropy to make the key robust repartition of number the bits.

Keywords: 646-06, 5G, key, U-SIM, operator

1. Introduction

Le réseau de télécommunication évolue vers un réseau programmable utilisant des radiologiciels. Dans cet article, un réseau de télécommunication 646-06 sera déployé puis analysé en matière des sécurités de clés.

2. Réseau de Télécommunication 646-06

Un réseau de télécommunication est défini par son MCC (Mobile Country Code) pour sépcifier le code pays de l'opérateur dont 646 pour Madagascar et MNC(Mobile Network Code) pour specifier le code de l'opérateur [1-7].

Tableau 1 : *Tableau des opérateur à Madagascar*

MNC	Opérateur réseau
01	Airtel
02	Orange
04	Telma
05	Bip

Le réseau mobile 646-06 est réseau mobile créé à partir d'un ordinateur et d'un radiologiciel. Les radiologiciels sont formés par un FPGA(Field Programmable Gate Arrays) et un circuit RF(Radio Fréquence).

2.1 Réalisation du prototype

Notre projet consiste à réaliser un prototype et des expériences, afin d'évaluer l'architecture du réseau de la future 5G. Une plate-forme à petite échelle a été proposée, en utilisant un ordinateur, un émetteur/récepteur SDR (LimeSDR mini), OpenAirInterface, OpenDaylight et open vswitch. Cependant, on se concentre sur les défis de prototypage de l'implémentation de l'EPC SDN/NFV, ainsi que la tendance vers la virtualisation, afin de résoudre le problème de gestion des ressources en 5G et réduire les coûts de déploiement.

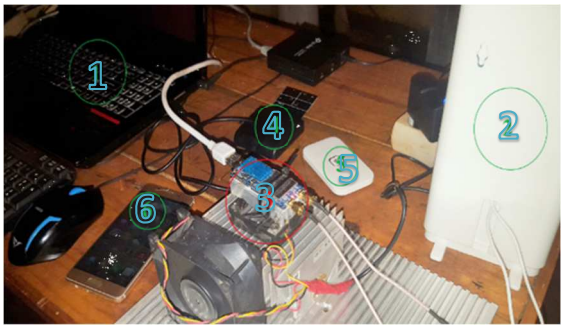

Figure 01 : *Environnement de travail*

Dans la figure 01, la représentation des matériels est la suivante :

- (1) : PC MSI GP 62 2QE Leopard Pro utilisé pour l'installation de EPC, eNodeB et le contrôleur SDN.
- (2) : Antenne Blazing Fast 4G LTE
- (3): LimeSDR mini avec un système de refroidissement
- (4) : Programmateur USIM
- (5) : Domino Huawei E5573B
- (6) : Téléphone Samsung S5

2.2 Architecture proposée

Notre architecture repose sur l'approche EPC SDN/NFV présentée par la figure 02.

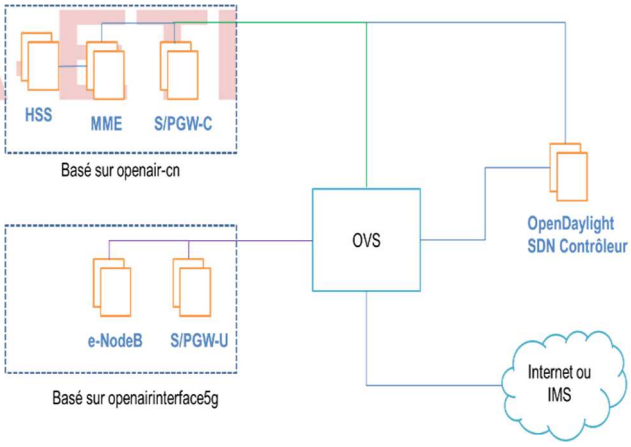

Figure 02 : *Architecture du prototype proposé.*

2.3 Description de l'architecture proposée

On a choisi l'architecture EPC SDN qui est compatible avec les spécifications 3GPP, et vise à évoluer l'architecture 4G actuelle vers l'intégration du SDN/NFV. Ainsi, cette architecture intègre un contrôleur SDN basé sur OpenDaylight (ODL) avec une API REST que nous avons développée pour supporter les procédures 3GPP. La figure 01 illustre l'architecture du réseau mobile avec EPC SDN. Par conséquent, il sépare le S / P-GW-C et le S / P-GW-U.

Pour le réseau LTE, nous avons utilisé le logiciel OpenAirInterface EPC (openairCN) [6]. OpenairCN est une implémentation open source des spécifications 3GPP de la CBE [6], c'est-à-dire qu'il inclut la mise en œuvre de l'entité de gestion de la mobilité (MME), Serveur de l'abonné hôte (HSS), la passerelle de service (S-GW) et la passerelle de donnée (P-GW). OpenairCN a été déployé sur Ubuntu 16.04 LTS avec la version 4.7 du noyau lowlatency. Les différents composants EPC ont été interconnectés via des interfaces virtuelles. Les deux premières interfaces facilitent la communication S11 entre la MME et le S-GW, tandis que le troisième prend en charge le GPRS Tunneling. Ainsi, la communication S1 entre EPC et E-UTRAN est réalisée par l'interface virtuelle de la machine physique.

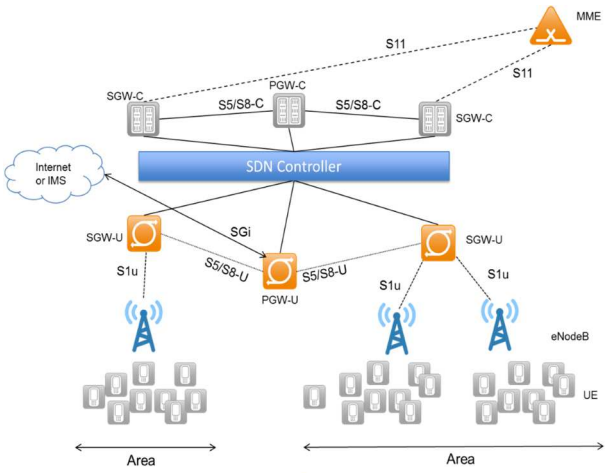

Figure 03 : *Architecture proposée du réseau mobile avec EPC SDN*

Le contrôleur ODL est déployé sur une machine virtuelle noté ODL-contrôleur et communique à la fois avec : le S / P-GW-C (par l'interface vmnet1) et S/P-GW-U (par l'interface vmnet1), OVS (par l'interface vmnet0) sur l'API REST via http.

Dans la figure 03, le S_PGW-U est connecté à plusieurs eNodeB à l'aide de l'interface S1-U. L'interface entre le contrôleur S_PGW-C et le contrôleur SDN est basé sur l'API REST. Le MME est connecté au P/SGW- C via l'interface S11, et le S_PGW-Cest connecté au PGW-C via interface S5 / S8-C (spécifié dans CUPS). Notez qu'un SGW-C peut gérer un ou plusieurs SGW-U (PGW-U). Par souci de simplicité, notre implémentation fusionne SGW et PGW en un seul élément, ce dernier étant divisé S_PGW-C et S_PGW-U pour intégrer SDN.

2.4 Tests de connectivité

Pour effectuer ces tests, nous avons utilisé le Samsung Galaxy S5, et le Huawei E5573B avec les différentes cartes SIM programmées. Notre réseau est 64606.

- Domino Huawei E5573B

Une fois les périphériques configurés, on réalise une recherche de tous les réseaux disponibles avec le domino dont la figure 05 le montre.

Figure 04 : *Domino E5573B connecté au réseau LTE 64606*

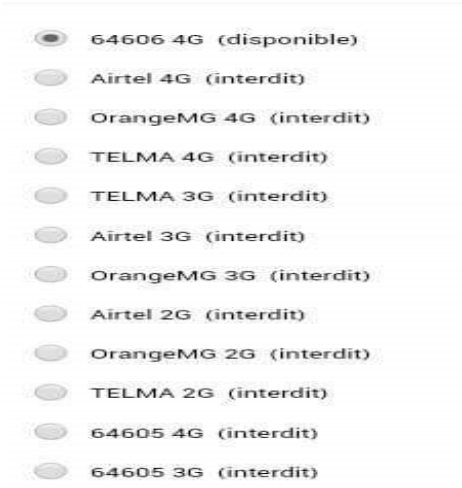

Figure 05 : Résultat de recherche

- Mobile Samsung Galaxy S5

De manière analogue, le mobile arrive à se connecter au réseau 64606.

Figure 06 : *Mobile connecté au réseau LTE 64606*

Le téléphonne Samsung possède un monitoring pour connaitre.

Figure 07 : *NetMonitoring Samsung S5*

2.5 Paramétrage de la clé de securité

L'opérateur et l'utilisateur utilisent une clé maitresse partagée identique. La sécurité de la clé réside alors sur le fait que les clés soient secrètes. Le secret signifie que l'opérateur à l'aide d'un programmateur enregistre la clé secrète dans la carte U-SIM et la même valeur de clé dans la table des bases de données de l'opérateur.

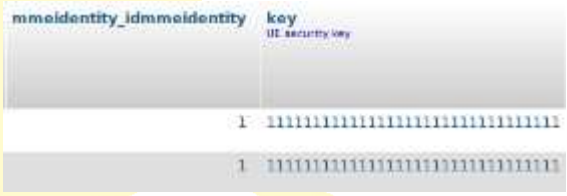

Figure 08 : *Extrait de clé dans la base de donnés de l'opérateur 646-06*

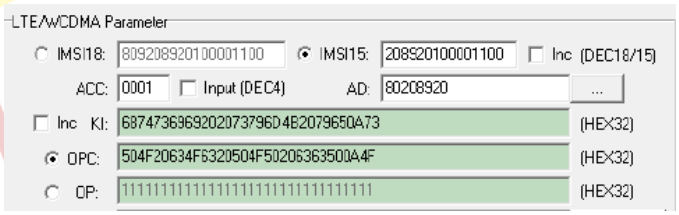

Figure 09 : *Extrait de clé lors de programmation de l'U-SIM*

4. Attaque homme du milieu en connaissance de la clé

La clé protégeant l'utilisateur est de 256 bits. Tester toutes les possibilités signifie à compter tous les éléments de l'univers tout entier.

D'autres méthodes peuvent être utilisées par une personne malveillante pour avoir la clé :

- Acheter la clé par une personne de l'intérieur ou un hacker expérimenté qui a pu avoir accès à la base de donnée de l'opérateur
- Acheter à l'opérateur comme l'affaire Snowdeen
- Utiliser des attaques physiques telles que : DPA (Differential Power Analysis) essayé de connaitre la clé en utilisant les dissipations des puissances. L'attaque physique évolue même aujourd'hui par l'utilisation d' un microscope Un hacker doit avoir la même clé que l'utilisateur pour que la victime connecte dans son réseau pirate. Le réseau mobile utilise une authentification mutuelle, càd l'opérateur et l'utilisateur utilise l'authenticité de l'un sur l'autre en utilisant la clé cachée nommée clé maitresse. Un hacker possédant la clé de l'utilisateur peut créer un réseau pirate près de la victime. De ce fait, le mobile s'y connecte automatiquement au faux réseau qui est au milieu. Le pirate peut connaitre toutes les données transitant au réseau : voler des mots de passe, injecter des virus aux victimes, manipuler les victimes … Une telle attaque s'appelle MITM ou homme du milieu.

5. Clé dynamique et critère de pérformance

- Probabilité d'extrémité :

L'attaque de force brute consiste à parcourir toutes les possibilités de manière aléatoire n'est pas rentable par rapport à la manière ordonnée. Selon la logique ainsi, un adversaire voulant tester toutes les clés possibles en utilisant l'algorithme de la brute force commence toujours par 00..000 jusqu'à 1111….1 en utilisant l'incrémentation ou en commençant par 111…..11 jusqu'à 0000…..0 en utilisant la décrémentation.

$$\underset{Incrémentation}{\begin{cases}00000\ldots\ldots\ldots000\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ 11111\ldots\ldots\ldots.111\end{cases}} \quad \underset{Décrementation}{\begin{cases}11111\ldots\ldots\ldots.111\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ 00000\ldots\ldots\ldots000\end{cases}} \qquad (1)$$

Plus la clé est proche de 0000….000 ou proche de 111….111, plus la probabilité de ne pas détecter la clé est faible.

Si la clé est proche de 0, le bit de valeur un des poids forts est difficile à détecter. De ce fait, la probabilité de ne pas détecter la clé si elle est proche de zéro est définie par :

$$p = \frac{\sum_{i=0}^{n-1}[k(i) == 1].2^i}{\sum_{i=0}^{n-1}.2^i} \qquad (2)$$

Si la clé est proche de 1, le bit de valeur zéro des poids forts est difficile à détecter. De ce fait, la probabilité de ne pas détecter la clé si elle est proche de bit un est définie par :

$$q = \frac{\sum_{i=0}^{n-1}[k(i) == 0].2^i}{\sum_{i=0}^{n-1}.2^i} \qquad (3)$$

En utilisant les deux approches, la probabilité pour que la clé soit proche de 0000…000 et de 1111….11 est formée par l'apparition de l'une de deux équations (2) et (3):

n étant la taille de la clé.

prob_extr étant la probabilité pour que clé k soit proche de l'extrême 0000…000 ou 1111…111

La fonction proche est donnée dans l'équation :

$$prob_{extr} = \begin{cases} p = \frac{\sum_{i=0}^{n-1}[k[i] == 1].2^i}{\sum_{i=0}^{n-1}.2^i} \; si \; proche(k, 0000\ldots000) \\ q = \frac{\sum_{i=0}^{n-1}[k[i] == 0].2^i}{\sum_{i=0}^{n-1}.2^i} \; si \; proche(k, 1111\ldots111) \\ proche(k) \begin{cases} proche(k, 0000\ldots000) = (k[n] == 0) \\ proche(k, 1111\ldots111) = (k[n] == 1) \end{cases} \end{cases}$$

- Probabilité de proximité :

La probabilité de proximité utilise deux clés : clé actuelle et clé suivante sont d'autant plus proches l'une sur l'autre. En imaginant deux clés spécifiques à comparer :

$$(k_1, k_2) = (0010{,}0100)$$

La distance entre les deux binaires étant la soustraction entre les deux clés :

$$xor(k_1, k_2) = 0110$$

Pour aller de $k_1 \rightarrow k_2$ sera équivalent à aller de $0000 \rightarrow xor(k_1, k_2)$
Pour aller de $k_2 \rightarrow k_1$ sera équivalent à aller de $1111 \rightarrow xor(k_1, k_2)$

$$prob\_prox = prob\_extr\big(xor(k_1, k_2)\big) \quad (4)$$

- Probabilité de bit changé :

En supposant deux $(k_1, k_2), si$ i le nombre de bits changé est très proche du nombre 0 de 256 alors la clé génèrée est facile à casser, la probabilité de bit changé est définie ainsi par :

$$prob_{change} = \begin{cases} \frac{\sum_{i=0}^{n-1} xor(k_1, k_2)[i]}{n} & si \ \frac{\sum_{i=0}^{n-1} xor(k_1, k_2)[i]}{n} \leq 0.5 \\ \left| 1 - \frac{\sum_{i=0}^{n-1} xor(k_1, k_2)[i]}{n} \right| & sinon \end{cases}$$

- Entropie : L'entropie de la clé suivante est définie par :

$$H = -p(0)log_2(p(0)) - p(1)log_2\big(p(1)\big) \quad (5)$$

3. Conclusion

Un réseau de télécommunication pirate peut être créé en possédant la clé maitresse de la victime. Le pirate peut faire une attaque de type homme du milieu pour faire un vol de données, injection de code mailvaillant dans le mobile de l'utilisateur. Des critères d'évaluation pour la dynamicité de clé sera également analysée : la clé de proximité pour la robustesse contre les attaques par test d'incrémentation et de décrémentation, probabilité de proximité pour la robustesse contre les attaques d'incrémentation et de décrémentation par rapport à la clé précédente, probabilité de bit changé pour la résistance contre les modifications des bits et probabilité de l'entropie pour la robustesse contre la répartition des bits. En faisant le calcul, la probabilité d'extrémité, de l'entropie sera aléatoire et dépendant de la clé statique tandisque la probabilité d'extrémité, la probabilité de proximité et la probabilité de bit changé seront de 0% pour une clé statique.

4. Références

[1] N. Panwar, S. Sharma, et A. K. Singh, « *A survey on 5g: The next generation of mobile communication* », Physical Communication, 2015.

[2] C. Chen, « *C-ran: the road towards green radio access network* », http://labs.chinamobile.com/cran/wpcontent/uploads/CRAN, white paper v2 5 EN.pdf, Janvier 2019.

[3] E. Hernandez-Valencia, S. Izzo, et B. Polonsky, « *How will nfv/sdn transform service provider opex?* », Network, IEEE, vol. 29, no. 3, pp. 60–67, 2015.

[4] I. Giannoulakis, E. Kafetzakis, « *On the applications of efficient nfv management towards 5g networking* »,5GU, 2014 1st International Conference on, pp. 1–5, IEEE, 2014.

[5] J. Markendahl, O. Akitalo, « *A comparative study of deployment ¨ options, capacity and cost structure for macrocellular and femtocell networks* », Personal, Indoor and Mobile Radio Communications Workshops (PIMRC Workshops), 2010 IEEE 21st International Symposium on, pp. 145–150, IEEE, 2015.

[6] OAI, « openairinterface5G », https://gitlab.eurecom.fr/oai/openairinterface5g, Janvier 201

[7] Andriamiaranarivo M., Randriamitantsoa P.A, Randriamitantsoa A.A., *« Contribution à l'implémentation SDN/NFV pour le réseau mobile 5G»,* Article n.7, Vol.1, 2019