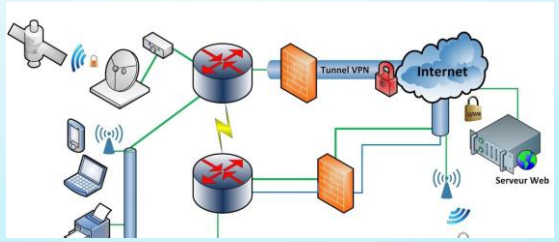

Brazzaville, 25 Mai 2022

Evolution des Technologies/architectures et problématiques de sécurité sur les réseaux mobiles

Présentation: Benjamin MOUANDZA

Directeur des Réseaux et Services des Communications Electroniques (ARPCE)

PLAN

1 - Quelques dispositions réglementaires

2 –Evolution des Technologies et problématique de sécurité les réseaux mobiles

3 – Vulnérabilité des techniques d'authentification et cryptage

4 – Approches de solution

DISPOSITIONS REGLEMENTAIRES

Loi n°9-2009 du 25 novembre 2009 portant règlementation du secteur des communications électroniques	Loi n" 30 - 2019 portant création de l'Agence nationale de sécurité des systèmes d'information
Article 124 :. tout fournisseur d'un service de communications électroniques accessible au public prend les mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité de ses services,… Article 146 : La fourniture, l'importation d'un moyen de cryptologie n'assurant pas exclusivement des moyens d'authentification ou de contrôle sont soumis à une déclaration auprès de l'agence de régulation.	Article 3 : L'agence nationale de sécurité des systèmes d'information est chargée notamment, de : - réduire la vulnérabilité du cyberespace national - gérer les incidents de sécurité, des systèmes d'information ; - suivre l'exécution des plans et des programmes relatifs de la sécurité informatique et assurer la coordination entre les intervenants dans ce domaine, - procéder aux contrôles réguliers des réseaux et systèmes d'information
Article 130 : Pour les besoins de défense et de sécurité, de lutte contre la pédophilie et le terrorisme, les exploitants des réseaux des communications électroniques ouverts au public ou leurs représentants sont tenus, au moment de la souscription au service de téléphonie, de procéder à l'identification des abonnés.	Contribuer à l'élaboration des normes spécifiques de la sécurité des systèmes d'information ; Veiller au respect des dispositions légales et réglementaires relatives à la sécurité. des systèmes d'information et des réseaux de communications électroniques;

APPROCHE DE SECURITE ET LUTTE ANTI FRAUDE

La loi donne à l'ANSSI, **de veiller au respect des dispositions légales et réglementaires relatives à la sécurité des systèmes d'information et des réseaux de communications électroniques;**

L'ARPCE a l'avantage d'être informée sur tout changement qui s'opère sur le réseau , mais n'intervient pas directement sur la politique de cyber sécurité des opérateurs.

L'approche utilisée par l'ARPCE pour lutter contre les phénomènes de fraude et de hacking est pénale: Identification de la SIM, historique des appels et poursuite .

Sécurité des Réseaux mobiles–Evolution en fonction des architectures

Sécurité sur le GSM

- La sécurité sur les RX mobiles comme sur les réseaux informatiques repose essentiellement sur l'authentification pour accéder au réseau et chiffrement du contenu pour assurer la discrétion et l'intégrité des échanges sur ces Rx. Evoluant vers les réseaux mobiles haut débit, connectés sur internet, la sécurité des RX mobiles devient un problème de cybersécurité.
- En décembre 1999 lorsque le Congo a vu naitre son premier réseau GSM, le protocole utilisé pour sécuriser le réseau était déjà vulnérable, car il était cassé deux ans auparavant.

Vulnérabilité de la sécurité sur le GSM

- **Vulnérabilité du COMP 128 :**
- Les stations pirates appelée IMSI catcher se faisaient passer pour la BTS et récupéraient toutes les infos échangées entre le mobile et le réseau , brisant ainsi la discrétion des échanges entre le mobile et la BTS.
- **Authentification sur le GPRS**
- Dans les année 2003 apparait le GPRS/EDGE, pour qui le cryptage devait être fait non pas par la BTS mais par le SGSN.

Sécurité sur le réseau 3G

- Au lancement du réseau 3G en Octobre 2011 par Airtel , le problème de vulnérabilité causé par les Sim catcher était résolu à l'aide d'un nouveau protocole AKA, basé sur l'authentification bilatérale. Le chiffrement et le déchiffrement s'effectuait au niveau du RNC (*Radio Network Controller*)
- Le protocole AKA a mis fin au IMSI Catcher ou man in the middle, et a été amélioré pour être utilisé sur les réseaux 4G et 5G.

Vulnérabilité du protocole AKA

- Le problème des Sim catcher apparemment résolu, mais vu que les MNOs utilisent toutes les couches 2G/3G/4G et voir 5G, les IMSI-catcher reviennent avec une méthode qui force le mobile à se connecter en 2G, et accèdent aux données du MS.
- Pour remédier google et certains fabricant ont ajouté une option permettant de désactiver la connectivité 2G non sécurisée sur les smartphones.
- Autre révélation, les chercheurs allemands, ont montré la vulnérabilité de la protection en 5G, qui était censé être imparable. Ils ont conçu un appareil qui déchiffre les derniers bits du numéro de séquence exploité par le protocole AKA. Avec cette technique et ces seuls derniers bits, les chercheurs pouvaient identifier l'identité de l'abonné et relever les métadonnées de l'activité du mobile.

Une nouvelle sim GEMALTO pour la 5G est donneuse d’espoir

- Une nouvelle sim GEMALTO pour la 5G est donneuse d’espoir en matière de sécurité. Elle permet aux opérateurs mobiles d’échanger à la demande - en toute sécurité et à distance - l'algorithme d'authentification contenu dans la SIM grâce à la gestion des clés par rotation

AUTRES CAS DE PIRATAGE INDUITS PAR LA CONNEXION A INTERNET

- **Les RX IMT** connectés sur internet font appel à multiples hackers, si bien que certains programmes qui était utilisés sur les réseaux informatiques, pour détourner les données des cartes bancaires comme des malware, et le protocole de communication SSH sur les serveurs Proxy arrive a contourner les plateformes de billing pour consommer gratuitement le data. Les hackers profitent des failles pour accéder au serveur web d'un opérateur.
- **Piratage et problème d'intégrité:** les simboxe Qui injecte dans les réseaux locaux le trafic issu de l'international, le faire passant pour un trafic local.

La carte Sim un atout incontournable de sécurité :

Le danger que courent les Rx mobiles de nouvelle génération est celui de faire perdre à la carte sim son identité. Les réseaux 4G, 5G n'utilisent la sim plus que pour l'authentification. Les communications se font sur les adresses IP et l'IMSI perd son identité. Ce qui est très grave. Certaines applications comme Textnow et google voice permettre de creér un compte **WhatsApp sans carte SIM**.

La sim avec l'IMSI sont un atout important parce que derrière il y'a une identité. On voit même que pour s'authentifier sur certaines applications, sensibles, ou pour refaire un mot de passe oublié, le système vous envoie un code par sms sur votre mobile, parce que derrière le mobile il y'a le propriétaire et son identité.. Cet atout est en pleine perdition et en même temps des réseaux IP, qui échappent au contrôle à cause de l'usage répandu des adresses dynamique, je veux proposer l'usage des sims avec IP V6 fixe pour tout type de « device » (routeur, objet connecté, modem et pourquoi pas

CONCLUSIONS ET APPROCHES DE SOLUTION

- Comment protéger les réseaux de nouvelles génération qui ne font plus que un avec le Web, duquel ils sont très dépendant mais le contrecoup à payer reste la sécurité. ?
- On ne peut assurer la sécurité des RX IMT qui deviennent tout IP qu'avec le levier authentification et cryptage. Il faut donner les bons moyens au pénal pour dissuader les fraudeurs/hacker.
- D'où la nécessiter d'opter pour une sim avec adresse IP fixe (IP V6) utilisable sur tous les devices connectés au Rx.


MERCI