VoLTE : risques d'espionnage et usurpation d'identité

Alors que la VoLTE (voix sur LTE) apporte son lot d'innovations (meilleure qualité de voix, latence réduite à presque rien, visio-communication, usage simultané d'autres applications sur le smartphone…), elle charrie aussi de nouvelles vulnérabilités. Lesquelles permettent à la fois d'attaquer les utilisateurs d'un smartphone Android mais aussi les infrastructures des opérateurs.

C'est du moins ce qu'avance une équipe de chercheurs de la société française de sécurité P1 Security à l'occasion du SSTIC (Symposium sur la sécurité des technologies de l'information et des communications) qui se déroule à Rennes du 7 au 9 juin. *« Certaines de ces vulnérabilités sont nouvelles et jamais divulguées jusqu'à présent : elles peuvent permettre à un attaquant de récupérer discrètement des informations privées sur les abonnés ciblés, tels que leur géolocalisation »*, soulignent Patrick Ventuzelo, Olivier Lemoal et Thomas Coudray dans leur rapport. Aussi technique que détaillé, ce dernier prend soin de décortiquer les mécanismes de la voix en 4G pour mieux démontrer ses faiblesses qui l'exposent à de potentielles écoutes indiscrètes. Et même à de l'usurpation d'appel.

La VoLTE, une technologie simplifiée

Il faut savoir que la voix sur 4G est une technologie volontairement simplifiée afin que de la rendre accessible à de non-experts télécoms. *« L'héritage de la VoIP et du protocole SIP basé sur le texte créent de nouvelles surfaces d'attaque qui rendent les réseaux des opérateurs plus accessible et exposés qu'avec les réseaux historiques (2G et 3G, NDLR) »*, font remarquer les auteurs. Du coup, comme souvent, la sécurité du réseau dépend de la configuration de ses différents éléments.

Le problème viendrait de la façon dont est implémentée la VoLTE sur Android. Laquelle s'appuie sur une interface générée par le pilote Ehternet virtuel RMNET. L'interface apparaît généralement sous le nom rmnet1 sur le téléphone et elle est utilisée pour le transfert des données utilisateur sur le réseau mobile. Aucune norme n'a été définie pour gérer cette interface. Du coup, la qualité de son implémentation dépend du bon vouloir de chaque constructeur. Par exemple, selon P1 Security, un Samsung Galaxy S6 permet facilement, en utilisant un outil de débogage, d'espionner l'interface rmnet1 afin d'accéder à la communication et aux contenus qui y transitent ainsi qu'aux critères de sécurité associés (IPsec Security Associations) accessible sur le Netkey (la pile IPsec du noyau Linux). En revanche, le rmnet1 d'un Xperia de Sony ne laisse fuiter aucun trafic depuis ou vers le terminal et l'IPsec Security Associations reste invisible du noyau.

Aspirer et injecter des données

Il en résulte que les chercheurs ont réussi à exploiter cette faille pour aspirer du trafic SIP et injecter des données entre le terminal et le réseau mobile même lorsque les opérateurs utilisent des mécanismes d'authentification et de chiffrement IPsec. Une brèche qui ouvre la porte aux appels gratuits en contournant le système de facturation de l'opérateur. Ou encore pour contourner les écoutes légales mise en place par les autorités judiciaires, estime les experts en

sécurité. Des risques d'usurpation d'utilisateurs ne sont pas non plus à exclure alors qu'un attaquant pourrait manipuler l'entête d'une requête SIP. Pas plus que la possibilité pour un attaquant de dresser la carte du réseau d'un opérateur.

Bref, le danger est réel de voir des attaquants exploiter les vulnérabilités de la VoLTE pour dérober des informations et contourner des usages. D'autant qu'une carte SIM VoLTE et un smartphone Android rooté (accès aux droits d'administration) suffisent pour lancer des attaques, insistent les chercheurs. Adopté à partir de 2012, la VoLTE est aujourd'hui supportée par 104 opérateurs dans 55 pays. Et son adoption se poursuit un peu partout dans le monde offrant des surfaces d'attaques toujours plus grandes aux cyber-criminels. *« P1 Security espère que cet article et les discussions connexes vont à aider les opérateurs et les fournisseurs à mieux comprendre ces risques et contrer efficacement les attaques de faible complexité auxquelles ils seront confrontés dans les années à venir »*, concluent les experts.

Lire également
2 milliards de connexions VoLTE en 2020
MWC 2016 : Orange tire tous azimuts IoT, VoLTE, SDN, 5G…
La VoLTE fait ses premiers pas en France chez Bouygues Telecom

crédit photo © Theera Disayarat – Shutterstock