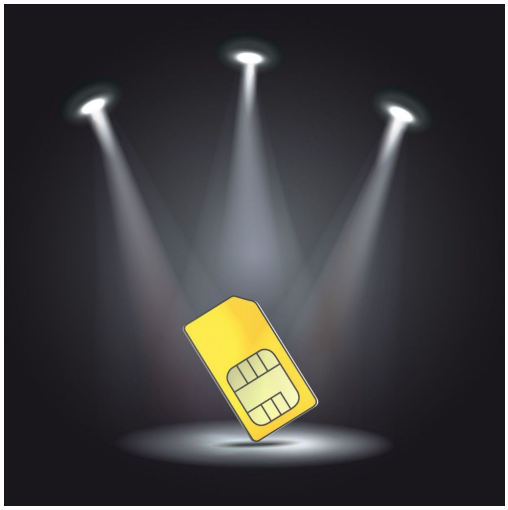
L’évolution De La Carte SIM

	L’évolution De La Carte SIM

Une carte SIM, ou Suscriber Identity Module en anglais (module d'identification de l'abonné), est un élément familier d'un téléphone portable. Elle peut facilement être échangée ou remplacée, mais elle n'est néanmoins pas née en même temps que le téléphone portable. Les premiers téléphones portables ne permettaient que des normes de communication « intégrées » : les paramètres de souscription étaient codés en dur dans la mémoire du terminal mobile.

Les normes analogues les plus anciennes comme NMT-450 n'utilisaient aucune sécurité : les données d'abonnement pouvaient être copiées sur un autre appareil et clonées, ce qui permettait d'appeler et d'accepter des appels au nom du propriétaire légitime sans payer.

Le premier dispositif de sécurité, inventé un peu plus tard, fut le code SIS, Suscriber Identity Security en anglais (sécurité de l'identité de l'abonné) : il s'agissait d'un nombre à 18 chiffres unique à chaque appareil et codé en dur dans un processeur d'application. Les codes SIS étaient répartis entre les fournisseurs de manière à ce que deux appareils ne puissent pas partager le même code SIS. Le processeur comportait également un code RID de 7 chiffres qui était transmis à une station de base lorsqu'un abonné s'inscrivait dans un réseau mobile.

La station de base générait un nombre aléatoire que le processeur SIS utilisait couplé avec une réponse SIS unique pour produire la clé d'autorisation.

Les clés et les nombres étaient relativement courts, mais appropriés pour l'année 1994 ; de façon assez prévisible, le système a été décrypté plus tard, tout juste trois ans avant l'apparition de la norme GSM, Global System for Mobile en anglais (Communications – Système global pour les communications mobiles). Il était conçu de manière plus sûre étant donné qu'il utilisait un système d'autorisation similaire, mais au chiffrement plus résistant. Ainsi, la norme est devenue « détachée » .

Cela signifie que l'autorisation dans sa totalité avait lieu sur un processeur externe intégré dans une carte intelligente. La solution a été appelée SIM. Avec l'introduction des cartes SIM, l'abonnement ne dépendait plus l'appareil et l'utilisateur pouvait changer d'appareil aussi fréquemment qu'il le désirait tout en gardant son identité mobile.

Fondamentalement, une carte SIM est une carte intelligente selon la norme ISO 7816, qui ne présente pas de différence significative par rapport à d'autres cartes intelligentes de contact comme les cartes de crédit ou les cartes téléphoniques. Les premières cartes SIM faisaient même la taille d'une carte de crédit, mais la tendance globale de réduction des dimensions a mené à une nouvelle forme plus compacte.

Les cartes SIM traditionnelles 1FF (1st Form Factor) de taille complète ne rentraient plus dans les téléphones, et l'industrie a donc trouvé une solution de compatibilité simple : une carte SIM plus petite (mini-SIM, 2FF ou 2nd Form Factor) qui est commune pour les utilisateurs modernes, a été placée dans un support en plastique de taille 1FF afin que la nouvelle forme de carte comporte la puce et les contacts, mais avec une empreinte plus petite, et puisse facilement être sortie.

Bien que cette tendance à la réduction continue avec la micro-SIM (3FF) puis la nano-SIM (4FF) , la forme et les contacts ainsi que les fonctionnalités de ces puces intégrées n'ont pas changé depuis presque 25 ans. De nos jours, de grands supports en plastique sont produits pour répondre aux besoins des utilisateurs qui préfèrent encore des combinés à l'ancienne.

Ceci dit, de nombreux appareils obsolètes ne supporteraient pas les cartes SIM actuelles, même dans leur version complète. Cela vient du fait que la tension de fonctionnement était de 5 V dans les anciennes cartes SIM alors que les actuelles exigent 3 V. De nombreux fabricants de SIM préfèrent sacrifier la compatibilité pour réduire les coûts, et la majorité des cartes SIM modernes ne supporteraient donc pas deux tensions. C'est pour cela que dans un ancien téléphone uniquement compatible avec 5 V, les cartes SIM de seulement 3V ne fonctionneraient même pas à cause de la protection de la tension de leur processeur.

Lors de la production, certaines informations sont écrites dans la mémoire d'une carte SIM : l'IMSI (International Mobile Suscriber Identity, Identité de l'abonné mobile international), en accord avec le porteur ayant commandé la carté, ainsi qu'une clé de 128 bits nommée Ki (Key Identification, identification de clé). Pour résumer simplement, on peut dire que l'IMSI et le Ki sont le l'identifiant et le mot de passe respectifs de l'abonné codés en dur dans la puce de la carte SIM.

La correspondance entre l'IMSI d'un abonné et son numéro de téléphone est stockée dans une base de données spéciale appelée HLR (Home Location Register). Ces données sont copiées sur une autre base de données, VLR (Visitor Location Register) dans chaque segment du réseau, sur la base de l'enregistrement temporaire de l'abonné en tant qu' « invité » sur une autre station de base.

Le processus d'autorisation est relativement simple. Lorsqu'un abonné est inscrit dans la base de données temporaire, VLR envoie un numéro de 128 bits aléatoire (RAND) au numéro de téléphone. Le processeur de la carte SIM utilise l'algorithme A3 pour créer une réponse de 32 bits (SRES) au VLR basé sur le numéro RAND et le Ki. Si VLR obtient une réponse qui correspond, l'abonné est inscrit dans le réseau.

La SIM crée également une autre clé temporaire appelée Kc. Sa valeur est calculée sur la base du RAND et du Ki mentionnés ci-dessus, à l'aide de l'algorithme A8. Cette clé est ensuite utilisée à son tour pour chiffrer des données transmises par l'algorithme A5.

Les noms de tous ces acronymes peuvent paraître un peu compliqués, mais l'idée de base est très simple : vous avez tout d'abord un identifiant et un mot de passe codés en dur dans la SIM, puis vous créez des clés de vérification et de chiffrement avec quelques trucs mathématiques et ça y est : vous êtes connecté !

Ce chiffrement est toujours activé par défaut, mais dans certaines circonstances (par exemple si un mandat est fourni), il peut être désactivé, ce qui permet qu'une agence de renseignement puisse intercepter les conversations par téléphone. Dans ce cas, les anciens dispositifs affichaient un cadenas ouvert, alors que les téléphones modernes (à part Blackberry) n'affichent aucune indication de ce type.

Il existe une attaque spécifiquement conçue pour intercepter les conversations téléphoniques ; pour la réaliser, l'adversaire a seulement besoin d'un appareil appelé IMSI Catcher qui imite une station de base et enregistre les téléphones qui se connectent avant d'envoyer tous les signaux vers une station de base réelle.

Dans ce cas, tout le processus d'autorisation se déroule de façon normale (il n'est pas nécessaire de décrypter les clés de chiffrement), mais la fausse station de base ordonne au dispositif de les transmettre sous forme de texte brut afin qu'un adversaire puisse intercepter les signaux sans que la compagnie ou l'abonné ne le sachent.

Cela peut paraître étrange, mais cette vulnérabilité n'en est pas vraiment une : en fait, cette fonctionnalité a été conçue pour faire partie du système depuis le début, afin que les services de renseignements puissent réaliser des attaques intermédiaires dans les cas appropriés… [Lire la suite]

Réagissez à cet article

Source : *L'évolution De La Carte SIM – Kaspersky Daily – | Nous Utilisons Les Mots Pour Sauver Le Monde | Le Blog Officiel De Kaspersky Lab En Français.*