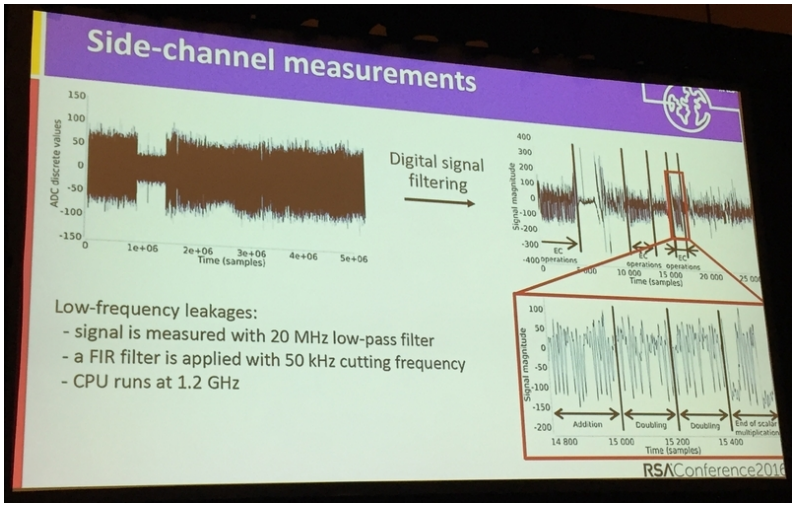
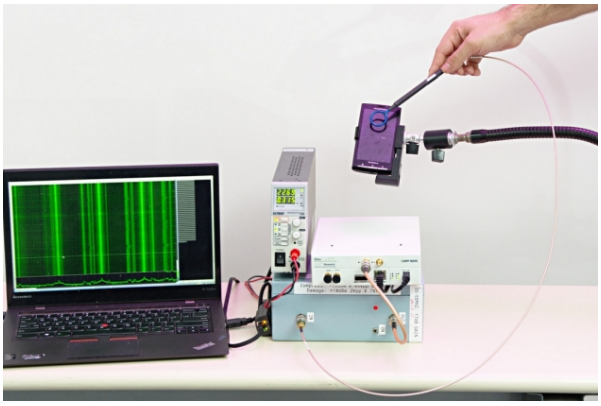
Piratages des smartphones iOS ou Android possibles à cause de leurs fuites électromagnétiques

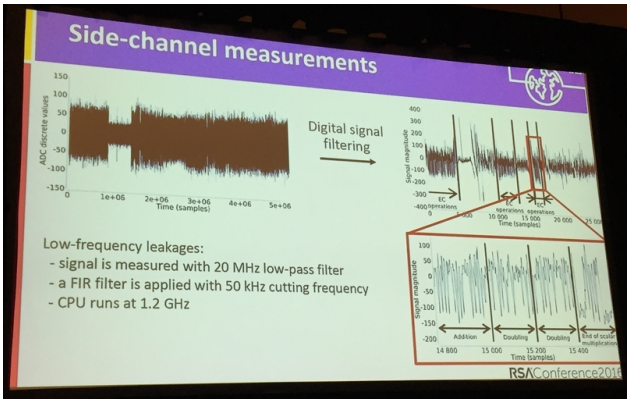


Piratages des smartphones iOS ou Android possibles à cause de leurs fuites électromagnétiques

Des chercheurs arrivent à extraire des clés de chiffrement privées en captant les signaux involontaires des circuits imprimés. Parmi les applications vulnérables figurent OpenSSL et les porte-monnaie Bitcoin.



Les smartphones d'aujourd'hui embarquent de plus en plus procédés cryptographiques pour sécuriser tout un tas d'échanges et de transactions. L'équipement matériel, toutefois, n'est pas forcément à la hauteur des enjeux. Deux équipes de chercheurs viennent de présenter concomitamment des attaques non invasives qui s'appuient sur les émanations électromagnétiques des terminaux mobiles pour récupérer des clés privées de signatures électroniques. Elles permettraient, par exemple, de pirater des porte-monnaie Bitcoin, des transactions Apple Pay ou des connexions sécurisées par OpenSSL.
La première équipe est française et regroupe quatre chercheurs issus d'Orange Labs, HP Labs, NTT et l'université de Rennes. Le 3 mars, à l'occasion de la conférence RSA 2016, ils ont montré comment extraire d'un téléphone Android des clés privées basées sur les algorithmes de courbes elliptiques (Elliptic Curve Digital Signature Algorithm, ECDSA). Leur étude se limite à une librairie cryptographique spécifique, à savoir Bouncy Castle 1.5. Quand celle-ci réalise les calculs mathématiques liés à la signature d'un message, les circuits intégrés du téléphone émettent des ondes électromagnétiques à basse fréquence (50 kHz).



Le traitement du signal révèle les opérations mathématiques (« addition », « doubling »)

Les chercheurs captent ce signal au moyen d'une antenne appliquée sur le téléphone et arrivent, par traitement de signal, à reconnaitre les différentes opérations de ce calcul. Cette information est suffisante pour récupérer in fine la clé secrète. La librairie vulnérable a, depuis, été modifiée de telle manière que l'on ne puisse plus reconnaitre les opérations (version 1.51). Néanmoins, une attaque concrète aurait pu être, selon les chercheurs, de cibler les porte-monnaie Bitcoin car ils s'appuient sur Bouncing Castel.
Ainsi, un attaquant aurait pu piéger le lecteur NFC d'un commerce qui accepte les Bitcoins et, ainsi, récupérer les adresses Bitcoin des clients. Ce qui lui permettait alors d'en disposer comme bon lui semble. « On pourrait également imaginer des attaques à plus longue distance, à condition de disposer d'un équipement de captation suffisamment puissant, comme peuvent en avoir les agences gouvernementales », nous explique Mehdi Tibouchi, l'un des quatre chercheurs français, à l'issue de leur présentation.

Des attaques low-cost
La seconde équipe qui a planché sur ce type d'attaques est israélienne et regroupe cinq chercheurs issus de l'université de Tel Aviv et de l'université d'Adelaide (Australie). Leur attaque cible également les signatures basées sur les courbes elliptiques ECDSA, mais son domaine d'application est nettement plus large.
Ainsi, ces chercheurs ont réussi à extraire des clés privées sur les librairies OpenSSL et CoreBitcoin sur iOS, qui sont toujours vulnérables à l'heure actuelle. Ils ont également réussi des extractions partielles de clés privées avec la librairie CommonCrypto d'iOS et la version Android d'OpenSSL. Toutefois, CommonCrypto – qui est notamment utilisé par Apple Pay – n'est pas vulnérable au-delà de la version iOS 9 car Apple a intégré des « mécanismes de défense » contre ce type d'attaques.
Selon les chercheurs israéliens, les fuites de signaux peuvent être captées de façon électromagnétique par une petite antenne, ou de manière électrique par une petite résistance intégrée au niveau du câble de chargement USB (prix : quelques dollars). Dans les deux cas, le signal est envoyé dans l'entrée d'une carte son Creative Track Pre Sound, ce qui permet de le numériser et de l'amplifier (prix : 50 dollars). Au final, la mise en œuvre de l'attaque est donc de faible coût. Les chercheurs ont réalisé leurs tests avec un iPhone 3GS et un Sony-Ericsson Xperia x10 … [Lire la suite]

Réagissez à cet article

Source : *On peut pirater les smartphones iOS ou Android à cause de leurs fuites électromagnétiques*