Comment pirater un code PIN avec une montre connectée

Exploiter une smartwatch pour pirater un code PIN. Tel est en substance l'objet du travail de recherche de Tony Beltramelli, développeur et étudiant français qui officie à l'université de Copenhague, au Danemark, dans le cadre de sa thèse. Le chercheur a souhaité attirer l'attention sur les risques de sécurité qu'induit l'exploitation des données générées par les capteurs de mouvement. *« Par leur nature portable, ces dispositifs (montres connectées et traqueurs d'activité, NDLR) fournissent toutefois une nouvelle surface d'attaque omniprésente menaçant la vie privée des utilisateurs, entre autres »*, écrit le scientifique dans son introduction.

Pour soutenir sa démonstration, Tony Beltramelli s'appuie sur la puissance de l'intelligence artificielle *« qui fournit des possibilités sans précédent pour traiter efficacement des données complexes »*. L'idée étant donc d'utiliser le machine learning pour déterminer la saisie d'un code chiffré par «simple» analyse des mouvements du poignet de l'utilisateur.

Le machine learning au service du piratage

A cette fin, le chercheur a développé le RNN-LSTM (Recurrent Neural Network – Long Short-Term Memory), un algorithme de deep learning pour «apprendre» des saisies effectuées sur un clavier à 12 touches typique de ceux des distributeurs de billets (DAB) mais aussi des écrans de connexion des smartphones. Développé en Java, Python et Lua, l'algorithme d'apprentissage a été associé à une application (en l'occurrence exploitée sur une SmartWatch 3 de Sony) qui utilise les capteurs du gyroscope et de l'accéléromètre. Les données étaient ensuite envoyées sur un smartphone local (un Nexus 4 LG) en Bluetooth avant d'être récupérée par le serveur de traitement.

Le résultat est «encourageant». L'algorithme est ainsi capable de différencier la saisie sur un clavier de DAB de celle d'un smartphone, par exemple. Et parvient à déterminer les différents codes PIN respectifs non sans un certain succès. *« Le système est en mesure de déduire les frappes avec une précision de 19% quand il est formé et évalué avec des données enregistrées selon différents claviers »*, déclare le chercheur.

Des travaux théoriques

Il suffirait donc à un attaquant de parvenir à appairer en Bluetooth la montre connectée ou le bracelet traqueur d'activité de la victime à son terminal (un smartphone généralement) pour installer l'application qui permettra de capter les données lorsque l'attaqué saisit des codes numériques (sur son smartphone, au distributeur de billets, etc.) et de les renvoyer. Ce qui, certes, n'est pas une mince affaire et s'avèrera peu utile si la victime saisit ses codes avec le membre dépourvu du dispositif bardé des capteurs. Mais *« le but de ce travail est de sensibiliser sur les risques potentiels liés à des détecteurs de mouvement intégré dans les dispositifs portables et de démontrer les risques d'abus motivés par les avancées des architectures de réseaux de neurones »*, souligne Tony Beltramelli.

A ce jour, il s'agit donc de travaux purement théoriques et, pour l'heure, non mis en application. C'est probablement pour éviter qu'il le soit que le chercheur a partagé son projet sur GitHub. Au risque de produire le résultat inverse.

Lire également

Un hacker pirate le vol d'un avion depuis un siège passager
Piratage des panneaux à Lille : une blague qui fait (un peu) peur
Sécurité : des hackers testent le contrôle à distance d'une Jeep