A Side Journey To Titan

Revealing and Breaking NXP's P5x ECDSA Implementation on the Way

Camille Mutschler[1,2], Thomas Roche[1], Victor Lomné[1], and Laurent Imbert[2]

[1]NinjaLab, Montpellier, France
[2]LIRMM, Univ. Montpellier, CNRS, Montpellier, France

Abstract

La *clé de sécurité Google Titan* [3] est un produit matériel implémentant le standard FIDO U2F [2] proposé par Google (disponible depuis juillet 2018). FIDO U2F est un protocole de *second facteur d'authentification* permettant de se connecter à des applications tel que son compte Google. Dans notre papier *A Side Journey To Titan* [5], nous présentons une attaque par canaux auxiliaires qui cible l'élément de sécurité de la *clé de sécurité Google Titan*, le composant NXP A700x, par l'observation de ses radiations électromagnétiques (EM) pendant l'exécution de signatures ECDSA (l'opération cryptographique principale du protocole FIDO).

Pour cette attaque, on considère que l'attaquant réussit à obtenir un accès physique à la *clé de sécurité Google Titan* de sa victime. L'attaquant doit récupérer les traces EM de quelques milliers de signatures. En analysant chacune de ces traces, il peut obtenir des bits d'information sur les clés éphémères utilisées pour ces signatures. Une fois ces information en sa possession, l'attaquant est capable de retrouver la valeur de la clé secrète du schéma de signature ECDSA de la clé Titan.

Pour trouver une fuite d'information sur les clés éphémères, nous avons dû rétro-concevoir l'algorithme de multiplication scalaire utilisé pour la génération de signature ECDSA dans la clé Titan, et ainsi exploiter ses failles.

Le protocole FIDO ne permet pas de choisir la valeur de la clé secrète et ainsi limite grandement les possibilités de rétro-conception par la simple analyse de traces EM. Nous avons alors décidé de passer par un autre produit NXP (la JavaCard NXP J3D081), possédant des caractéristiques très proches du composant NXP A700x et permettant que l'on choisisse la valeur de la clé secrète ECDSA. Nous avons nommé ce produit Rhéa[1]. En plus de leurs caractéristiques proches, l'analyse des traces EM de génération de signatures ECDSA de Titan et de Rhéa nous a confirmé que l'algorithme de multiplication scalaire utilisé pour ces deux produits était très similaire.

Les analyses de traces EM faites sur Rhéa nous ont permis de retrouver l'algorithme utilisé pour effectuer la multiplication scalaire sur la clé Titan. La compréhension de cet algorithme nous a permis d'identifier une faille permettant la récupération de quelques bits d'informations répartis aléatoirement dans les clés éphémères.

La connaissance partielle des clés éphémères utilisées pour générer des signatures ECDSA permet de récupérer la valeur de la clé secrète du schéma en ré-écrivant ce problème comme une instance de l'Extended Hidden Number Problem (EHNP) [1]. Nous savons résoudre EHNP par la recherche du vecteur le court dans un réseau euclidien spécifique [4]. En résolvant le problème EHNP à l'aide des signatures récupérés et des informations obtenues sur les bits connus des clés éphémères, notre attaquant peut donc retrouver la valeur de la clé secrète du schéma de signature ECDSA utilisé pour la clé Titan.

Grace à cette attaque, un attaquant est donc capable de cloner une *clé de sécurité Google Titan*.

En parallèle du travail réalisé pour cette attaque, nous avons révélé une nouvelle corrélation entre l'ordre du groupe de la courbe elliptique utilisée pour le schéma de signature ECDSA et le taux de succès de l'attaque EHNP.

Pour mon exposé, je me concentrerais sur la partie de l'attaque basée sur la résolution du problème de réseaux euclidiens EHNP.

[1]du nom de la deuxième plus grosse lune de saturne après Titan

References

[1] Dan Boneh and Ramarathnam Venkatesan. Hardness of Computing the Most Significant Bits of Secret Keys in Diffie-Hellman and Related Schemes. In Neal Koblitz, editor, *Advances in Cryptology — CRYPTO '96*, pages 129–142, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg.

[2] FIDO Alliance. Universal 2nd Factor (U2F) Overview. `https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-overview-v1.2-ps-20170411.pdf`. [online; accessed 1-June-2021].

[3] Google. Google Titan Key. `https://cloud.google.com/titan-security-key/`. [online; accessed 1-June-2021].

[4] Nick Howgrave-Graham and Nigel P. Smart. Lattice Attacks on Digital Signature Schemes. *Des. Codes Cryptogr.*, 23(3):283–290, 2001.

[5] Thomas Roche, Victor Lomné, Camille Mutschler, and Laurent Imbert. A side journey to titan. In Michael Bailey and Rachel Greenstadt, editors, *30th USENIX Security Symposium, USENIX Security 2021, August 11-13, 2021*, pages 231–248. USENIX Association, 2021.