Las claves de seguridad de hardware, como las de Google y Yubico se consideran el medio más seguro para proteger las cuentas de ataques de suplantación de identidad y de toma de control.

Sin embargo, una nueva investigación publicada el jueves demuestra cómo un adversario en posesión de un dispositivo de autenticación de dos factores (2FA) puede clonarlo mediante la explotación de un canal lateral electromagnético en el chip integrado.

La vulnerabilidad, rastreada como CVE-2021-3011, permite que el actor malintencionado extraiga la clave de cifrado o la clave privada ECDSA vinculada a la cuenta de una víctima desde un dispositivo FIDO Universal 2nd Factor (U2F) como Google Titan Key o YubiKey, socavando de este modo las protecciones 2FA.

> *«El adversario puede iniciar sesión en la cuenta de la aplicación de la víctima sin el dispositivo U2F y sin que la víctima se dé cuenta»,* dijeron los investigadores de NinjaLab, Victor Lomne y Thomas Roche.
>
> *«En otras palabras, el adversario creó un clon del dispositivo U2F para la cuenta de la aplicación de la víctima. Este clon dará acceso a la cuenta de la aplicación siempre que el usuario legítimo no revoque sus credenciales de autenticación de segundo factor»*, agregaron.

La lista completa de productos afectados por la vulnerabilidad incluye todas las versiones de Google Titan Security Key, Yubico Yubikey Neo, Feitian FIDO NFC USB-A/K9, Feitian MultiPass FIDO / K13, Feitian ePass FIDO USB-C / K21 y Feitian Fido USB-C / K40.

Además de las claves de seguridad, el ataque también se puede llevar a cabo en chips NXP JavaCard, incluidos NXP J3D081_M59_DF, NXP J3A081, NXP J2E081_M64, NXP J3D145_M59, NXP J3D081_M59, NXP J3E145_PM64_D, y NXP J3E145_PM64_D, y NXP J3E145_PM64_D, y sus variantes respectivas.

El ataque de recuperación de claves, aunque sin duda es grave, debe cumplir una serie de requisitos previos para tener éxito.

Un actor de amenazas primero tendrá que robar el nombre de usuario y contraseña del objetivo de una cuenta protegida por la clave física, luego obtener acceso de forma sigilosa a la Titan Security Key en cuestión, sin mencionar adquirir equipos costosos que cuestan más de 12,000 dólares y tener suficiente experiencia para construir software a medida para extraer la clave vinculada a la cuenta.

> *«Aunque es más seguro usar su llave de seguridad Titan de Google u otros productos afectados como un token de autenticación de dos factores FIDO U2F para iniciar sesión en aplicaciones en lugar de no usar una»,* dijeron los investigadores.

Para clonar la clave U2F, los investigadores tuvieron que abrir el dispositivo con una pistola de aire caliente para quitar la carcasa de plástico y exponer los dos microcontroladores soldados en ella: un enclave seguro (chip NXP A700X) que se utiliza para realizar las operaciones de criptografía y un chip de propósito general que actúa como un enrutador entre las interfaces USB/NFC y el microcontrolador de autenticación.

Una vez logrado esto, los investigadores afirman que es posible conseguir la clave de cifrado ECDSA a través de un ataque de canal lateral al observar las radiaciones electromagnéticas que salen del chip NXP durante las firmas ECDSA, la operación criptográfica central del protocolo FIDO U2F que se realiza cuando se produce un U2F ocasiona que la clave se registre por primera vez para trabajar con una nueva cuenta.

Un ataque de canal lateral por lo general funciona con la información obtenida de la implementación de un sistema informático, en lugar de explotar una debilidad en el software. Por lo general, los ataques aprovechan la información de tiempo, el consumo de energía, las fugas electromagnéticas y las señales acústicas como fuente de fugas de datos.

Al adquirir 6000 de estos rastreos de canal lateral de los comandos de solicitud de autenticación U2F durante un período de seis horas, los investigadores dijeron que pudieron recuperar la clave privada ECDSA vinculada a una cuenta FIDO U2F creada para el experimento utilizando un modelo de aprendizaje automático no supervisado.

Aunque la seguridad de una llave de seguridad de hardware no se ve disminuida por el ataque anterior debido a las limitaciones involucradas, una posible explotación en la naturaleza no es inconcebible.

> *«Sin embargo, este trabajo muestra que la llave de seguridad Titan de Google (u otros productos afectados) no evitarían una brecha de seguridad inadvertida por parte de los atacantes dispuestos a esforzarse lo suficiente. Los usuarios que enfrentan esta amenaza probablemente deberían cambiar a otras llaves de seguridad de hardware FIDO U2F, donde aún no se ha descubierto ninguna vulnerabilidad»,* concluyeron los investigadores.