# Cómo mejorar la seguridad del DNI 3.0

Investigadores del Centro Universitario de la Defensa y de la Universidad de Valladolid han evaluado la seguridad contra el robo de identidad del DNI 3.0, un documento que permite realizar diversas gestiones de forma inalámbrica con dispositivos móviles. Según el estudio, si se incorpora un temporizador, los ciberatacantes tendrían prácticamente imposible conseguir la contraseña que se establece en la conexión inicial.

SINC 4/12/2017 08:14 CEST


La principal novedad del DNI 3.0 frente a su antecesor, el DNIe, es la presencia de un chip con interfaz dual que permite la conexión mediante hardware o de forma inalámbrica a través de la tecnología NFC (Near Field Comunication). / Dirección General de la Policía

El robo de información personal para suplantar la identidad de las personas es uno de los delitos que más ha aumentado en los últimos años, en paralelo al desarrollo de las nuevas tecnologías. El uso de estos datos por parte de delincuentes para cometer fraudes y otros delitos graves supone una amenaza común hoy en día, pese a los avances tecnológicos y los sistemas de seguridad.

En 2015, la Dirección General de la Policía española comenzó a expedir el

DNI 3.0. A las funcionalidades de su predecesor, el DNIe –lanzado en 2006–, se añadió un chip con interfaz dual que permite la conexión mediante un lector en el que introducir la tarjeta, pero también de forma inalámbrica, a través de la tecnología NFC (siglas en inglés de Near Field Comunication). Esta tecnología está integrada en la mayoría de los dispositivos móviles del mercado y su funcionamiento se basa en la creación de un campo electromagnético en el que, mediante inducción, se genera un intercambio de datos entre dispositivos.

El pequeño problema de software detectado puede resolverse fácilmente con la instalación de un temporizador

Esta tecnología, ya utilizada desde hace algunos años en los pasaportes electrónicos, permite al ciudadano conectarse con la Administración de forma digital, sin necesidad de contacto, con tan solo disponer del DNI 3.0, de un smartphone o tablet con tecnología NFC y de una aplicación (APP) del servicio al que se desee conectar. Pero, como sucede con cualquier nuevo dispositivo que se pone en circulación, supone una nueva ventana para el posible ataque de ciberdelincuentes.

Ahora, investigadores del Centro Universitario de la Defensa y de la Universidad de Valladolid (UVa) han evaluado la seguridad contra el robo de identidad del DNI 3.0, y han comprobado que, instalando un temporizador, un ciberatacante tendría prácticamente imposible conseguir la contraseña que se establece en la conexión inicial. El estudio se ha publicado en la revista *IET Information Security.*

“Para comunicarse de forma segura con el DNI, un lector establece esa conexión inicial y, antes de establecer una clave de alta seguridad, utiliza una más sencilla, basada en la información que aparece escrita en la parte delantera del documento”, explica a DiCYT Juan Carlos García-Escartín, investigador de la UVa, quien ha llevado a cabo el trabajo junto con Ricardo Julio Rodríguez, del Centro Universitario de la Defensa.

**Un ataque cercano**

Según recuerda, la idea de hacer una evaluación independiente del DNI 3.0, tiene como objetivo conocer hasta qué punto este documento es seguro frente a un ataque de fuerza bruta de alguien que, externamente, no conozca los datos que contiene el DNI, pero que esté lo suficientemente cerca como para conectarse al documento sin que el usuario se dé cuenta.

Una espera de milisegundos frente a un lector no supone una molestia para el usuario, pero el ciberdelincuente tendría problemas

"Un ataque de fuerza bruta consiste en que alguien que no puede ver la información de la cara delantera del DNI intente todas las combinaciones posibles hasta llegar a la contraseña", precisa. En función de cuánta información haya en ese campo la contraseña puede ser más o menos difícil de acertar, aunque existen parámetros que no son completamente aleatorios y que reducen el tiempo que un delincuente tendría que emplear hasta conseguir la contraseña.

Por ejemplo, la fecha de caducidad del DNI está relacionada con la edad del usuario. "Afinando por ese parámetro, en un ataque se puede reducir el número de intentos necesarios. La solución es bastante sencilla y la tienen muchos sistemas de contraseñas que lo que hacen es, ante dos o tres intentos fallidos, poner un tiempo de espera para volver a intentar introducir la contraseña.

De este modo, para una persona que esté en el lector esperando a pasar su DNI, un retardo de milisegundos no le supone una molestia, mientras que en caso de ataque el delincuente tendría problemas porque unos solos milisegundos, con todos los intentos que tiene que hacer, supone pasar de días a meses o años para lograr la contraseña", detalla.

No obstante, apunta el investigador de la UVA, en general los sistemas del DNI 3.0 que han evaluado están bien implementados. "Ese pequeño problema de software que hemos detectado puede resolverse fácilmente con la instalación, como decimos, de un temporizador, que ya nos consta que se considerará en futuras actualizaciones del software. De esta forma, el

ataque pasaría de ser poco probable a prácticamente imposible", concluye García-Escartín.

**Referencia bibliográfica:**

Rodríguez, R. J., y Garcia-Escartin, J. C. (2017). "Security assessment of the Spanish contactless identity card". *IET Information Security* 11(6): 386-393, 2017.



TAGS | DNI | CIBERSEGURIDAD | DNI 3.0 |

La ciencia es noticia