Seguridad en pagos móviles

Después de varios posts hablando acerca del comercio online y de las posibilidades que brindan los pagos online a empresas o entre particulares, quizá deberíamos hacer un repaso a los riesgos que conlleva sustituir el dinero físico en nuestras transacciones, por una divisa digital, que está en nuestro Smartphone.

En primer lugar, el proceso de autenticación debe asegurar con la máxima fidelidad, que el que está realizando el pago es el usuario legítimo al que pertenece la cuenta y no se está utilizando un Smartphone robado o se está suplantando la identidad del propietario, a priori, puede sonar fácil, vivimos en un mundo de contraseñas que utilizamos para casi todos los servicios que mantienen nuestra vida online, actualmente las formas de autenticar a una persona son en base a lo que sabe o lo que tiene[1] en el primero de los casos hablamos de las contraseñas, cadenas de texto que pueden ser olvidadas en caso de ser largas y contener muchos caracteres o adivinadas por personas que intentan suplantar al usuario. Por otro lado, se nos puede autenticar con respecto a lo que tenemos, como puede ser un token, que no es más que un fragmento binario ubicado en nuestro dispositivo que nos identifica como legítimos, esta última medida como ya se está imaginando el lector, tiene más de una manera de ser trampeada mediante el robo de este token. Sin embargo, actualmente hay un nuevo tipo de autenticación que los fabricantes de dispositivos móviles están extendiendo cada vez más en sus últimos modelos, se trata de la biometría.

Hoy en día es común ver cómo la mayoría de terminales de gama media o alta cuentan con sensores de huellas dactilares que permiten proteger tanto el acceso al teléfono en sí como a sus aplicaciones, actualmente, son muchos los bancos y sistemas de

pago que se benefician de esta funcionalidad para garantizar un pago seguro. Pero debemos preguntarnos, ¿Todo son ventajas en este tipo de autenticación para pagos? Lo cierto es que no, ya que para empezar el ni siquiera la misma persona va a tener un escaneado de su huella dactilar idéntico al anterior, lo que hace que estos sistemas cuenten con una tolerancia a fallo[2] que tiene que entrar dentro de los niveles considerados "aceptables", como esta tolerancia no esté ajustada de una forma muy precisa, puede darse el caso de personas que pueden suplantar identidad de otras a las que físicamente puedan tener una medida corporal parecida. Otro riesgo implícito de la identificación biométrica es la propia naturaleza única e insustituible de tu parte de la anatomía que utilices para esta autenticación, mientras que una contraseña es fácilmente reemplazable y sustituible, difícilmente vamos a poder cambiar nuestro iris o nuestras huellas dactilares en caso de haber conseguido de alguna forma replicar nuestra medida biométrica. En definitiva, el problema de autenticación que implica un pago a través de un Smartphone puede ser subsanado con una mezcla de autenticación biométrica y de contraseña tradicional.

Por otro lado, existen otros riesgos en las transacciones económicas móviles, para comprender la complejidad que implica todos los actores relacionados con este tipo de operaciones primero tenemos que diferenciar qué tipo de entidad es la que gestiona la cuenta cliente[2], principalmente se pueden diferenciar en:

- Bancarizada "bank-centric", la cuenta cliente es gestionada por un banco y toda la operativa relacionada con la seguridad, transacciones y responsabilidad está ubicada en la propia entidad.
- No bancarizada "nonbank-centric", la cuenta del cliente está gestionada por organizaciones no financieras, por ejemplo PayPal o Yaap money, donde el cliente gestiona un saldo virtual en el servicio y es con el que opera en

las transacciones.

Es este último modelo no bancarizado el que plantea más dudas en cuanto a la seguridad, aunque la unión europea está dando pasos para regular la actividad de estas nuevas empresas que no son bancos como operadoras de telefonía y grandes almacenes, existe el riesgo que sus sistemas o los que puedan subcontratar a otras empresas no cuenten con las medidas de seguridad suficientes como para garantizar una transacción segura.

Indudablemente, los pagos móviles representan un claro avance en países en desarrollo donde no existan infraestructuras tradicionales para pagos electrónicos, y una extensión de los métodos de pago habituales en países desarrollados donde aportan comodidad en las transacciones online[3], sin embargo, hay que tener en cuenta que la llegada de nuevos actores al escenario financiero introduce nuevos riesgos y el replanteamiento de las formas de autenticación online para la prevención del fraude.

Referencias:

[1] “Biometrics for securing mobile payments: Benefits, challenges and solutions”, IEEE Explore, acceso el 16 de noviembre del 2016

[2] “Pagos mediante dispositivos moviles: cuestiones relacionadas con los riesgos, la seguridad y el aseguramiento”, ISACA, acceso el 16 de noviembre del 2016

[3] “MOBILE PAYMENT – RISKS OF A NEW TECHNOLOGY”, Deusto OCEANO, acceso el 16 de noviembre del 2016