>> Jorge Dávila

Criptomonedas y nuevos servicios de pago en Internet

Apple ha incluido en el último momento el lanzamiento de su iniciativa Apple Pay dentro de la campaña de lanzamiento del iPhone 6 y el nuevo iOS 8. Con esto, Apple parece querer entrar en el sector financiero poniendo su teléfono como único procedimiento cómodo y seguro de pagar ante los nuevos terminales inalámbricos. Viendo el clásico estancamiento de los sistemas de pago y los servicios financieros, quizás sea pertinente ver si con la aparición de este nuevo jugador llegan innovaciones significativas que abran una nueva etapa para los sistemas de pago en Internet.

Un anuncio glamuroso

El pasado mes de septiembre la glamurosa compañía Apple hizo un abundante número de lanzamientos, prácticamente simultáneos, al mercado internacional. Por una parte vio la luz el deformable[1] **iPhone 6**[2], y además se lanzaron la actualización del sistema operativo de la casa a **iOS 8**[3], el reloj de pulsera **iWatch**[4] y el servicio financiero **Apple Pay**[5]. De los cuatro, los que más sorprendieron, por imprevistos, fueron los del reloj de pulsera y el nuevo sistema de pago electrónico, que quiere convertir al nuevo *token* en la tarjeta de crédito del futuro que se nos avecina.

Con el eslogan "*Your wallet. Without the wallet*", Apple quiere desterrar las carteras, los monederos y las muy populares tarjetas de crédito, de modo que, con ellos y su tecnología, el acto de desembolsar un pago se reduzca a un "*touch*". Con este lanzamiento, la empresa de la manzana mordida quiere ponerse a la cabeza de los pagos mediante técnicas sin contacto (NFC)[6], argumentando que su seguridad sólo es posible utilizando los detectores de huella que incluye ya en sus dos últimos modelos de teléfono. Además, por si fuera poco, se anuncia que, de este modo, los pagos con el iPhone 6 serán sencillos, seguros y "*privados*".

Touch ID no deja de ser un sofisticado y compacto lector de huellas dactilares. El análisis de esa huella normalmente desbloquea el teléfono, pero también autoriza un pago si tal cosa se ha solicitado. Algunos siguen creyendo erróneamente que la huella dactilar es la contraseña perfecta porque siempre la llevas encima, pero se olvidan de que, aunque nadie puede a priori adivinarla, la vamos dejando en todos y cada uno de los objetos que tocamos con las manos desnudas, por lo que es trivial hacerse con ellas.

Touch ID y Apple Pay

A diferencia de otras aplicaciones de pago que ya existen dentro del mundo AppStore, en el caso del iPhone es tal la integración del sistema de pago con el objeto que no será necesario abrir ninguna aplicación o incluso activar la pantalla para poder pagar; bastará con colocar el iPhone cerca del lector NFC y poner la huella dactilar en el denominado **Touch ID**. Puestos a exagerar más la sencillez del estilo *Eloi*[7] de Apple, en su publicidad resaltan que incluso "*no es necesario mirar la pantalla para conocer la cantidad que se está pagando*", lo cual debe estar dirigido a la clases pudientes y no afectadas por ninguna crisis. De hecho, con el flamante iPhone ni siquiera es necesario comprobar que la transacción ha ido bien, pues una suave vibración del artefacto se encargará de informarnos de ello.

El Touch ID no deja de ser un sofisticado y compacto lector de huellas dactilares. En él, un anillo de acero que enmarca el botón detecta la presencia de un supuesto dedo y activa un sensor táctil capacitivo construido alrededor de un exquisito cristal de zafiro con el que obtiene una imagen de la huella dactilar que lo toca. El análisis de esa huella normalmente desbloquea el teléfono, pero también autoriza un pago si tal cosa se ha solicitado. **Algunos siguen creyendo erróneamente que la huella dactilar es la contraseña perfecta porque siempre la llevas encima**, pero se olvidan de que, aunque nadie puede *a priori* adivinarla, **la vamos dejando en todos y cada uno de los objetos que tocamos** con las manos desnudas, por lo que **es trivial hacerse con ellas**. Poco han tardado algunos[8] en demostrar lo sencillo que es engañar al guardián de los últimos iPhone con un sustituto de goma[9].

Con el eslogan "Your wallet. Without the wallet", Apple quiere desterrar las carteras, los monederos y las tarjetas de crédito, de modo que, con ellos y su tecnología, el acto de desembolsar un pago se reduzca a un "touch". Con este lanzamiento, quiere ponerse a la cabeza de los pagos mediante técnicas sin contacto (NFC), argumentando que su seguridad solo es posible usando los detectores de huella que incluye ya en sus dos últimos modelos de teléfono.

Apple no pretende con su nuevo sistema de pago desban-

[1] Ver http://cramersshirt.weebly.com/blog/kids-dont-try-this-at-home
[2] Ver http://www.apple.com/es/iphone-6/?cid=wwa-es-kwg-iphone-com
[3] Ver https://www.apple.com/mx/ios/
[4] Ver http://www.apple.com/es/watch/?cid=wwa-es-kwg-watch-com
[5] Ver https://www.apple.com/apple-pay/
[6] Ver http://en.wikipedia.org/wiki/Near_field_communication
[7] En la novela "Illium" de Dan Simmons (2003, ISBN 0-380-97893-8), "Eloi" es el apodo para los perezosos y no-educados descendientes de la raza humana después de que los post-humanos haya abandonado la Tierra. Los *Eloi* son técnicamente hábiles pero no entienden la tecnología; regresan y olvidan milenios de cultura, pensamiento y razón, hasta que su satisfacción mana del mero hecho y placer de existir.
[8] Ver http://arstechnica.com/apple/2013/09/chaos-computer-club-hackers-trick-apples-touchid-security-feature/
[9] Ver http://dasalte.ccc.de/biometrie/fingerabdruck_kopieren.en

car a los jugadores de siempre en el mercado de las tarjetas de crédito (VISA, MasterCard y American Express), sino que son los números de éstas los que almacena y gestiona en su interior (**Passbook**)[10]. Apple ha llegado a acuerdos con grandes bancos norteamericanos (Bank of America, Capital One Bank, Chase, Citibank y Wells Fargo), que pagarán una comisión a Apple por su colaboración en la transacción. De hecho, esos datos de tarjeta de crédito ya los tiene Apple en sus cuentas de **iTunes**.

El paradigma MP ("Mobile Payment")

Apple Pay es un ejemplo más de lo que se conoce como "Mobile Payment" (MP), y se refiere a los servicios financieros de pago que, de forma regulada, se construyen alrededor de los teléfonos móviles. En principio, cualquier instrumento de pago, ya sean las cuentas bancarias, las tarjetas de crédito/débito y las cuentas de valor almacenado (Stored Value Accounts) como son las tarjetas de precarga, las tarjetas regalo, Paypal o los *mobile wallets*, pueden considerarse formas de *m-payment*.

El paradigma MP persigue sustituir al dinero, los cheques y las tarjetas de crédito/débito en el pago de servicios digitales y analógicos por transacciones hechas con el móvil. Dentro de esta corriente han puesto en pie propuestas MP tanto instituciones financieras, como compañías de tarjetas de crédito (**PayPass** de MasterCard)[11], compañías de Internet (**Google Wallet**)[12], operadoras de redes móviles, algunas de las telcos (**w-HA**)[13] y las multinacionales de los terminales como es el caso de **Ericsson Money**[14].

El argumento principal sobre la supuesta superioridad de este nuevo método de pago frente a las tradicionales tarjetas con el chip EMV es que, con estas últimas, **cada vez que se paga, el número de tarjeta y los datos de filiación son visibles para el comerciante**. En las nuevas propuestas como la de Apple, se opta por enterrar esos datos en la aplicación **Passbook**[15], y en su lugar asignarles un "*Device Account Number*" único que es cifrado y almacenado en un chip (hardware) contenido en el teléfono y que han dado en bautizar como "**Secure Element**"[16]. Este elemento seguro **viene a ser la versión NFC del chip EMV**[17], que hasta hace poco no estaba en todas las tarjetas de crédito; de hecho, en EE.UU. está empezándose a implantar ahora el estándar EMV que lleva once años difundiéndose por Europa[18].

Aunque no hay información detallada para poder corroborarlo, se dice que esos nuevos números mágicos nunca se almacenan en los servidores de Apple, por lo que, en principio, no se podrían confeccionar perfiles relativos a las compras y pagos de los cliente. En el sistema propuesto, cada pago utiliza ese nuevo número de identificación (*Device Account Number*) junto con otros detalles de la transacción y un cambiante código de autenticación que llaman "*security code*". De este modo, el número de tarjeta no se comparte con los comerciantes ni es transmitido como parte de la transacción, permaneciendo oculto.

La interposición de este nuevo número de cuenta no resuelve las limitaciones que siempre ha tenido el sistema de tarjetas bancarias, y es el de **que la mera mención del número impreso en la tarjeta todavía surta efecto comercial**. Esta funcionalidad que deja fuera la libre y explícita voluntad del pagador es lo que se pretende corregir creando un nuevo número (*payment token*) que está vinculado a uno secreto (firma ECDSA) que está protegido en un recóndito rincón del artefacto que llamamos "nuestro" teléfono móvil. Cuando se den (o se filtren) más detalles de este protocolo de pago[19] en iOS 8, podremos considerar si es seguro, o si adolece de debilidades inconfesadas pero aceptadas en aras de la compatibilidad "hacia atrás" en el mundo de las tarjetas bancarias.

En lo que se refiere a la privacidad y a la amenaza del Gran Hermano, Apple declara que no se queda con copia de los datos de la transacción y, sin embargo, son sus teléfonos los que las realizan. Esto va en la línea de sus últimos anuncios sobre que la nueva versión del sistema operativo iOS 8 lo va a cifrar todo y Apple no va a poder entregar ninguna información a las agencias de seguridad cuando éstas se lo soliciten. La verdad es que eso no parece ser exactamente como se cuenta y quizás todavía quede un modo de hacerlo.

En cualquier caso, una vez más, esta afirmación habrá de ser aceptada (por algunos) como acto de fe, sobre todo cuando la propia Apple reconoce que algo queda en la aplicación Passbook y que será recompensada por los bancos proporcionalmente a la cuantía de esa transacción no anotada.

A la vista de todo lo anterior, **no se puede considerar que haya nada nuevo en la entrada de Apple como intermediador en el mundo de los sistemas de pago**. De hecho,

El argumento principal sobre la supuesta superioridad del nuevo método de pago frente a las tradicionales tarjetas con chip EMV es que, con estas últimas, cada vez que se paga, el número de tarjeta y los datos de filiación son visibles para el comerciante. En las nuevas propuestas como la de Apple, se opta por enterrar esos datos en la aplicación Passbook, y en su lugar asignarles un "Device Account Number" único que es cifrado y almacenado en un chip contenido en el teléfono y que han dado en bautizar como "Secure Element", que viene a ser la versión NFC del chip EMV.

No se puede considerar que haya nada nuevo en la entrada de Apple como intermediador en el mundo de los sistemas de pago. De hecho, es un ejemplo más de la iniciativa sectorial que se conoce como GlobalPlatform y que tiene los mismos objetivos que en su tiempo dieron a luz el sistema EMV o las propias tarjetas inteligentes (smartcards) a finales del siglo pasado.

[10] Ver http://en.wikipedia.org/wiki/Passbook_(application)
[11] Ver https://mobile.mastercard.com/Partner/MobilePayPass/Home
[12] Ver https://www.google.com/wallet/
[13] Ver http://www.w-ha.com/en/
[14] Ver http://www.ericsson.com/m-commerce/
[15] Ver http://www.nfcworld.com/2014/09/18/331547/apple-joins-nfc-secure-element-standards-body/
[16] Ver https://mobile.mastercard.com/Partner/MobilePayPass/SecureElements y http://www.globalplatform.org/
[17] Ver http://en.wikipedia.org/wiki/EMV
[18] Ver http://www.cl.cam.ac.uk/~sjm217/papers/cacm14emv.pdf
[19] Ver https://developer.apple.com/library/IOs/documentation/UserExperience/Reference/PassKit_Framework/index.html

es un ejemplo más de la iniciativa sectorial que se conoce como **GlobalPlatform**[20] y que tiene los mismos objetivos que en su tiempo dieron a luz el sistema EMV o las propias tarjetas inteligentes (*smartcards*) a finales del siglo pasado. Como si fuese obra de una tenaz falta de imaginación, esta nueva iniciativa repite lo que antes hicieran otras, y sigue buscando el "Santo Grial" de lo que ahora llaman "**Trusted Execution Enviroments**" y que en otras épocas llamaron "Trusted Computing base"[21] cuando se hablaba de ordenadores en general, o de la "Trusted Platform Module"[22] si hablamos de las tarjetas inteligentes.

Las buenas noticias para ese nuevo intento de meter toda la seguridad en un chip (y por ende dentro de un smartphone de alta gama) son que los sistemas EMV han estado más de diez años a prueba en Europa y que se dispone de experiencia real de campo de la que aprender. Toda esta experiencia debería tenerse en cuenta a la hora de proponer nuevos sistemas de pago, pero ese no es el caso de Apple Pay, que sólo pretende ser un diligente intermediario dentro del mercado actual de servicios de pago.

Las Criptomonedas

Por el momento, si lo que se busca son novedades, innovación, en el sector financiero llevado al mundo digital de Internet, los únicos indicios los encontramos en las denominadas **Criptomonedas**[23],que mantienen vivo el antiguo ideal de los sistemas anónimos (pero trazables) para micropagos[24]. La más conocida de estas iniciativas es **Bitcoin**[25] (Satosi Nakamoto, 2008), por su implicación en diferentes actividades ilegales como el mercado de la Internet profunda conocido como "la Ruta de la seda", o el pago de rescates al ciberfilibustero conocido como CryptoLocker, pero en realidad Bitcoin no es la única moneda virtual disponible.

Según el Banco Central Europeo, estos nuevos productos[26] deben verse como "*un tipo de dinero digital no regulado que es utilizado y usualmente controlado por sus desarrolladores, a la vez que es utilizado y aceptado por los miembros de algunas comunidades virtuales específicas*".

Todas estas nuevas monedas son iniciativas extraordinariamente jóvenes que todavía arrastran muchos inconvenientes técnicos como son la cada día más grande "Cadena de Transacciones" (*Blockchain*) y su subordinación a una élite de mineros a través de las comisiones de transacción, por poner algún ejemplo. Sin embargo, sus comisiones son significativamente más bajas que las cobradas por la media docena de compañías internacionales que se reparten el negocio de las tarjetas de crédito/débito, lo cual puede terminar abriéndolas un campo de existencia real en la futura Internet.

Estas iniciativas virtualizantes gozan del rechazo y desconfianza de los sistemas financieros nacionales e internacionales, pero no está claro que vayan a desaparecer como una tormenta de verano. De hecho, no es descabellado pensar que, de mantenerse más tiempo, esas iniciativas terminen desarrollando en Internet un sector financiero digital análogo al que el dinero de curso legal ha desarrollado en Occidente desde el Renacimiento europeo.

El vetusto protocolo EMV que ahora rediseña la GlobalPlatform, en realidad no es una norma rígida con la que construir sistemas de pago con tarjetas, sino que, más bien, es una caja de herramientas con la que el sector financiero puede construir sistemas de pago bastante seguros o, según su falta de pericia, también puede crear sistemas con efectos desastrosos.

Las malas noticias son que los intereses de los bancos, comerciantes, vendedores, titulares de las tarjetas y de los reguladores divergen considerablemente y no está claro que ninguno de ellos esté realmente interesado en que el sistema resultante sea seguro frente al fraude.

Las buenas noticias para ese nuevo intento de meter toda la seguridad en un chip (y por ende dentro de un *smartphone* de alta gama) son que los sistemas EMV han estado más de diez años a prueba en Europa y que se dispone de experiencia real de campo de la que aprender. Casi todo lo que podía ir mal, ya ha ido mal con las tarjetas chip: se han dado fallos de protocolo que han permitido ataques no imaginados; la resistencia frente a manipulaciones de los chips (*tamper-resistance*) no ha funcionado en todos los casos; algunos esquemas de certificación sectorial han sido una peligrosa farsa, y los sistemas de recolección de evidencias, cuando se les ha necesitado, no han cumplido su misión. Toda esta experiencia debería tenerse en cuenta a la hora de proponer nuevos sistemas de pago, pero ese no es el caso de Apple Pay, que sólo pretende ser un diligente intermediario dentro del mercado actual de servicios de pago.

Las malas noticias son que los intereses de los bancos, comerciantes, vendedores, titulares de las tarjetas y de los reguladores divergen considerablemente y **no está claro que ninguno de ellos esté realmente interesado en que el sistema resultante sea seguro frente al fraude**. En Europa tenemos una larga experiencia de que los bancos culpen de sus muchos errores a comerciantes y a clientes finales que nunca están preparados para defenderse frente a ellos. Esta facilidad que tienen los bancos de que sean otros los que paguen las consecuencias del fraude relaja mucho sus exigencias de diseño de los sistemas puestos en explotación.

La innovación digital en el sector financiero está todavía muy lejos, pero puede que algún día sí haya cambios en la realidad social y económica que lo dejen atrás y ello permita la entrada de nuevos agentes e ideas que ventilen un poco este bastión de tan selectos miembros. ■

Jorge Dávila Muro
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es

[20] Ver http://en.wikipedia.org/wiki/GlobalPlatform
[21] Ver http://en.wikipedia.org/wiki/Trusted_computing_base
[22] Ver http://en.wikipedia.org/wiki/Secure_cryptoprocessor
[23] Ver http://en.wikipedia.org/wiki/Cryptocurrency
[24] Ver http://en.wikipedia.org/wiki/Micropayment
[25] Ver https://bitcoin.org/bitcoin.pdf
[26] Ver http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf