Gestión de identidades digitales basada en el paradigma de la reducción de tiempo de exposición

Jose María Alonso
Telefonica Digital Identity - Privacy
Security researcher
Email: chema@11paths.com

Antonio Guzmán
Telefonica Digital Identity - Privacy
Security researcher
Email: antonio.guzman@11paths.com

Alfonso Muñoz
Telefonica Digital Identity - Privacy
Security researcher
Email: alfonso.munoz@11paths.com

***Resumen*—La presente investigación analiza la problemática actual de la gestión de identidades digitales centrada en tres pilares fundamentales: la seguridad de la solución, su usabilidad y el coste de su implementación. En este artículo se profundiza en la posibilidad de utilizar el paradigma de la reducción de tiempo de exposición para garantizar una mejor aproximación a la gestión de identidades, dando lugar a una gestión robusta, usable y de menor coste que soluciones previas. La argumentación teórica se justifica con el desarrollo de la infraestructura de gestión de identidades Latch, analizando datos reales en escenarios de comunicación comunes en Internet**

***Palabras clave*—gestión de identidades, tiempo de exposición, Latch**

I. Introducción

Cada individuo que accede al mundo digital acumula múltiples identidades digitales, cada una correspondiente con la forma en la que se decide interactuar con los diferentes servicios. El número de identidades cuya suma converge en una única identidad física se incrementa constantemente, a pesar de los esfuerzos invertidos en el desarrollo y adopción de esquemas de federación que permiten delegar los procesos de autenticación y autorización en terceros de confianza [1] [2] [3]. Algunas de las explicaciones que hay detrás de este comportamiento son:

- La desconfianza en los propietarios de los servicios digitales que usan los usuarios.
- Ver en la generación de identidades digitales la posibilidad de ganar en anonimato.
- Definición de contenedores que permitan parcelar diferentes regiones de nuestras vidas digitales (trabajo, amigos, familia, etc.).
- Evaluación de la tecnología.

En la práctica, si no se es muy escrupuloso en la forma en la que se utilizan estas identidades, aparecerán relaciones entre todas ellas. De hecho, lamentablemente, es una realidad que una mayoría de usuarios repiten las contraseñas en más de un servicio [4]. Esto plantea un escenario en el que, si el usuario ha elegido una contraseña que sea deducible, podrá comprometer la seguridad de todas las identidades que confíen en un esquema login-password. Incluso si la contraseña que el usuario ha elegido es una contraseña fuerte, si esta contraseña se usa en un sistema de seguridad débil, podrá ser capturada por un atacante. De nuevo si el usuario ha utilizado la misma contraseña en más de un servicio la fortaleza de las medidas de seguridad de estos no tendrá ningún valor. Este uso indebido de las contraseñas es tan solo una de las razones por las que las cifras que modelan el robo de identidad no dejan de crecer [5].

Este robo de identidades es uno de los problemas más importantes según el informe[6]. Es un problema que pone manifiesto la ineficacia de las soluciones propuestas para proteger la forma en la que los usuarios acceden a los servicios. Aunque el robo de identidades puede localizarse en diferentes puntos de los sistemas informáticos o estar debido a equivocadas actitudes de los usuarios, es en los mecanismos de autenticación y de autorización donde esta amenaza se convierte en un ataque al permitir que un usuario ilegítimo tenga acceso a recursos sólo accesibles a los usuarios legítimos. Aunque existen multitud de mecanismos para resolver estos procesos de autenticación y autorización todos ellos apuestan por aumentar la complejidad de la contraseña para impedir su suposición o robo [7][8] y algunos apuestan por minimizar la probabilidad de que una contraseña se reutilice para varios servicios[8]. En [9] se propone un criterio de evaluación que permite comparar unas soluciones frente a otras. Este criterio propone tres aspectos a evaluar que a su vez queda descompuesto en diversas métricas: la seguridad que ofrece una solución determinada, la usabilidad y el coste de su implementación. En la aplicación de este criterio no es posible encontrar ninguna solución que maximice los tres aspectos de su definición simultáneamente.

El NIST estadounidense propone la siguiente relación de amenazas definidas sobre los sistemas autenticación y, por extensión, sobre los sistemas de autorización [10].

- Online Guessing.
- Phising.
- Pharming.
- Eavesdropping.
- Replay.
- Session hijack.
- Man-in-the-middle (MitM).
- Denial of Service.
- Malicious code (Man-in-the-device (MitD) or Man-in-the-Browser (MitB))

ISBN: 978-84-9717-323-0

Aquellas soluciones que más seguridad ofrecen como son los mecanismos de autenticación y autorización basados en el uso de token hardware [10] proponen soluciones de seguridad frente a todas las amenazas listadas anteriormente. Sin embargo, adolecen de una baja usabilidad y su coste de implementación es muy alto. En este artículo se propone una solución de seguridad que propone un nivel de seguridad comparable a estos token hardware pero sin menoscabar su usabilidad y simplificando la complejidad de su adopción por los proveedores de los servicios.

II. Paradigma de la reducción del tiempo de exposición

La mayoría de los modelos de seguridad en los que se basan las soluciones existentes realizan una serie de asunciones para determinar cuál es el escenario en el que se propone su utilización. Es frecuente encontrar asunciones que consideran que los atacantes dispondrán de recursos infinitos para la implementación de sus ataques. Estos recursos son los medios materiales y el tiempo de los que podrán disponer para vulnerar las medidas de seguridad. En base a esta asunción es posible hacer una estimación relativa a qué amenazas se pretende hacer frente cuando se propone una medida de seguridad.

La idea principal de este trabajo se centra en proponer una propuesta que complemente a los sistemas de autorización y autenticación actuales, por tanto el cambio pudiera ser inmediato y no abrupto, centrándose en el paradigma de la reducción del tiempo de exposición. Si se limita los recursos que un atacante puede aplicar para vulnerar las medidas de seguridad (autenticación y autorización) se debería minimizar el robo de identidades. El tiempo de exposición que un sistema de autorización y autenticación está expuesto a un atacante, cuando un usuario legítimo no tiene intención de autenticarse, es crítico. Analíticamente esta propuesta puede razonarse de la siguiente forma:

Si se define la relación entre el éxito (o fracaso) de un ataque a un sistema de autenticación y el tiempo en que este sistema está accesible (tiempo de exposición) como una probabilidad condicionada $p(SuccessfulAttack—exposed)$ es posible cuantificar el riesgo relativo RR como 1:

$$RR = \frac{p(SuccessfulAttack|exposed)}{p(SuccessfulAttack|unexposed)} > 1 \qquad (1)$$

Es decir, asumimos que existe una relación directa entre la probabilidad de éxito de un ataque sobre un sistema y la exposición de este sistema. Nuestra intuición nos lleva a plantear la hipótesis de que esta probabilidad será menor si existe una reducción en esta exposición que si no se adopta ninguna medida que reduzca dicha exposición. Si, intuitivamente, podemos considerar esta hipótesis como válida, del razonamiento anterior se puede deducir la siguiente expresión 2:

$$OR = \frac{\frac{p(SuccessfulAttack|exposed)}{p(FailedAttack|exposed)}}{\frac{p(SuccessfulAttack|unexposed)}{p(FailedAttack|unexposed)}} > 1 \qquad (2)$$

La ecuación 2 refleja el *odd ratio (OR)* que mide la probabilidad condicionada en el comportamiento de dos grupos, que en esta argumentación están formados por aquellos ataques en los que no hay límite en el tiempo en el que los objetivos del ataque son accesibles y los ataques que si encuentran restricciones en la exposición de estos servicios. Si se considera que OR>1 entonces se puede concluir que existe una mayor probabilidad de éxito de ataque si existe un sistema expuesto continuamente. A partir de este punto, puede deducirse el porcentaje de riesgo atribuible (*attributable risk percentage, ARP*) a la reducción de la exposición de los sistemas, ecuación 3, que indica qué porción de ataques exitosos podrían ser evitados (independientemente del sistema de autorización que utilice un proveedor de servicios) si se minimizara la exposición en relación con todos los casos.

$$ARP = \frac{RR - 1}{RR} \qquad (3)$$

Esta expresión 3 permite estimar, conocido RR, si la inversión requerida para habilitar estos procesos encaminados a reducir el tiempo de exposición es aceptable o no, en comparación con el riesgo a sufrir un ataque y el daño que este ataque puede producir (ARP). La experiencia profesional y el conocimiento técnico de las técnicas de ataque a los sistemas protegidos por la reducción de su exposición, confirman la asunción inicial de que el riesgo relativo es mayor que 1. Las ecuaciones anteriores reflejan claramente la utilidad de incorporar estos principios a los sistemas de autenticación/autorización actuales. No obstante todavía quedan una serie de preguntas en el aire que no es posible resolver sin experimentación:

1. Cómo de costoso/complejo sería implantar este concepto en sistemas de autorización actuales. Entendiendo que el sistema, como tal, no se modifica si no que se le proporciona una capa extra que gestione esta característica.

2. Usabilidad. Por definición un sistema de autenticación es un entorno incómodo para un usuario, es algo que se interpone entre él y los servicios que desea consumir lo más rápido y fácil posible. ¿Supone algún inconveniente esta capa extra de seguridad?

3. Mitigación/utilidad. Por desgracia, no es sencillo estimar de manera específica y pormenorizada el impacto de este tipo de mecanismos en el fraude y vulneración de mecanismos de protección actual en Internet. Existen multitud de informes globales (medidas reales pero agregadas) pero es difícil conocer valores reales para evaluar si un mecanismo de seguridad concreto mejora o no la situación actual en la protección de identidades digitales.

En los siguientes apartados, mediante experimentación, se podrá obtener algunas medidas reales de la utilización de este paradigma en escenarios reales y estimar con mayor precisión

su utilidad si fuera adoptada en el mercado.

III. Pestillos digitales. Minimizar el tiempo de exposición con Latch

La aplicación del paradigma de la reducción de tiempo de exposición a sistema de autenticación en escenarios reales se podría aplicar de diferentes formas. Nuestra propuesta se centra en la utilización del concepto de pestillos (latch, en inglés) digitales, este concepto, como se verá posteriormente, introduce una serie de ventajas notorias en términos de seguridad, anonimato, usabilidad y transparencia. El concepto de pestillo digital es sencillo de entender con un símil cotidiano. Cuando una familia está en su casa además de cerrar la cerradura utilizando sus llaves podría instalar un cerrojo/pestillo que podría utilizar para proporcionar mayor seguridad a su puerta. Las ventajas que introduce esto son las siguientes:

1. La seguridad no depende de las llaves que tenga la familia y que un atacante podría haber duplicado o robado una copia.
2. El pestillo es una capa extra. El usuario decide cuándo está activo o no (tiempo de exposición) no interfiriendo en la forma en la que se implementa la seguridad por parte de un fabricante de sistemas de autenticación (en nuestro caso, la puerta o la seguridad de la cerradura de la misma). Como se verá posteriormente el proveedor de servicios podría considerar o no este pestillo, esto da garantía absoluta de que un gestor de un sistema de autenticación tiene el control del sistema independientemente del estado del pestillo digital.
3. El sistema es muy sencillo. En su generalización a servicios digitales facilitaría homogenizar la seguridad de diferentes cuentas digitales (identidades) con uno o pocos pestillos digitales. Esto ofrece un nivel de seguridad comparable al nivel 4 definido por el NIST [10].

El concepto de pestillo digital se ha llevado a la práctica en el desarrollo de la arquitectura Latch. En esencia, la arquitectura propuesta tiene dos fases: el pareado de cuentas y el modo de operación. El pareado de cuentas (1) supone vincular, sin que ello suponga niguna pérdida de privacidad por parte del usuario, una cuenta de un proveedor de servicios con una cuenta de un usuario de Latch. Información detallada puede encontrarse en [11], esta arquitectura puede resumirse de la siguiente forma:

1. El proveedor de servicios que utiliza un sistema de autenticación determinado podrá disponer de una capa extra (pestillo digital). Esta información la recibirá por un canal específico con las protecciones adecuadas (confidencialidad, integridad y autenticidad). Para facilitar la integración de Latch con la arquitectura del proveedor de servicios se proporcionan SDKs en diferentes lenguajes (.net, ruby, .c, python, php, java, dotnetnuke) así como múltiples plugins (drupal6, drupal7, joomla, prestashop, redmine, wordpress, openvpn, ssh, roundcube, squirrelMail) [11].
2. Latch no interfiere en la forma en que un sistema de autenticación/autorización toma sus decisiones, por tanto el sistema podría obviar esta información. No parece razonable que si implementa esta capa ignore el pestillo definido, no obstante se habilita esta característica para que si existiera algún problema a la hora de recibir la información del pestillo (por ejemplo en un entorno de tiempo real limitado a una respuesta antes de 2 milisegundos) pudiera decidir qué hacer con la autorización concreta de un usuario, permitir acceso o no. Tal es la flexibilidad que actualmente ya existen proveedores de cierta relevancia que utilizan Latch: Telefónica, Movistar, Acens, Tuenti, Grupo Cortefiel, Cajamar, Universidad de la Rioja o la Universidad de Salamanca.
3. La gestión de los pestillos digitales se traslada a una aplicación móvil (disponible para android, iphone, windows mobile y firefox os) [12]. Acercando el control de la identidades digitales al usuario. El usuario mediante la aplicación movil podrá vincular uno o más pestillos con la autenticación de servicios/operaciones concretas de un proveedor. Por tanto, el usuario solo tendrá que hacer ON/OFF en sus pestillos y el proveedor de servicios solo necesitará consultar el estado de los mismos antes de proceder a la autenticación.

Figura 1: Proceso de pareado de cuentas con Latch

Una vez que se ha completado el proceso de pareado de cuentas, el usuario está en disposición de poder determinar cuál es el nivel de exposición de los servicios y operaciones proporcionadas por el proveedor con quien ha contratado los servicios (figura 2). Cuando un usuario solicita alguna de estas

operaciones (e.g. el login en el servicio), el proveedor, que habrá integrado en la lógica de sus sistemas las llamadas básicas que aseguran la lógica de la interacción con Latch, solicitará el estado en el que el usuario en cuestión había decido que, en ese instante, se encontrara la operación. El servidor de Latch recuperará el estado de esta operación y se la devolverá al proveedor. Si el estado de esta operación fuera *bloqueado*, el proveedor podría deducir que está ante un intento fraudulento de acceso y actuar en consecuencia.

Con todas estas características queda claro que es posible diseñar una solución basada en el paradigma de la reducción del tiempo de exposición, enmascarando la complejidad de la plataforma, simplificando su uso y minimizando el coste/tiempo tanto a usuarios como a proveedores. Del mismo modo son notorios aspectos de flexibilidad de la propuesta. Algunos de ellos son:

1. Configuración de políticas de gestión de identidades basadas en múltiples parámetros: tiempo, geolocalización, etc.
2. Delegación del acceso a sus cuentas a otros usuarios. Por ejemplo, sería útil para control parental.
3. Monitorización por parte del usuario de accesos basado en robo de identidad. Permite tomar contramedidas frente al posible robo de claves de acceso.
4. One-time use. Los servicios pueden configurarse para que se habiliten cuando el usuario se autentica pero inmediatamente después no permita autenticarse de nuevo por un atacante que tuviera las claves. Esto lleva al extremo la protección basada en mínimo riesgo de exposición.

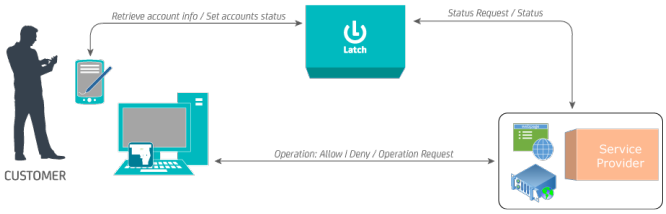

Figura 2: Arquitectura propuesta para garantizar la reducción del tiempo de exposición

En este punto, se puede observar que mediante el diseño y desarrollo de la arquitectura Latch es viable aplicar el paradigma de reducción de tiempo de exposición a entornos reales con sistemas de autenticación variados. Demostrando como estas propuestas pueden adaptarse rápidamente a servicios actuales.

Para concluir nuestra investigación, cubierto ya la investigación analítica y el entorno de experimentación, presenta interés analizar datos reales de cientos de usuarios, a modo de ejemplo, en un CMS (Content Management System) real, así como analizar tendencias en el uso de nuevos mecanismos de seguridad basados en el paradigma que implementa Latch.

IV. Ejemplos de uso

IV-A. Ejemplos de uso en un CMS (CONTENT MANAGEMENT SYSTEM)

En la actualidad la plataforma Latch tiene 4 meses de vida y aunque es un período corto ya cuenta con más de 600 integradores (proveedores de servicios) y miles de usuarios registrados. En la situación actual es posible estudiar una serie de comportamientos relacionados con el uso de los sistemas de autenticación. En esta investigación se centra el foco en el servicio en producción que más usuarios tiene actualmente Latch. Estamos hablando en concreto del Content Management System Joomla [13]. Joomla es un Sistema de gestión de contenidos que permite desarrollar sitios web dinámicos e interactivos. Permite crear, modificar o eliminar contenido de un sitio web de manera sencilla a través de un panel de administración. Latch protege las cuentas de usuarios en su autenticación (independientemente su rol). Joomla tiene pareados 24797 usuarios, lo cual es una cantidad razonable para extraer alguna conclusión real sobre el uso del paradigma de reducción de tiempo de exposición en usuarios reales.

En primer lugar puede observarse como en el 22 % de las solicitudes han intentado accesos ilegítimos (con credenciales válidas). Este acceso ha sido bloqueado dado que el bloqueo estaba activo, el usuario legítimo fue notificado de dicha circunstancia. Del mismo modo se detecta que el 69 % de los usuarios han configurado alguna opción de autobloqueo (temporizador para cerrar cerrojo si abierto), así como existe un número menor de usuarios, un 17 % que desea aprovechar características extras de Latch y utilizarlo como un canal de segundo factor (OTP). Cada vez que alguien se autentique en la web y el cerrojo está abierto se solicitará introducir una clave de un solo uso enviado al móvil del usuario original.

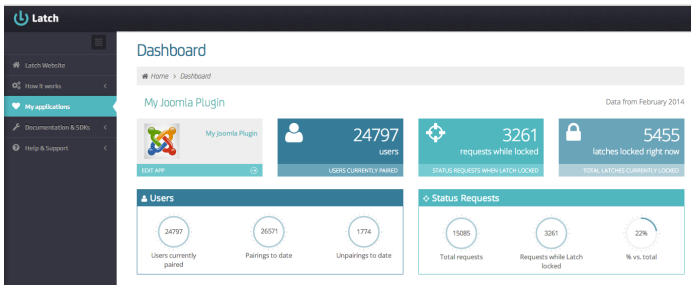

Figura 3: Panel de control simplificado de Latch

IV-B. Ejemplo y tendencias en protección frente a fraude bancario

Es difícil cuantificar el efecto de aplicar una medida de seguridad como es Latch. Aunque si bien es cierto que permite devolver al usuario la sensación de control sobre su vida digital, es complicado trasladar esta sensación a una métrica cuantitativa. Por otro lado, aunque su aplicación sí ofrecería resultados medibles desde la perspectiva de los integradores de esta tecnología, por ejemplo, en términos de prevención del fraude, las políticas de privacidad de las compañías, que

Tabla I: Impacto de Latch en las pérdidas por fraude CNP

	Q4 - 2013	Q1 - 2014	Q2 - 2014	Q3 - 2014	Q4 - 2014	Q1 - 2015	Q2 - 2015	Q3 - 2015	Q4 - 2015
A	0,00012	0,05087	0,1016	0,1524	0,2031	0,2539	0,3046	0,3554	0,4061
B	47779	20804529	41561279	62318029	83074779	103831529	124588279	145345029	166101779
C	$2{,}29{\cdot}10^{8}$	$9{,}99{\cdot}10^{10}$	$1{,}99{\cdot}10^{11}$	$2{,}99{\cdot}10^{11}$	$3{,}99{\cdot}10^{11}$	$4{,}98{\cdot}10^{11}$	$5{,}98{\cdot}10^{11}$	$6{,}98{\cdot}10^{11}$	$7{,}97{\cdot}10^{11}$
D	$2{,}9347{\cdot}10^{-2}$	$2{,}8500{\cdot}10^{-2}$	$2{,}7653{\cdot}10^{-2}$	$2{,}6806{\cdot}10^{-2}$	$2{,}5960{\cdot}10^{-2}$	$2{,}5113{\cdot}10^{-2}$	$2{,}4266{\cdot}10^{-2}$	$2{,}3419{\cdot}10^{-2}$	$2{,}2572{\cdot}10^{-2}$
E	$6{,}73{\cdot}10^{4}$	$2{,}85{\cdot}10^{7}$	$5{,}52{\cdot}10^{7}$	$8{,}02{\cdot}10^{7}$	$1{,}04{\cdot}10^{8}$	$1{,}25{\cdot}10^{8}$	$1{,}45{\cdot}10^{8}$	$1{,}63{\cdot}10^{8}$	$1{,}80{\cdot}10^{8}$
F	43,02	42,60	42,40,48	34,18	43,77	47,55	43,06	47,71	49,32
G	$2{,}90{\cdot}10^{4}$	$1{,}21{\cdot}10^{7}$	$2{,}34{\cdot}10^{7}$	$2{,}74{\cdot}10^{7}$	$4{,}53{\cdot}10^{7}$	$5{,}95{\cdot}10^{7}$	$6{,}25{\cdot}10^{7}$	$7{,}79{\cdot}10^{7}$	$8{,}88{\cdot}10^{7}$

apuestan por el uso de Latch, hacen imposible la publicación de esta información. Por ello, y para finalizar este artículo, se presenta una simulación que pretende estimar a cuánto podría ascender la cantidad prevenida de ser defraudada en caso de que se apostara por Latch como medida de protección de uno de los tipos de fraude que más impacto ha tenido en los últimos tiempos. En [14] se justifica una tendencia descendente en la cantidad defraudada por el uso fraudulento de tarjetas de crédito. A pesar de ello la cantidad absoluta perdida debido a esta lacra en 2013 ha sido próxima 1030 millones de euros. Esta cantidad se divide en tres tipos de fraude que tienen que ver con estas tarjetas: fraude relacionado con los procesos en los que no es posible la comprobación de que efectivamente se está en posesión de la tarjeta (Card Not Present (CNP)) (e.g. procesos de compra por Internet), fraude derivado de su utilización en terminales punto de venta (Point Of Sale (POS)) sin supervisión y derivado de su uso en cajeros automáticos (Automatic Teller Machine (ATM)). Para este estudio concreto, se propone el uso de Latch como medida mitigadora del fraude CNP. Se trata de un escenario en el que la necesidad de comprobar que quién está solicitando una operación es quien dice ser, hoy por hoy, no se ha resuelto eficientemente. Con Latch, y gracias al canal extra de seguridad que facilita, es posible, a día de hoy, demostrar que quién está solicitando la operación, al menos, conoce las credenciales de acceso a Latch.

Para poder estimar en qué medida la implantación de Latch puede suponer un beneficio para, en este caso, las entidades bancarias que emitan tarjetas para sus clientes es necesario modelar la adopción de una nueva tecnología. Para esta labor se han utilizado las métricas propuestas por la International Telecommunication Union [15] para estimar la evolución en la madurez tecnológica de distintas regiones. Esta madurez mide diferentes aspectos de las sociedades tecnológicas, entre los cuáles están el acceso a las nuevas tecnologías y la formación en su uso adecuado. Se ha trasladado la tendencia definida en el informe [16] a la forma en que podría comportarse el número de usuarios de Latch en los países de Europa occidental y se han fijado las condiciones iniciales en el número de usuarios que existen ya para Latch en el primer cuarto de 2014 y el porcentaje de la población de Europa Occidental (409000000 habitantes) que posee un smartphone (56 %). En la fila A de la tabla I, se indica cuál es el porcentaje de adopción esperado de Latch a lo largo del año 2014. En la fila B se traduce este porcentaje al número de usuarios esperados de Latch. Además, en esta adopción, se han considerado una serie de perturbaciones para modelar las fluctuaciones debidas a condicionantes externos (noticias, etc) sobre los gustos de los usuarios. Así, a partir de los usuarios registrados durante el primer cuarto del año 2014 (50000 usuarios de Latch), es posible estimar cuál será el número de usuarios de Latch durante un año. En la fila C se establece la cantidad movida por usuarios de Latch usando sus tarjetas. A partir de este valor, y usando los datos de los informes mencionados, es posible determinar la evolución del fraude en relación con el aumento de transferencias (fila D) y la cantidad defraudada por fraude de tarjetas por usuarios de Latch (fila E). A partir de esta información ha sido posible estimar cuál será la evolución del fraude CNP (fila F) y, por último, el ahorro esperado por el uso de Latch en la fila G.

V. Conclusiones

La presente investigación pone de relieve la problemática actual de la gestión de identidades digitales en Internet. Aunque muchas propuestas se han realizado, entre ellas esfuerzos notorios en esquemas de federación de identidades, hoy día no existe una propuesta definitiva que sin irrumpir bruscamente en cambios a los sistemas de autenticación actuales (y en funcionamiento) proporcione cierta seguridad extra, sea usable y el coste de implementación sea asumible (debe pensarse que en el peor de lo casos se compite con un sistema ampliamente difundido y de bajo coste como es el par usuario-contraseña).

Nuestra propuesta introduce de manera innovadora el concepto de pestillo digital y lleva a la práctica en una plataforma real, Latch, que aunque con pocos meses de vida está siendo utilizada por miles de usuarios. Se analizan datos reales en un escenario de ejemplo y se compara con diferentes estudios globales con el fin de demostrar la viabilidad de aplicar el concepto de reducción del tiempo de exposición a la protección de las identidades digitales.

Referencias

[1] Shibboleth, https://shibboleth.net/

[2] openID Foundation, http://openid.net/

[3] M. Urueña, A. Muñoz, D. Larrabeiti, “Analysis of privacy vulnerabilities in single sign-on mechanisms for multimedia websites”. *Multimedia Tools and Applications 2014*, Volume 68, Issue 1, pp 159-176. Doi: 10.1007/s11042-012-1155-4.

[4] SsplashData, “The 2013 list of worst passwords”, http://splashdata.com/press/worstpasswords2013.htm

[5] Visa, “Visa Europe 2013 Annual Report Enabling new commerce and delivering growth”, http://annualreport.visaeurope.com/downloads/visa_ar2013_complete.pdf

[6] D. Charoen, "Password Security". *International Journal of Security (IJS)*, Volume (8): Issue (1):2014
[7] M. Raza, M. Iqbal, M. Sharif, W. Haider, "A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication". *World Applied Sciences Journal* 19 (4): 439-444, 2012. ISSN 1818-4952; DOI: 10.5829/idosi.wasj.2012.19.04.1837
[8] S. Komanduri, R. Shay, P. Gage, ;. Mazurek, L. Bauer, N. Christin, L. Cranor, S. Egelman, "Of Passwords and People: Measuring the Effect of Password-Composition Policies". CHI 2011, May 7-12, 2011, Vancouver, BC, Canada
[9] J. Bonneau, C. Herley, P. Oorshot, F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes". *In Security and Privacy (SP), 2012 IEEE Symposium* on (pp. 553-567). IEEE.
[10] W. Burr, D. Dodson, E. Netwon, R. Perlner, W. Timothy, S. Gupta, E. Nabbus, "NIST Special Publication 800-63-1. Electronic Authentication Guideline", December 2011. http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf
[11] Latch, "Tu interruptor de seguridad digital". https://latch.elevenpaths.com/www/index.html
[12] ElevenPaths, "Latch. Añade un nivel adicional de protección a tus servicios digitales". http://goo.gl/ksXfm7
[13] Joomla, "Content Management System", http://www.joomla.org/
[14] European central bank, "Second Report on card fraud", july 2013. https://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201307en.pdf
[15] International Telecommunication Union, http://www.itu.int/
[16] Measuring the information Society 2012, http://goo.gl/iW1yWt