La gestione delle password. Strumenti disponibili e OpenID.

*Antonio De Martino**

Dalla nascita di Internet il problema dell'identità digitale si è evoluto moltissimo, soprattutto grazie all'introduzione del commercio elettronico che ha raggiunto cifre molto significative e ad oggi non accenna a diminuire la sua crescita. Inizialmente infatti il processo di autenticazione e di identificazione di un utente era limitato ad un numero piuttosto ristretto di persone, provenienti dall'ambiente universitario o addetti ai lavori, per un ambito molto limitato di servizi (come per esempio la posta elettronica).

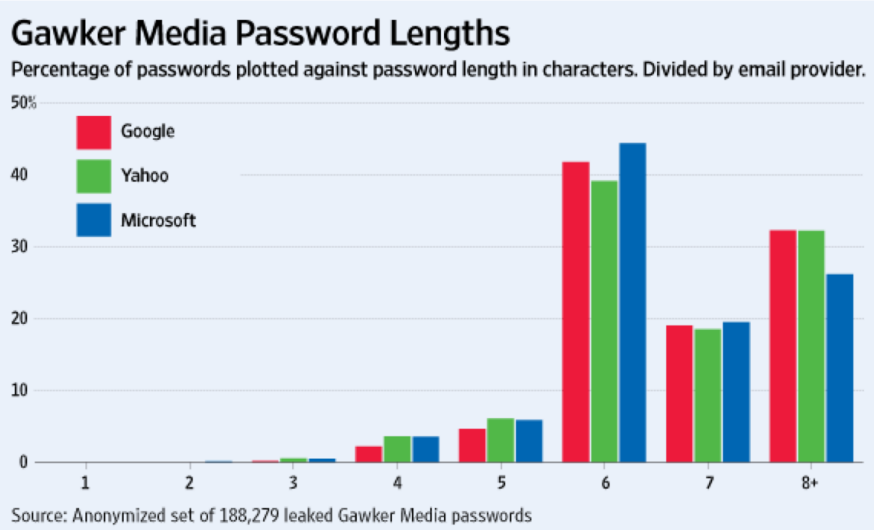
È proprio l'esplosione della disponibilità di servizi che ha alimentato la crescita di Internet e ne ha permesso la diffusione a un pubblico su larga scala, di diversa estrazione culturale e sociale. Dai customer care online delle aziende, all'internet banking fino ai più recenti social network e alle applicazioni "mobile", che hanno cambiato l'approccio ai dispositivi portatili e al mondo della rete. La complessità del problema dell'identificazione si amplifica quando il riconoscimento dell'utente deve avvenire su vari canali garantendo agli utilizzatori un adeguato livello di usabilità, soddisfazione e sicurezza.

Ciononostante, ad oggi il metodo più utilizzato per l'autenticazione rispecchia ancora il modello iniziale che prevede l'inserimento da parte dell'utente di qualcosa che conosce, ovvero la coppia identificativo e parola chiave note come *username* e *password*.

Il metodo delle password non costituisce una buona forma di autenticazione per vari motivi, queste sono certamente facili da usare, ma sono altrettanto facili da rubare.
Le password possono essere sottratte con tecniche di social engineering, tramite phishing, con un trojan o un malware nel computer, oppure possono essere intercettate se trasmesse su canali in chiaro o recuperate dai sistemi se memorizzate in maniera non sicura. L'incuria, le misconfigurazioni o i bug espongono, infatti, i sistemi che conservano i dati (e le password) a rischi d'intrusione e di furto.

C'è poi da considerare il fenomeno del riutilizzo delle credenziali e della scarsa complessità nella loro scelta. Spesso si è inclini all'inserimento della stessa parola chiave per vari servizi (es. posta elettronica, blog, social network, ecc.) e il più delle volte si tratta di termini comuni e facili da ricordare, come potrebbe essere la propria data di nascita. La sottrazione quindi o addirittura il *guessing* (indovinare) di una sola di esse potrebbe compromettere svariate identità digitali.
Per avere un'idea di quanto le password siano spesso troppo deboli, basti pensare al furto di password avvenuto nel Dicembre 2010 alla Gawker Media[1] (una media company online). Dai dati analizzati, è emerso che la password più comune era *123456* che quasi sempre corrisponde alla lunghezza e alla complessità minima richiesta dai sistemi di autenticazione.

[1] http://blogs.wsj.com/digits/2010/12/13/the-top-50-gawker-media-passwords/



Fonte: The Wall Street Journal Blog[2]

In base ai dati gestiti e alle informazioni da proteggere, i sistemi possono adottare meccanismi di autenticazione e gestione delle password più o meno complessi. Le principali caratteristiche che devono avere i sistemi informatici che trattano dati personali sul territorio italiano, sono contenute nell'allegato tecnico[3] del decreto legislativo 196/03 cit. [..] *5.La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi. [..]*

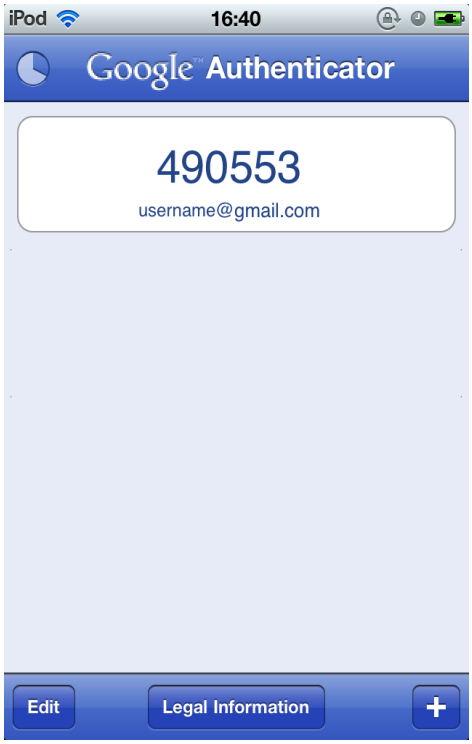
Lo scorso 6 Giugno anche il famoso social network Linked-In ha subito un furto di dati[4] ad opera di cyber criminali che hanno rubato e pubblicato su un sito internet russo circa 6,5 milioni di password cifrate. Purtroppo la contromisura adottata per la memorizzazione sicura delle password è risultata insufficiente ed ha permesso agli esperti di risalire facilmente alle password originarie partendo dalle codifiche dei dati rubati.

In generale un processo di autenticazione fa riferimento a tecniche classificabili in tre categorie, qualcosa che si conosce (es. parola chiave), qualcosa che si possiede (es. Token, telefono) e qualcosa che si è (es. impronte digitali). L'utilizzo congiunto di due di questi fattori tra loro indipendenti (es. parola chiave e token) costituisce un'autenticazione forte, detta *strong authentication*.

La strong authentication è il metodo utilizzato da molte banche per proteggere l'accesso dei propri clienti ai servizi disponibili online, ma di recente impiegato anche dai grandi service provider per il

[2] http://blogs.wsj.com/digits/2010/12/13/the-top-50-gawker-media-passwords/
[3] http://www.garanteprivacy.it/garante/doc.jsp?ID=1557184
[4] http://press.linkedin.com/node/1212

rischio crescente di violazioni da parte di malintenzionati. Google, infatti, utilizza un'applicazione gratuita chiamata Google Authenticator[5] per realizzare l'autenticazione forte per l'accesso ai suoi servizi (es. Gmail, Google+, Google Site, ecc.). Il software è disponibile per l'installazione su vari modelli di telefono cellulare e dispositivi mobili ed è semplice da configurare. Se non si dispone di uno smartphone è possibile utilizzare gli sms per implementare la "verifica in due passaggi". Ad ogni accesso, infatti, viene recapitato un sms con una password casuale da utilizzare come secondo fattore di autenticazione. La password casuale può essere utilizzata una sola volta, per questo si definisce OTP (one time password) e il dispositivo mobile rappresenta qualcosa che si possiede, dall'Inglese *something you have*.



I meccanismi di strong authentication descritti avrebbero reso parzialmente utilizzabili i dati rubati a Linked-In ed impedito il massiccio cambio password suggerito a tutti i suoi utenti, ma comportano l'utilizzo di un dispositivo aggiuntivo (telefono o token), non sono ancora diffusi per tutti gli ambiti ed in ogni caso non risolvono il problema della gestione di un numero sempre crescente di credenziali d'accesso ai servizi cui esse sono associate.

Programmi come *Password Safe*[6]*,* per i sistemi Microsoft, e *Keychain Access* per i sistemi Apple, realizzano una sorta di portachiavi elettronico dove conservare in maniera sicura (e successivamente recuperare) le proprie credenziali di autenticazione. Rimane il fatto che, per quanto queste siano correttamente custodite, sono conosciute dall'utente e quindi suscettibili di attacchi del tipo phishing. Se il browser generasse automaticamente la password, l'utente non sarebbe in grado di ricordarla e anche il problema del phishing, sotto questo aspetto, potrebbe essere risolto.

La soluzione di Google al problema, ancora in in fase di studio[7], dovrebbe sfruttare le funzionalità offerte da Chrome in combinazione con *OpenID.*[8]

[5] https://www.youtube.com/watch?feature=player_embedded&v=zMabEyrtPRg
[6] http://passwordsafe.sourceforge.net/
[7] https://sites.google.com/a/chromium.org/dev/developers/design-documents/password-generation
[8] http://openid.net/wordpress-content/uploads/2011/03/Introduction-to-OpenID-Foundation-March-2011.pdf

OpenID è una tecnologia che serve per effettuare il login nei siti web con un identificativo unico. In questo modo non si dovranno gestire e conservare le password di tutti i servizi a cui si è registrati, ma soltanto di un'unica identità che permetterà l'accesso ovunque ci sia OpenID, una sorta di sistema di identity management globale.

Fu sviluppato nel 2005 da una piattaforma di blogging americana, LiveJournal, per consentire ai propri utenti di inserire commenti su tutti i blog del circuito. La comunità di sviluppatori che si occupava di tecnologie per l'identità digitale si interessò al progetto e in breve tempo, grazie soprattutto al lavoro di numerosi sviluppatori web, nel 2006 venne proposta una prima bozza del protocollo che avrebbe permesso di integrare OpenID con qualsiasi sistema esistente di gestione delle utenze.

Nel 2007 con il supporto di aziende come Symantec, Microsoft, VeriSign, AOL e SUN Microsystem, fu fondata la "OpenID Foundation", organizzazione senza fini di lucro, per gestire il marchio OpenID e diffondere lo standard.
I maggiori service provider come Google, Facebook, collaborano già dal 2009 con la fondazione OpenID per integrare questa tecnologia nei propri sistemi. In Italia il portale Virgilio è stato il primo ad utilizzare OpenID.

Nonostante gli sforzi per renderla una tecnologia sicura, anche OpenID potrebbe essere esposta ai rischi di attacco da parte di malintenzionati. Il furto di dati avvenuto ai danni della società RSA[9] nella prima metà del 2011 e gli attacchi condotti contro alcune Certification Authority nello stesso periodo (es. Diginotar[10]) dimostrano che i sistemi possono essere attaccati e violati nonostante implementino sofisticati modelli di sicurezza. È importante quindi diffondere la cultura della sicurezza informatica in modo che gli utenti e le organizzazioni siano preparati a talune dinamiche e pronti ad affrontarle adottando i comportamenti corretti per utilizzare al meglio le soluzioni disponibili.

Riferimenti

https://sites.google.com/a/chromium.org/dev/developers/design-documents/password-generation
http://blogs.wsj.com/digits/2010/12/13/the-top-50-gawker-media-passwords/
http://www.garanteprivacy.it/garante/doc.jsp?ID=1557184
https://www.youtube.com/watch?feature=player_embedded&v=zMabEyrtPRg
http://passwordsafe.sourceforge.net/
http://openid.net/wordpress-content/uploads/2011/03/Introduction-to-OpenID-Foundation-March-2011.pdf
http://www.rsa.com/node.aspx?id=3872
http://www.diginotar.nl/
http://press.linkedin.com/node/1212
http://pastebin.com/5pjjgbMt

L'ing. Antonio DE MARTINO è laureato presso l'Università degli studi di Napoli Federico II in Ingegneria Informatica con tesi sull'Enterprise Application Integration. Si è occupato di progettazione di infrastrutture ICT sicure, hardening e sicurezza di apparati di rete, di piattaforme per l'identity management e controllo accessi. Oggi si occupa di sicurezza delle informazioni e project management di architetture di sicurezza informatica.

[9] http://www.rsa.com/node.aspx?id=3872
[10] http://www.diginotar.nl/