PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 19 - numero 4120 di lunedì 13 novembre 2017

Si chiama FIDO, è affidabile e sicuro, ma non è un cane!

Un nuovo protocollo standardizzato con autentica a due fattori potrebbe risolvere, per parecchi anni a venire, il problema della protezione dell'identità informatica di un utente.

I lettori sono certamente al corrente della differenza che vi è tra un protocollo di autentica ad un fattore, come ad esempio una parola chiave, ed un protocollo di autentica a due fattori. Quest'ultimo è un processo di sicurezza nel quale l'utente fornisce due fattori di autentica per verificare la propria identità.

Per solito si può utilizzare una parola chiave, abbinata ad un dispositivo elettronico, che fornisce un ulteriore elemento di identificazione. Il dispositivo elettronico può essere incorporato in una chiave USB o in una applicazione, che genera parole chiave utilizzabili solo una volta.

Il motivo per cui sino ad oggi i sistemi di autentica a due livelli non sono ancora molto diffusi è legato al fatto che l'autentica ad un solo fattore ha il vantaggio di essere oltremodo pratica da utilizzare, ma l'aumento dei profili di accesso, di cui ha oggi ha bisogno di un utente, sta rendendo sempre meno pratica questa soluzione.

Durante uno studio recentemente condotto nel Regno Unito, è stato rilevato che un utente medio britannico dispone di 25 profili di accesso, mentre una persona di giovane età, compresa tra i 25 34 anni, ne ha più di 40.

A questo punto appare evidente che una soluzione scelta dall'utente è spesso quella di utilizzare la stessa parola chiave per accedere a numerosi conti, con le criticità evidentemente connesse, mentre la seconda soluzione è quella di utilizzare una procedura di autentica a due fattori.

Per gestire la mancanza di interoperabilità fra le tecnologie disponibili a due livelli di autentica, nel luglio 2012 alcune grandi aziende mondiali si sono unite fondando la Fast Identity on line Alliance ? FIDO.

Alla fine del 2014 è stata pubblicata la prima norma, che ha cercato di superare i problemi di usabilità, senza sacrificare la sicurezza.

Questa norma non è stata sviluppata per una specifica tecnologia di autentica. Essa separa il server di autentica dal modello specifico di autentica. Ciò significa che il metodo di autentica o il provider possono essere cambiati senza intervenire sull'applicazione. L'utente viene autenticato utilizzando due procedure:

- passwordless UX, che usa il quadro di riferimento universale di autentica ? UAF, e
- il secondo fattore UX, che usa il protocollo universale per il secondo fattore, chiamatoU2F.

Ricordo ai lettori che l'acronimo UX significa esperienza dell'utente.

Utilizzando il primo protocollo, gli utenti devono registrare il proprio apparato in un servizio on-line, scegliendo un meccanismo locale di autentica. Può trattarsi di un meccanismo biometrico, come l'impronta digitale, il proprio volto o la registrazione di una frase detta in un microfono. Una volta registrato, l'utente ripete il processo ogni volta che deve autenticarsi ad un servizio, senza utilizzare parole chiave.

Un servizio può anche richiedere meccanismi multipli di autentica, come ad esempio un protocollo biometrico abbinato alla conoscenza di ulteriori elementi, come ad esempio una parola chiave. Il protocollo a secondo fattore invece ricorrere all'utilizzo di una parola chiave abbinata ad un hardware congruo con le specifiche FIDO.

Questo protocollo ha incontrato un favore elevato da parte di tutti coloro che sono coinvolti in procedure di autentica. Ad oggi sono ben 250 i componenti della lega FIDO e comprendono aziende ad alta tecnologia, produttori di apparati elettronici, istituzioni bancarie e istituzioni sanitarie, tutte le principali reti con carte di pagamento, molti enti governativi e dozzine di venditori di apparati di sicurezza e di tecnologia biometrica.

La commissione per il miglioramento della sicurezza informatica nazionale, voluta dal presidente Obama, ha espresso una valutazione oltremodo positiva su questo standard, condiviso anche dal governo del Regno Unito.

L'esperienza ha dimostrato che gli utenti, quando cominciano a rendersi conto del vantaggio legato al non utilizzo di parole chiave, cominciano ad adottare il protocollo con grande fiducia; anche le compagnie di assicurazione hanno evidentemente visto con grande favore la diffusione di questo protocollo.

Gli esperti di sicurezza informatica confidano che una diffusione crescente di questa procedura possa rendere sempre più difficile la vita per i criminali informatici, che certamente stanno già lavorando per trovare qualche maniera per aggirare il nuovo livello di sicurezza del sistema.

Adalberto Biasiotti