EIN PRESSWIRE

Pass the salt - Joggit mobile app redefines password security

The Joggit mobile app uses a low tech solution to the problem of generating and storing salted passwords as a primary defense against identity theft

MALAGA, SPAIN, September 4, 2016 /EINPresswire.com/ -- Whilst everyone is familiar with the process of adding salt to food to enhance its taste, not so many will be aware of a similar process used in IT to enhance security. Though the salt used in the latter has little to do with the chemical compound with which it shares a name (it's a number sequence) the net effect is actually quite similar, combining a random amount of a second component to permanently alter the identity of the first.

> You might think of Joggit as a decentralized alternative to salting a password where the randomness of the salt is provided by the mobile device in combination with raw data from the selected image.
>
> *Dean Talboys*

Unlike cases that hit the headlines involving trained programmers hacking the security of high-profile websites, most identity theft relies on the ignorance of the user in responding to illegitimate requests for information. This type of attack, where an official looking email redirects the unsuspecting user to the login page of a fake website, is nothing more than a con whereas true hacking involves accessing a website database and possibly the email and password of every registered user. However, in both cases the threat is not necessarily limited to the target website. Given the inability many people have when it comes to remembering PINs and passwords there is a tendency to reuse the same email and password to log in to every account. And who can blame us when we are faced with having to remember a word that must include upper and lower case letters, a number and a special character? Gone are the days when you could use “password” as your password! So unless the users' credentials are somehow encrypted within the database, hacking may provide access to tens of thousands of accounts across numerous websites. To make matters worse, it is the website with the least effective security that poses the greatest threat.

Salting passwords is a simple, cheap and effective way to protect user credentials. It involves four steps: generate a sequence of random numbers (the salt); combine the salt with the password entered by the user; pass the combined result through an algorithm to generate a token; store the salt and the token in the user record (but not the password). Confirming identity is then a matter of combining the salt in the user's record with the password used to log in, and comparing the token generated after passing this combination through the algorithm with that stored in the user's record.

Even if a hacker manages to access the database in one website, a token cannot be used to log in to a user's account because it would be re-salted, generating another token, and because the passwords are not stored, the hacker cannot use the information to access an account on another website – at least not so easily. It would just be a lot easier if the user could be relied upon to choose a different password for each account.

The Joggit mobile app overcomes this problem in a seamless operation that employs a photo to remind you of a password before generating the token required to confirm your identity. The app takes advantage of the thousands of numbers available within a digital photo, mapping each character on the keyboard to a random area of the image. After you have selected your photo from the gallery the corresponding numbers for each character in the word or phrase you associate with it are fed into an algorithm. In each case the result is derived from a code sent by the service provider, for example a QR code that the user scans. The resulting token can then be displayed on the mobile device and read by a webcam or barcode scanner. Both code and token can also be sent and received using SMS, Google Message Center, beacon, broadcast within the OS, or by instant messengers. It is also safe to use the same combination of image and word across all services, which can include accessing online accounts, authorizing online payments, point-of-sale transactions, ATM withdrawals, entry at a turnstile or electronic door, etc.

It is a solution that does not rely on any secure element of the hardware, operating system, SIM or SD cards and has the advantage of being compatible with any device containing a display and keyboard - not just smart phones and tablets. Simple to implement with any online account, Joggit reduces the risk of identity theft from fake websites, key-logging and hacking. The designer also claims the platform is able to provide incognito registration, identification and access to anything stored on file, including biometric data. For more information visit the website www.joggit.com.

Dean Talboys
Orderama Ltd
635304646
email us here

This press release can be viewed online at: http://www.einpresswire.com

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases.

© 1995-2016 IPD Group, Inc. All Right Reserved.