《双语：互联网联盟推新式在线身份认证》

为不同网站和设备设置不同密码并记住要消耗太多脑细胞，不少人干脆设置个简单密码或者图省事设置成同一个，但这也增加了被黑的风险。新式的在线身份认证将使用户用其他身份认证方法登录到网络和设备，这些方法包括硬件安全密钥、指纹、面部识别、虹膜扫描及其他生物特征识别解决方案。以后再也不用担心把密码搞忘了！

A new web standard is expected to kill passwords, meaning users will no longer have to remember difficult logins for each and every website or service they use.

??

The Web Authentication (WebAuthn) standard is designed to replace the password with biometrics and devices that users already own, such as a security key, a smartphone, a fingerprint scanner or webcam.

??“????”??

Instead of having to remember an increasingly long string of characters, users can authenticate their login with their body or something they have in their possession, communicating directly with the website via Bluetooth, USB or NFC.

??USB??????????????????????

“WebAuthn will change the way that people access the Web,” said Jeff Jaffe, chief executive of the World Wide Web Consortium (W3C), the body that controls web standards.

?????????????????-?????“????????????????”

One example of how WebAuthn will work is that when a user visits a site they want to log into, they input a user name and then get an alert on their smartphone. Tapping on the alert on their phone then logs them into the website without the need for a password.

??

WebAuthn promises to protect users against phishing attacks and the use of stolen credentials as there will be nothing to steal, the authentication token is generated and used once by their specific device each time the user logs in.

“????”??

“After years of increasingly severe data breaches and password credential theft, now is the time for service providers to end their dependency on vulnerable passwords and one-time-passcodes and adopt phishing-resistant FIDO Authentication for all websites and applications,” said Brett McDowell, executive director of the FIDO Alliance, one of the bodies pushing the new standard.

????????????FIDO??(??????????)????????-??????“??”

WebAuthn should also help people use unique login details for each and every service they use, instead of using the same login and password for every site, which many people still do leaving them vulnerable to further attacks if one site is hacked.

“????”??

The W3C has moved WebAuthn to what’s called the “candidate recommendation” stage – the penultimate step before it becomes an approved web standard – inviting sites and services to begin implementing it. The web standards body announced that Google, Microsoft and Mozilla had committed to supporting WebAuthn, meaning that all major web browsers short of Apple’s Safari will implement the new standard.

???????“????”????“????”??(??)????????????????????????Safari??????????????????????????

“While there are many web security problems and we can’t fix them all, relying on passwords is one of the weakest links. With WebAuthn’s multi-factor solutions we are eliminating this weak link,” said Jaffe.

?????“??”

Several sites and services already use similar methods to log in, including Google and Facebook, which can both be logged into using a USB security key. But a single cross-platform, cross-service standard ratified by the W3C will mean that many more sites and services will be able to kill the password as the defacto login method.

??USB??

WebAuthn is the culmination of many years of work and the change will not happen overnight. But as it increasingly seems inevitable that our email or other online services will get hacked into, removing the password is an important step in improving online security and making using sites and services easier.

“????”??