RISK ASSESSMENT —

This low -cost device may be the world’s best hope against account takeovers

Privacy-preserving “cryptographic assertions” are impossible to guess or phish.

DAN GOODIN - DEC 23, 2016 2:26 PM UTC

Enlarge

The past five years have witnessed a seemingly unending series of high-profile account take-overs. A growing consensus has emerged among security practitioners: even long, randomly generated passwords aren't sufficient for locking down e-mail and other types of online assets. According to the consensus, these assets need to be augmented with a second factor of authentication.

Now, a two-year study of more than 50,000 Google employees concludes that cryptographically based Security Keys beat out smartphones and most other forms of two-factor verification.

The Security Keys are based on Universal Second Factor, an open standard that's easy for end users to use and straightforward for engineers to stitch into hardware and websites. When plugged into a standard USB port, the keys provide a "cryptographic assertion" that's just about impossible for attackers to guess or phish. Accounts can require that cryptographic key in addition to a normal user password when users log in. Google, Dropbox, GitHub, and other sites have already implemented the standard into their platforms.

After more than two years of public implementation and internal study, Google security architects have declared Security Keys their preferred form of two-factor authentication. The architects based their assessment on the ease of using and deploying keys, the security it provided against phishing and other types of password attacks, and the lack of privacy trade-offs that accompany some other forms of two-factor authentication.

In a recently published report, the researchers wrote:

> We have shipped support for Security Keys in the Chrome browser, have deployed it within Google's internal sign-in system, and have enabled Security Keys as an available second factor in Google's Web services. In this work, we demonstrate that Security Keys lead to both an increased level of security and user satisfaction as well as cheaper support cost.

Other forms of two-factor authentication include the use of a cellphone to receive one-time passwords through text messages or the use of a smartphone to generate such one-time passwords. The additional password is then required when logging in. A second form involves smartcards that also provide cryptographic assertions. A third form relies on digital certificates based on the transport layer security protocol that uses a secret key to authenticate the end user to a service or account.

Using phones for two-factor authentication is problematic for a variety of reasons. For one thing, one-time passwords can often be phished using the same techniques that trick end users into revealing their normal password. Phones are also at risk of malware attacks that compromise the secrecy of one-time passwords. Using phones to receive one-time passwords through SMS text-messaging is especially risky because, in addition to all of the risks listed above, there's the threat the messages could be intercepted. Phones may not always have a signal or can run out of power, limitations that can make them unavailable for use when logging in.

Smartcards, the Google researchers said, are also problematic because they usually require custom reader hardware and the installation of driver software on any computer that will be used to log in. That makes smartcards much harder to use on a large number of devices. Also problematic: in some countries, such cards are provided by national governments, stoking concerns the cards could be used to track users' online usage.

TLS certificates used to authenticate users have been an option for years, but they have never caught on. The researchers said that's likely because they're too cumbersome for average users to generate, and TLS certificates are too likely to leak the user's identity across sites. TLS authentication certificates also reveal the user's identity to any network adversaries. What's more, they aren't portable, meaning it's difficult for average users to easily use them on multiple computers.

Security Keys, by contrast to the alternatives, provide the best mix of security, usability, and privacy. They sell for as little as $10, although some of the more popular brands—such as the U2F Security Key from Yubico—list for $18. They're smaller than a door key, plug into a computer's USB slot, and require no batteries.

Following the compromise of Hillary Clinton Campaign Chairman John Podesta's Gmail account through a simple phishing ploy, a growing number of people have realized the crucial importance of two-factor authentication. While there are a variety of ways to put it into place, the research paper makes a convincing case that

Security Keys based on the U2F standard are the best approach.

DAN GOODIN
Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001