the Availability Digest

www.availabilitydigest.com
@availabilitydig

Multifactor Authentication

September 2015

Authentication is the process of verifying that a person is who he says he is. In today's online technology, authentication of a user is usually accomplished by requiring that he log onto a system with his user name and password. However, usernames and passwords can be stolen, rendering this form of authentication risky.

The use of a username and password is a form of single-factor authentication. Only one factor is required – the knowledge of the password. The authentication process can be significantly strengthened by requiring additional identifications. This is multifactor authentication.

What Is Multifactor Authentication

Multifactor authentication (MFA) requires two or three (or in some cases more) forms of identification. Generally, two or three of the following forms of identification (factors) are required:

- Something you know (knowledge factor)
- Something you have (possession factor)
- Something you are (inherence factor) (biometrics)

A password is a form of a knowledge factor. Your zip code or national identification number (such as your Social Security Number in the U.S.) are other forms of knowledge factors.

Possession factors – something you have – could be an ATM card, a credit card, a USB stick, or a key.

Inherence factors are typically your biometrics. The most common inherence factor is fingerprints. Others might be retina scans, voice characteristics, or facial recognition.

How Secure is Single-Factor Authentication

Typical single-factor authentication (SFA) requires a username and a password. Even though this requires two items, they both belong to the same factor (knowledge) and therefore count as only one factor.

Do we really need multifactor authentication? How secure can single-factor authentication be?

A key to the answer to this question is how strong is the password? Programs exist to determine a password by brute force. A computer tries all possible combinations until it finds the password that works.

There is a website that will tell you how strong your password is. It is Random-ize and can be found at http://random-ize.com/how-long-to-hack-pass/. Some results are shown in Table 1:

	Password Length (characters)		
	6	**8**	**10**
Alpha only	1 second	1 minute 13 seconds	13 hours 48 minutes
Alphanumeric	1 second	16 minutes 33 seconds	14 days 21 hours
All characters	34 seconds	1 day 20 hours	23 years 11 months

Time to Brute-Force Guess a Password
Table 1

Clearly, the strength of the password can cover a broad range. The password “avdrtg” would take a computer less than one second to guess. The password “avdrtg$73*” would take the same computer almost 24 years to guess! The first password format has 3x10^{8} combinations. The second password format has 1x10^{18} combinations – almost ten billion more.

Single-factor authentication using usernames and passwords is the most common form of SFA because of its low cost, ease of implementation, and familiarity. No special hardware is needed. However, strong passwords can be difficult to remember, and as a result people tend to use the same password for many services. Hackers can infect systems and steal usernames and passwords, thus potentially gaining access to many services used by a single person. Once a password is stolen, it makes no difference how strong it is.

Two-Factor Authentication

Two-factor authentication (2FA) is gaining acceptance. Two-factor authentication is a security process in which the user provides two means of identification from separate categories of credentials; one is typically a physical token, such as a card (a possession factor); and the other is typically something memorized, such as a security code (a knowledge factor).

We may not be aware that we are now using two-factor authorization. Perhaps the most common 2FA usage is an ATM card. The user must be in possession of the card (possession factor) and must know its PIN (knowledge factor).

Another example is when we must provide our zip code when we are making a credit-card purchase. In either case, the system with which we are dealing can verify our knowledge factor and, in conjunction with the possession factor of the card, can be quite certain that we are the legitimate cardholder.

A major drawback to the use of a possession factor is that the token used (USB stick, bank card, key, …) must be carried around by the user at all times. If the token is lost or stolen, the user cannot authenticate himself.

Mobile Phone Authentication

An increasingly common form of 2FA uses the user’s mobile phone as the possession factor. A user will almost certainly have his mobile phone with him.

In order to use this form of 2FA, the user must have registered his phone with the service. Then, when he logs on to the service with his username and password, the service sends him a unique number (perhaps six digits in length) via SMS messaging. The user enters this number after his password to confirm to the service that he is who he says he is. The authentication has used a knowledge factor (the password) and a possession factor (the mobile phone).

One problem with mobile phone 2FA techniques is that text messages sent to mobile phones via SMS can be intercepted. This vulnerability may allow a hacker to impersonate a user and hack into his account.

Biometrics

In several Latin American countries, biometrics (inherence factors) are being used for authentication. The inherence factors are usually fingerprints. A citizen will register with a service by providing his national identification number and his fingerprints.

Then, for instance, when he visits an ATM, he has no need for a PIN. He inserts his ATM card and places a finger on a fingerprint reader pad. If his fingerprint matches, his transaction is authorized.

Fingerprint readers are available for use with desktop computers and laptops to control access to critical applications. Many smart phones today have screens capable of reading fingerprints. The phones include iPhones, Androids, and Blackberrys.

Fingerprints have several advantages over PINs. They cannot be forgotten. They cannot be lost, stolen, or cloned. However, they may require an additional hardware component.

2FA Products

There are several companies that are providing 2FA products that companies can use to incorporate two-factor authentication into their services. These include:

- RSA Security ID
- Microsoft Phonefactor
- Dell Defender (2FA and MFA)
- Google Authenticator

An RSA Security ID Key Fob

Interestingly, the RSA Security ID authentication tokens were hacked in 2011.

The PayPal Breach

In 2014, security researchers discovered a flaw in PayPal's implementation of two-factor authentication. PayPal offered 2FA on its website but not via its mobile apps. If a user wanted 2FA on the website, he signed up for it with PayPal. If the user then attempted to access his account via a mobile device, the server would halt the login process; and the user would be notified.

The researchers found that they could bypass two-factor authentication for a user who had subscribed to it. They created their own app that tricked the mobile app into thinking that it was dealing with an account that did not have 2FA enabled. Their app interfaced with two APIs provided by PayPal. One handled authentication and one handled money transfers.

When the PayPal mobile app tried to access a 2FA-enabled account, the researchers' app changed the "2fa_enabled" value in the server's response to "false." This caused the PayPal mobile app to ignore the 2FA feature and allowed it to log on to the user's PayPal account. Of course, a hacker would have had to obtain the user's username and password, perhaps through phishing.

PayPal immediately deployed a fix by disabling the ability to log on to 2FA accounts via any mobile app.

Summary

Multifactor authentication brings a great deal of additional security to applications. 2FA can drastically reduce the incidence of online fraud because stealing a victim's password will no longer be enough to support a malicious logon.

Each additional authentication factor makes a system more secure. Because the factors are independent, the compromise of one should not lead to the compromise of others

General two-factor authentication is still in its infancy in terms of mainstream online services. However, watch for it to pick up momentum as the cost of malicious activity increases.

Acknowledgements

Material for this article came from the following sources:

Two-factor authentication: What you need to know (FAQ), *cNet*; May 23, 2013.
PayPal error shows how NOT to use two-factor authentication, *CSO Online*; June 25, 2014.
Duo Security Researchers Uncover Bypass of PayPal's Two-Factor Authentication, *Duo Security*; June 25, 2014.
Two-factor authentication (2FA) definition, *TechTarget*; 2015.
Random-ize (http://random-ize.com/how-long-to-hack-pass/)
Two-step verification, *Wikipedia*.
Two-factor authentication, *Wikipedia*.