The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE...

- The Problem
- A Solution
- An Example

Two-Factor Authentication

GUEST EDITOR

Fred Kerby is the guest editor for this issue. He is a former Information Assurance Manager for the Naval Surface Warfare Center, Dahlgren Division. He is also a SANS Senior Instructor and track lead for the Intro to Information Security course (SEC301). Fred also teaches Information Security Leadership (MGT512) and Security Essentials (SEC401).

THE PROBLEM

To use many of the services on the Internet today, such as email, online banking or online shopping, you must first prove you are who you say you are. This process of proving your identity is known as authentication. Authentication is done by using something you know (such as your password), something you have (such as your smartphone), or something unique to you (such as a retinal scan or fingerprint). Traditionally, one of the most common ways of authenticating has been a username and a password. The problem with using just a password for authentication is simple: all an attacker needs to do is guess or compromise your password and they gain instant access to your online account and information. If you use the same username and password for multiple accounts, the harm can be even far greater. To better protect your online accounts, websites are moving to stronger authentication methods that require the use of more than one factor to authenticate. We will explain what this is, how it works and why you should use it.

THE SOLUTION

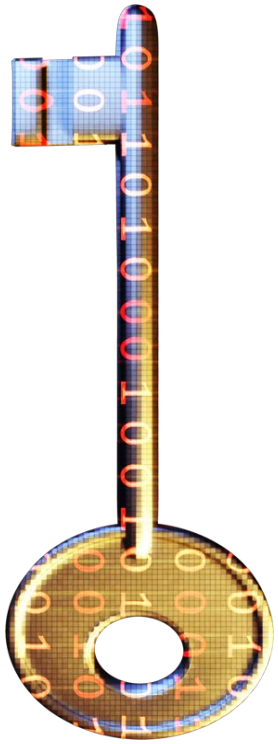
Stronger authentication uses more than one factor; not only do you have to know something like your password, but you have to have something (such as your smartphone) or present something unique to you (such as your fingerprint). Two-factor authentication is exactly what it sounds like; you need two factors to prove who you are instead of just one. A common example of two-factor authentication is your ATM card. To access your ATM you need to have

© The SANS Institute 2012

Two-Factor Authentication

something (your ATM card) and you need to know something (your PIN). If an attacker steals your ATM card, it does them no good unless they also know your PIN (which is why you never want to write your PIN on the card). By requiring two factors for authentication you are better protected as opposed to just one.

Two-factor authentication works online in a manner similar to your ATM card and PIN combination. You use your username and password when you want to access your online accounts. However, after you successfully enter the correct password, instead of going directly to your accounts the site requires a second factor of authentication, such as a verification code or your fingerprint. If you do not have the second factor then you are not granted access. This second step protects you. If an attacker has compromised your password, you and your account are still safe, as the attacker cannot complete the second step without having the second factor.



Use two-factor authentication whenever possible, it is one of the strongest ways to protect access to your accounts and information.

EXAMPLES

Let's walk through an example of how two-factor authentication can work. One of the most widely used online services is Gmail. Many people authenticate to their Gmail account or other Google services with their username and password. Google now offers improved security with two-factor authentication, or what Google calls two-step verification. Google's two-step verification requires two things for authentication: your password (something you know) and your smartphone (something you have). To prove you have your smartphone, Google will send it a one-time verification code via SMS that is unique for you (note that messaging charges may apply; check your service plan for information). You then enter the code. Also, if you prefer, instead of Google sending you the one-time verification code via SMS, you can install an app that generates the unique code for you. This way you do not even need access to your service

© The SANS Institute 2012

Two-Factor Authentication

provider, just your smartphone. The value of this stronger authentication is even if an attacker has compromised your Google password, they cannot access your Google accounts unless they also have physical access to your smartphone. You and your valuable information are protected.

Keep in mind, these verification codes sent to your smartphone are unique; they are different every time you authenticate. As such, you will have to go through this two-step process every time you have to authenticate to your Google account. In addition, this feature is not enabled by default. To enable this feature, log into your Google account, go into your Account Setting, select security and follow the options for two-step verification.

Other online sites also offer two-factor authentication, such as Dropbox, Paypal or perhaps even your bank. Some of these services may support your smartphone, while others such as PayPal, may send you a special token to generate your unique verification codes. Other sites may use special devices that plug into the USB port on your computer, such as Yubikey. If any of the services you use offer two-factor authentication, we highly recommend you enable and use it.

RESOURCES

Some of the links have been shortened for greater readability using the TinyURL service. To mitigate security issues, OUCH! always uses TinyURL's preview feature, which shows you the ultimate destination of the link and asks your permission before proceeding to it.

Google Two-Step Verification:
http://preview.tinyurl.com/cncte9n

PayPal (and EBay) Security Key:
http://preview.tinyurl.com/838dpds

Common Security Terms:
http://preview.tinyurl.com/6wkpae5

SANS Security Tip of the Day:
http://preview.tinyurl.com/6s2wrkp

BECOME A SECURITY PROFESSIONAL

Become a certified security professional from the largest and most trusted security training organization in the world at SANS 2013. Over 40 security classes taught by the world's leading experts. March 08-15, 2013 in Orlando, FL. http://www.sans.org/event/sans-2013/

OUCH! is published by the SANS Securing The Human program and is distributed under the Creative Commons BY-NC-ND 3.0 license. Permission is granted to distribute this newsletter as long as you reference the source, the distribution is not modified and it is not used for commercial purposes. For translating or more information, please contact ouch@securingthehuman.org.

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner