Multi-Step Authentication and Why You Should Use It
Multi-Step Authentication and Why You Should Use It

James Michael Stewart

Introduction
Authentication is one of the essential components of security. It is one part of the concept known as authentication, authorization, and accounting (AAA). Authentication is the process of claiming an identity then proving that you are that claimed identity. Authorization is the mechanism to control what you can access or do. Accounting is the recording of events into a log to review the activities against the rules and policies in order to detect violations or confirm compliance. All three of these should be addressed when constructing a system in order to have a reasonable foundation for reliable security.

As users of online sites and services, we have no control over the security policies and technologies implemented on those sites and services. At best, we may be offered a few authentication options. If any authentication mechanisms are available in addition to a standard password, you need to take full advantage of those benefits.

When a site or service offers authentication options, those options are usually one of the following:

- Certificate authentication
- OAuth single sign-on
- Multi-factor authentication
- Multi-step authentication

Certificate Authentication
Certificate authentication is the process of verifying identity, which involves the use of a digital certificate. A digital certificate is produced by a certificate authority (CA) using asymmetric public key cryptography. The digital certificate itself is the subject's public key signed (i.e., encrypted) the CA's private key. A digital certificate is a form of trusted third-party authentication. Its most common use is by servers (i.e., web sites) on the Internet. A web site with a digital certificate is the first party. The second party is the visiting end-user. The third party is the CA that issued the certificate to the web site. If the end-user already knows and trusts in the CA, then the end-user can trust in the identity of the web site by validating the digital certificate.

Unfortunately, most end-users do not have a digital certificate. And, even if users obtained a digital certificate from a public and respected certificate authority, most online sites and services are not configured to accept client-side certificates. When it becomes common or standard for servers to accept client-side certificates, this will be the most secure authentication option. Until then, you will likely have to use one of the other options (assuming one of them is offered/supported by a particular site).
OAuth Single Sign-On

OAuth is a type of single sign-on solution that is gaining popularity online. Single sign-on is the concept of authentication when a single logon event can be used to allow access into a collection of systems. This is different than traditional authentication where each system would require its own unique and local authentication. Single sign-on has been a standard element in company networks for decades. There have been many attempts to duplicate this concept on the Internet, but only now with the adoption of OAuth is that actually becoming a reality.

OAuth is a way to share or borrow the authentication from one site to grant access to another site. Let’s call the first site a primary site. The primary site must support OAuth and allow its authentication to be shared by other secondary sites. Secondary sites must also support OAuth and then select which primary site’s authentications they will accept. The way OAuth works is:

1. You visit a secondary site and click on an offering to use a primary site’s authentication to access the secondary site.
2. This takes you to the primary site. If you do not have a current active session with the primary site, you are prompted to authenticate to the primary site.
3. With an active session to the primary site, you are prompted to confirm or accept the secondary site’s request to link to your account on the primary site.
4. Clicking to confirm this returns you to the secondary site where you now have access to that site.

Once OAuth has been confirmed on a secondary site, all future visits to that site will automatically log you in as long as you have a current active session with the primary site. The three most common or popular sites used as primaries are Facebook, Twitter, and Google, but there are dozens of other potential primary sites as well, including Amazon, Dropbox, Evernote, Flickr, LinkedIn, Microsoft, Netflix, PayPal, Tumblr, and Yahoo. Plus, there are numerous sites supporting OAuth to function as secondary sites.

OAuth is a huge convenience for users as it reduces the number of unique logon credential sets that you must keep track of. However, this is not necessarily a good security option. If the primary site’s authentication is a basic password only, then when your account is compromised on the primary site, the intruder automatically gains access to all the linked secondary sites as well.

By the way, the primary site will maintain a list of secondary sites that have been linked. This list is for your convenience when you want to disconnect an OAuth link, but an intruder can use it to follow your links to those secondary sites.

ONLY use OAuth to link sites back to a primary site if you have configured multi-factor or multi-step authentication on the primary site. Otherwise, you would be better served setting a long and complicated password for each site and putting up with the hassle of managing multiple difficult credential sets (see my whitepaper Ten Steps to Better, Stronger Passwords for guidance on this).
Multi-Factor Authentication

Multi-factor authentication is a method of logon verification where at least two different factors of proof are provided. There are three generally recognized types of authentication factors:

- Type 1 - Something You Know
- Type 2 - Something You Have
- Type 3 - Something You Are

Type 1 includes passwords, PINs, combinations, code words, or secret handshakes. Anything that you can remember and then type, say, do, perform, or otherwise recall when needed falls into this category. Type 2 includes all items that are physical objects, such as keys, smart phones, smart cards, USB drives, and token devices. (A token device produces a time-based PIN or can compute a response from a challenge number issued by the server.) Type 3 includes any part of the human body that can be offered for verification, such as fingerprints, palm scanning, facial recognition, retina scans, iris scans, and voice verification.

By combining two or three factors from these three categories, a multi-factor authentication is crafted. Multi-factor authentication is preferred as it is much more difficult for an intruder to overcome. With just a password, an attacker only has to have a single attack skill and wage a single successful attack to impersonate the victim. With multi-factor authentication, the attacker must have multiple attack skills and wage multiple successful attacks simultaneously in order to impersonate the victim. This is extremely difficult and, thus, a more resilient logon solution.

However, few online services offer true multi-factor authentication, but the number is growing. One excellent example of a multi-factor authentication supporting online service is that of PayPal. They currently offer at least two different multi-factor options. One option involves a credit card-sized device that produces on demand a one-time-use six-digit PIN. The second option sends an SMS text message to your cell phone with a six-digit PIN. In either case, the PIN is used alongside your name and password credentials to gain access to your PayPal account.

Multi-Step Authentication

Multi-step authentication differs from multi-factor authentication in that it does not strictly require that each authentication factor be different, and the authentication can take several steps or phases to complete. Some of the first forms of multi-step authentication online took the form of security questions. These were a set of questions that a user was asked to provide the answers to during the initial setup of their account. Then, during each logon event, some of those questions were asked again to prove identity. This method is still very common. Other forms of multi-step authentication include displaying a picture, a user-provided statement, or having the user enter a code or PIN using an on-screen keyboard.

A new variation on this idea has become popular and may be a viable option to that of multi-factor, namely two-step authentication. Two-step authentication is potentially the same as some forms of multi-factor, but since most of the sites implementing it are labeling it as two-factor, we need to use their label for it to be consistent and to avoid confusion.
Often the two-step authentication process involves sending the user a one-time use code or PIN via e-mail or SMS, calling the user over a voice connection with an automated system where the user either responds to questions or enters a code displayed on the screen, or using a dedicated device or smart phone app to generate one-time use access codes.

One of the leaders in this movement is Google. With the release of the Google Authenticator for Android, iOS, BlackBerry, and Windows Phone, as well as many other platforms, your mobile device can generate a one-time use token to authenticate to Google or dozens of other sites without the need to send SMS text message or even have a data connection (from the mobile device running Google Authenticator). Basically, the authenticator is a one-time synchronous dynamic password generation token. That means that it creates codes that can be used only one time, those codes are generated based on time stamps, and the codes are different for each user and each time used.

The list of sites that support two-step authentication is growing. Many of the sites that support OAuth, happen to also support two-step (or other multi-step) authentication. This is not because the authentication methods are the same, but because those sites respect their users enough to offer stronger authentication options than just a password. Unfortunately, the fact that a site is using multi-factor, multi-step, or two-step authentication does not imply that they are implementing good behind-the-scenes security. But we can at least hope that the public-facing improvements reflect an operational understanding of effective security.

**Why Should You Bother?**

Using the same old password method to authenticate to online sites and services has been common, standard, and easy. But that is, in fact, the problem. There are myriad ways that password authentication can be compromised. This includes guessing, discovering re-used passwords, brute force attacks, plain text user database theft, lost backup tapes, social engineering, shoulder surfing, infrared heat detection on keypads, keystroke logging, phishing attacks, web-spoofing attacks, DNS pharming attacks, session hijacking, network traffic sniffing, and man-in-the-middle attacks. Whether you have a short and simple password or a long and complex password, many of these attacks are just as successful against both. There just is not a reliable means of password selection and use that can avoid all possible means of password compromise.

You need to choose better authentication security whenever it is offered. Hackers are actively seeking to compromise your online accounts. They want to be able to take over your accounts and identities. They want to take your money. You have to defend yourself by taking full advantage of the strongest authentication options provided by the sites you visit.

It is and will be a hassle, at least initially. It is a different way of accessing online resources. It will fail from time to time, and you will forget the process every now and then, but stick with it. Eventually, it will become an automatic process for you, just like putting on your seatbelt or applying sunscreen (you are doing that right?). By using better authentication options, you remove yourself from the masses of online users who remain vulnerable to basic password compromises. You want to be different. Take action. Be more secure.
Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

- Cybersecurity Foundations
- Security+ Prep Course
- IINS 2.0 - Implementing Cisco IOS Network Security
- JNCSIS Security Certification Boot Camp (JSEC, JUTM)

Visit www.globalknowledge.com or call 1-800-COURSES (1-800-268-7737) to speak with a Global Knowledge training advisor.

About the Author

James Michael Stewart has been working with computers and technology for nearly thirty years. His work focuses on security, certification, and various operating systems. Recently, Michael has been teaching job skill and certification courses, such as CISSP, ethical hacking/penetration testing, computer forensics, and Security+. He is the primary author on the CISSP Study Guide 6th Edition, the Security+ Review Guide 2nd Edition (SY0-301), and Network Security, Firewalls, and VPNs. Michael has also contributed to many other security-focused materials, including exam preparation guides, practice exams, DVD video instruction, and courseware. In addition, Michael has co-authored numerous books on other security, certification, and administration topics. He has developed certification courseware and training materials as well as presented these materials in the classroom. Michael holds a variety of certifications, including CISSP, ISSAP, SSCP, CPTE, CDFE, Q/SA, Q/EH, CEH, CHFI, and Security+. Michael graduated in 1992 from the University of Texas at Austin with a bachelor’s degree in Philosophy. Despite his degree, his computer knowledge is self-acquired, based on seat-of-the-pants, hands-on “street smarts” experience. You can reach Michael by e-mail at michael@impactonline.com.