

(Approx. 1135 words)

Two Factor Authentication — Proof of Identity

By Phil Sorrentino, Staff Writer, The Computer Club, Inc., Sun City Center, FL

March 2014 issue, The Journal

www.sccccomputerclub.org/

philsorr (at) yahoo.com

When you walk up to a teller in a bank and request information about your bank account, the teller may ask you to authenticate yourself by providing a picture form of identification. But if you have been going to this bank for many years and she is familiar with you, she may just give you the information. In truth, your face and her knowledge of you have provided the necessary authentication for her to respond to your requests. Authentication is much easier in the real world than it is in the software and computer-network world.

Authentication is the act of proving one is really who one says he or she is. In the computer world, we all experience this every time we sign on to one of our accounts or websites. Typically we are asked for a User Name and a Password. The correct User Name and Password combination proves, to the software requesting these items, that we are who we say we are. Of course, we could give our User Name and Password to a friend, something we rarely want to do because then he would be able to authenticate himself as the owner of our account. “Hacking” occurs when someone or some software program attempts to guess your Password after acquiring your User Name: maybe from some public information source. (Remember, User Names are available all over the internet.) This is a form of brute force “hacking” of an account. And unfortunately, there are many other, more sophisticated, ways of hacking into an account.

So, more formally, “Authentication is the act of confirming the truth of an attribute of a datum or entity, which might involve confirming the identity of a person or software program, or ensuring that a product is what it’s packaging and labeling claims to be.”

In other words, Authentication involves verifying the validity of at least one form of identification. As it turns out, practically, there can be three forms of authentication, called factors. Now, two-factor authentication requires the use of two of the three authentication factors. These factors are:

- Something only the user knows (e.g., password, PIN, pattern);
- Something only the user has (e.g., ATM card, email account, mobile phone); and
- Something only the user is (e.g., biometric characteristic, such as a finger print).

(These factors are so important for authentication that they are identified in government documents in the standards and regulations for access to U.S. Federal Government systems.) Some security procedures now require *three-factor authentication*, which involves possession of a password, and a physical token, used in conjunction with biometric data, such as a fingerprint, or a voiceprint, or a retina scan.

Two-factor authentication is not a new concept. When a bank customer visits a local automated teller machine (ATM), one authentication factor is the physical ATM card that the customer slides into the machine (“something the user has”). The second factor is the PIN the customer enters through the keypad (“something the user knows”). Without the corroborating verification of both of these factors, authentication does not succeed. Another example is when you use your credit card for a gasoline purchase and you have to enter your ZIP code to confirm the charge. You must provide a physical factor (something you own), the card, and a knowledge factor (something you know), the ZIP code. These examples show the basic concept of a two-factor authentication system: the combination of something the user knows and something the user has.

“Something only the user knows” is termed a Knowledge factor and is the most common form of authentication used. In this form, the user is required to prove knowledge of a secret in order to authenticate, typically, a password, PIN, or a Pattern. All of us are familiar with the password which is a secret word or string of characters. This is the most commonly used mechanism for authentication. Many two-factor authentication techniques rely on a password as one factor of authentication. A PIN (personal identification number), is a secret series of numbers and is typically used in ATMs. A Pattern is a sequence of things, like lines connecting the dots on the login screen of a cell phone or tablet.

“Something only the user has” is termed a Possession factor. A key to a lock is a good example. With today’s computer systems your email account or your phone or a swipe-card is used as a possession factor.

“Something only the user is” is termed an Inheritance factor. Historically, fingerprints, a biometric method, have been used as the most authoritative method of authentication. Other biometric methods such as retinal scans are possible, but have shown themselves to be easily fooled (spoofed) in practice.

Two-factor authentication is sometimes confused with “strong authentication”, but these are fundamentally different processes. Soliciting multiple answers to challenge questions may be considered strong authentication, but, unless the process also retrieves “something the user has” or “something the user is”, it would not be considered two-factor authentication.

Two-factor authentication seeks to decrease the probability that the requester is presenting false evidence of its identity. The more factors used, the higher the probability that the bearer of the identity evidence is truly that identity. These systems ask for more than just your password. They require both “something you know” (like a password) and “something you have” (like your phone or email account). After you enter your password, you’ll get a second code sent to your phone or email, and only after you enter it will you get into your account. It is a lot more secure than a password only, and helps keep unwanted snoopers out of your accounts.

Many well-known systems employ two-factor authentication. Some of these are: Amazon Web Services, Dropbox, Facebook, Google Accounts, Microsoft/Hotmail, Paypal/eBay, Twitter, and Evernote. The two factor authentication will typically be employed when you are using a different computer, or a computer from a different location, when trying to access one of your accounts.

Most of these two-factor implementations send you a 6 digit code via a text message for you to input when you receive it. This 6 digit code becomes the second factor to be used with the original password. This definitely adds an extra step to your log-in process, and depending on how the account vendor has implemented it, it can be a minor inconvenience or a major annoyance. (And it also depends on your patience and your willingness to spend the extra time to ensure the higher level of security.) But in the long run the use of a two-factor authentication improves the security of your private information, no doubt something we all want.