TIPS AND TRICKS FOR USING TWO FACTOR AUTHENTICATION TECHNOLOGY

Single password protection techniques, while a well-used and ancient method of protecting access to information or location, are no longer something that can guarantee a reliable means of protecting what you want to keep private.

With the widely distributed existence of intrusion methods like keystroke loggers, phishing attacks, eavesdropping in general and dictionary attacking programs that can run through millions of possible passwords in minutes, having a single password as your only protective barrier to data entry is not something you can entirely trust.

Because of this a new standard in data protection has had to be developed that is much more secure. It is called Two Factor Authentication and has become very popular in the digital world recently. Used by online software applications like DropBox, data storage platforms like those belonging to Google and numerous other server or physical machine based access points, two factor verification comes in many forms.
However, its essential structure is as follows: Instead of a single access password that gives a user entry to a given area of digital space, two independent and separated factors are used instead. One of these remains the password while the other is a piece of completely distinct access data that is usually delivered either via message to a mobile device or directly to a physical data token.

However two factor authentication is specifically implemented, the key feature that it needs to have is a two level access system of two completely distinct pieces of login data. In less robust systems, the secondary token or mobile device based login data will be a secondary static password or a static access chip; in more robust two factor authentication setups, in addition to the original classical password, the secondary access key is a one-time item, meaning that each new login attempt generates a unique access key for that one single session, sent to a physical token or a mobile device (phone usually, could also be a tablet.

Most commercially available two factor systems are too complex and expensive for home or small business computer networks and, although this is changing thanks to innovations by the people at Google and other companies, cost remains something of a burden for smaller operators who want to secure their computers or compact server networks.

However, not all is lost; even you, whether you're working with online data management apps, your personal computer or even a small Linux based server network, can set up two factor authorization to maximally protect all your crucial data access points with the best reasonably possible security.

Online Applications

Numerous online applications and platforms are designed to let you enable two factor authentication. The online cloud storage system DropBox, Google and all of its accounts, Facebook and a number of other lesser known programs are all two factor capable. Let's cover the three most commonly used online platforms.

If you happen to use Google for your email, social networking and document storage (through Drive) you can set up two factor protection simply by visiting this page: http://support.google.com/accounts/bin/answer.py?hl=en&answer=180744 and following the steps that are clearly outlined.

In the case of Facebook, two factor authorisation can be enabled from within your account settings gear icon by clicking on the “Privacy Settings” tab and then clicking on “Security on the left-hand side. There you will be presented with a list of items, “Login Approvals” and “Recognized Devices being the two you should select. A handy guide that’s been created by Facebook itself is available here: http://www.facebook.com/note.php?note_id=10150172618258920

With DropBox, arranging two factor authentication is also pretty simple. You simply log into your DropBox dashboard, go to “Settings”; select the “Security Settings” tab and enable two factor authentication. From there you should follow the step by step instructions that the system itself gives you.

In the case of all of these above web-based applications and many others that you’re likely to find with services such as online banking and cloud computing companies, the essential secondary login token will be either a static or variable passkey that’s delivered to your mobile phone. This represents a classical and very common two facto setup that is both hassle free and easy to implement amongst millions of customers because it does not depend on any specialized hardware or programming knowledge.

Linux Servers and Machines

If you’re running a small home or business Linux server distribution, you can create remote access to it at no cost and without going through numerous expensive enterprise level two factor providers like RSA Verisign or Pinsafe. How do you do this? Simple; you can rely on the power of a freely downloadable authentication module called Google Authenticator, created by none other than Google for allowing you to use your mobile device, be it iPhone, Android or Blackberry based, as a soft token for two factor access to your Linux server logins through dynamic (variable) passcodes.

As a starting point, you’ll need to download Google Authenticator from here for

your particular device: http://code.google.com/p/google-authenticator/.

After that and before doing anything else, you'll also have to enable two factor verification to your Google Accounts as described above. The steps that follow from there include installing a PAM module for your particular Linux system (Ubuntu, Red Hat, etc.) and configuring it to create a series of authentication keys for different mobile users you plan on allowing into your system. PAM stands for pluggable authentication module, and is designed specifically for plugging different kinds of authentication into Linux.

After you have done the above, you will also need to activate Google authenticator on your mobile devices and configure it so that it connects to your Linux server's SSH login.

There are a lot of further technical details behind this process, many of which get addressed in far more detail here: http://www.howtogeek.com/121650/how-to-secure-ssh-with-google-authenticators-two-factor-authentication/ and here: http://www.mnxsolutions.com/security/two-factor-ssh-with-google-authenticator.html

But, on the whole, using Google Authenticator to set up two factor verification with multiple access codes and multiple mobile user accounts for SSH based Linux access is quite a bit easier than doing the whole thing through the OpenSSH that's built into the Linux OS itself.

Commercial Network/Computer Protection Alternatives

If you're not inclined towards technical two factor enabling related work, there are also some very low priced commercial vendors out there who will create highly secure two factor authentication systems for your smaller organization/business network. These security companies don't offer the more robust physical token systems that Verisign and RSA handle, but they will allow you to install easy to use mobile phone based two factor access on your own system.

Source : http://www.opensourceforu.com/2013/04/tips-and-tricks-for-using-two-factor-authentication-technology/