Bootstrappist

Multi-Factor What? A Few Words On A (Sort Of) New And Crucial Authentication Method

BY MIGUEL LEIVA-GOMEZ ON JANUARY 8, 2013 IN PLATFORMS

If the purpose of authentication is to keep a site's confidential data behind locked doors, multi-factor authentication can be explained very simply: It adds locks to that door. The more locks your door has, the more keys you need to open it. If you don't know what multi-factor authentication is, it would be easier to explain with an example:

Have you ever been to those sites where, while you're registering, you have to verify that your phone number is real? They send you an SMS through a gateway and you receive a code that you're supposed to type into a field on the site's interface to authenticate your number. This adds another factor to your authentication, hence the clever name that took no less than 20 seconds for someone to come up with.

When developers learn about this, they treat it like they treat any new toy: They play around with it and contemplate implementing it everywhere. But does your site really need multi-factor authentication?

One of the biggest benefits perhaps is the enormous rise in security. If you log someone in on his or her account, this person probably wants to remain logged in. But the “Remember me” feature in a website is probably one of the most overused features since butter on bread, and hackers have learned to sniff out a session’s crucial data in order to imitate the logged in user. While we cannot prevent such infiltration, we can still prevent the hacker from taking things to the next step: changing the user’s password. Multi-factor authentication then steps in and trumps the hacker’s effort.

Is it really worth putting all the man-hours into a system that requires an expensive and complicated SMS gateway? Should you really spend all that time learning the API?

Most of the time, the short answer is “no.” The long answer is “not unless you’ve got some really sensitive data in there.” For an email provider, giving users access to multi-factor authentication outside of a certain device reduces the risk of privacy intrusion. On the other hand, if you’re making a site like 9gag, the damage caused by a compromise is minimal.

There is, however, a situation in which multi-factor authentication is absolutely necessary no matter what kind of site you’re writing. Every site’s administrative interface should have at least one form of authentication, but two forms will protect the administrative sphere of the site more effectively. Sure, it’s annoying, but there are ways around that. For example, you can check whether the user is accessing his/her account through a “recognized device.” If the device is not recognized, prompt authentication. Hackers can get around this, but you can wish them luck. Most of them would back off from a challenge like this unless you’re running a bank or the CIA.

And SMS isn’t the only way to authenticate. If you prefer not spending a buttload of cash sending messages to people’s phones through a gateway, you can get into cryptography. When you have time, have a look at SmartSignin. This identity management service authenticates you through a password and a crypt phrase. The crypt phrase is basically a private key within an algorithm that you select. The encryption algorithm (AES 256, in this case) revolves around your chosen key. After it’s done encrypting stuff, you keep that key and no one else has it. Talk about effective authentication! If you take their example, your users will just see it as two passwords; one that can be recovered, and one that they have to remember permanently or else they’re screwed. This is good for administrative accounts, but

not good for user accounts, where feeble-minded users might not understand that they cannot restore that “password.”
Whatever you choose to do, remember to lock the door!