Entrust Solutions Nepal

Two factor authentication:

Ever thought of this?

Abhibandu Kafle
Entrust Solutions Nepal

Abstract:

Two Factor Authentication commonly known as 2FA in technical field is a measure to identify the user by the application with ‘what they have’ and ‘what they know’, so that it can authenticate any specific person logging into the system as the real owner of that account.

Majority of reputed websites implement 2FA process to enhance the user security. Comprehending the benefits the 2FA scheme offers, more are on the process of implementing the feature. A comprehensive list of sites implementing/planning to implement 'Two Factor Authentication' can be seen on http://twofactorauth.org .

Any new portals bringing forth 2FA security feature should consider possibility of Denial of Service (Dos) before implementing it to production. Premature implementation of this scheme without considering verification module working may lead to Denial of Service (DoS) to a legitimate user which sadly is prevalent at present.

The problem:

If every kind of information that uniquely identifies a user -something that can't be attribute of multiple users- are not being verified before allowing an account to have access to 2FA management portal, it could lead to DOS, because the account could be impersonating someone with their details.

As an instance, I could use email of a guy, say Derp , which is derp@company.com, a unique identifier, and make account on his behalf. I don't have email access of derp@company.com but I will be able to use that account to impersonate him. Now I add 2FA to that account and attach my cell number to his account.

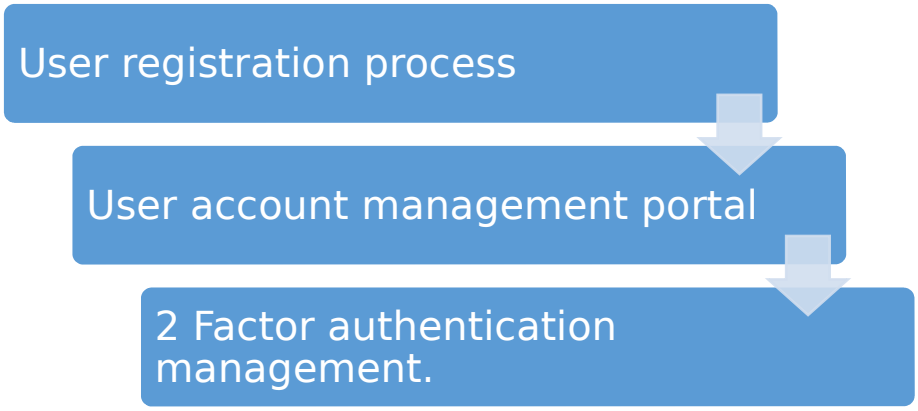
Someday, Derp wants to join the portal with his email. When he sees that the email has been already used in other account, he will try to reset the password. He can reset the password, but even if he knows the password, there's a dead-end because the account has 2factor enabled with my mobile phone attached to the account. All of 2FA service providers mask the mobile number for privacy reasons and give out message that "the text has been sent to your mobile ending with *******123, which is not going to help.

In some other portals, it was also possible to search users by unverified email, thus allowing an attacker have an added benefit in impersonating a real person.

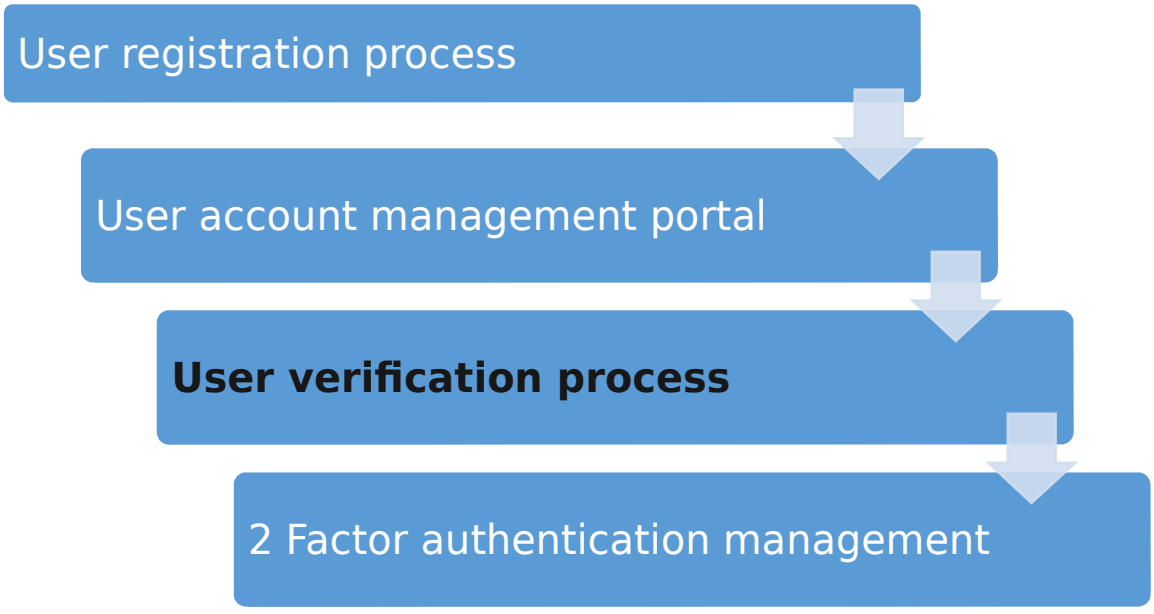
Since 2FA is the ultimate power that could be granted to end user, authenticity of user should be considered prior to handing him over the ultimate power. What apparently seems to instill the sense of security in users, can also lead to authentication problem like this.

The authentication flow:

How it actually works in vulnerable portals?



How should it have been?



Some popular sites that still use this scheme:

I spent few hours looking sites that used this type of authentication scheme and it seemed more than 70 percent of those are still vulnerable.

Some popular portals like Facebook, Twitter, and Stripe now only allow adding 2 FA after verifying email account.

The impact (a scenario) :

Let us take an example of github.

Github doesn't ask you to verify your email (as your identity) while you sign up. Now, you can sign up on anyone's behalf using their email. Since there is no verification process, you can add 2FA to that account so that it will be inaccessible to legitimate user.

It can really come handy at times like when you have a edu mail and if someone else makes an account for you before you even register. If they add 2 FA to your account, it apparently becomes inaccessible to you [unless you mail the service provider and show them your identity]. Thus one won't be able sign up to github using his edu mail and is deprived from using student pack services offered by github.

It is not very hard to enumerate email addresses of a specific target company since most educational institute or email users use firstname@domain.com or classroll@domain.com .

Likewise, in portals where email from specific domain are only allowed to sign up or join a team, this kind of attack can prove insidious, as long as users aren't verified. Because when a team from a company is to be signed up, probably the whole company will be dispossessed from having an account in that vulnerable portal.

Conclusion:

Every application that allows user to activate 2FA on their portal should ask for verification of identity separately. For e.g. A user can not only be verified by sending a text to mobile number mentioned during registration, it is equally important to verify the email address and similar pertinent information that are unique and can possibly lead to ‘denial of service’ for legitimate user thus preventing a legit user from accessing the portal.