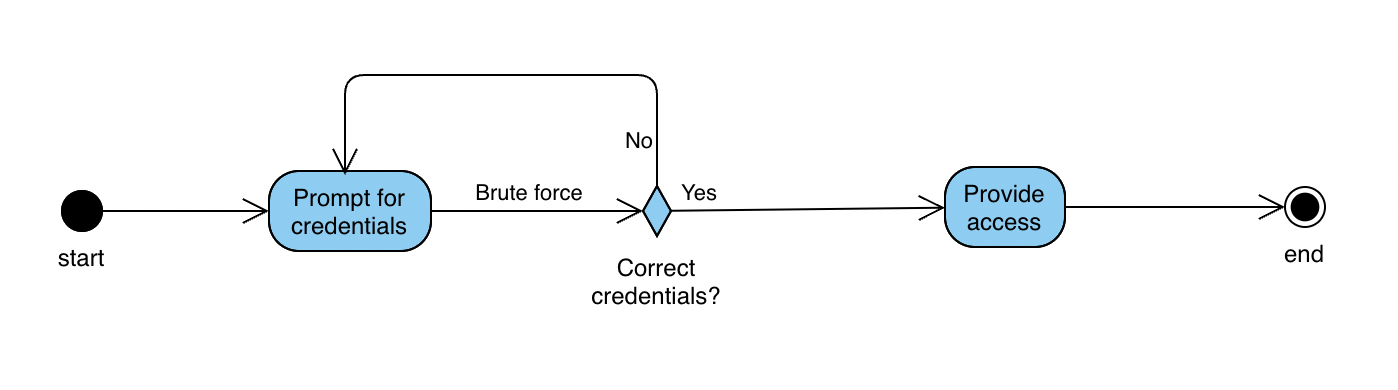
**Identification and Authentication Failures (Initial post) by Etkin Getir**

According to the OWASP Top 10:2021, Identification and Authentication Failures rank seventh among the most common weaknesses (OWASP, 2021). Indeed, even though measures like 2FA and robust password policies are applied widely, it still comes down to the final user to keep his/her credentials and data safe. From my point of view, this human factor remains as one of the weak spots in today’s world, as evidenced by the staggering amount of stolen data/assets online every year (III, N.D.).

Hence, the mitigation to identification and authentication failures needs a two-pillar approach: The technical pillar encompasses robust password policies and additional security checks (e.g. 2FA) that would enforce user compliance. On the other hand, in the user pillar, the users must be aware of the security risks associated with the weak passwords or the potentials vulnerabilities associated with storing credentials or other sensitive information.

In the flowchart (activity diagram) below, a brute force attack is depicted. As we can see, no additional methods like 2FA is in place and the attacker is allowed to try entering the correct credentials for infinite times (i.e. no restriction on number of attempts). The system prompts for credentials and rejects the incorrect ones, but the attacker keeps trying until he/she comes up with the correct one, potentially starting from the common weak passwords (e.g. ‘Password’, ‘12345’, etc.) and making his way towards passwords containing potential personal data (e.g. name, surname, birthdate, etc.). As mentioned above, if the user sets a complex password that is hard to guess and/or there is a 2FA authentication method in place, attacker’s job might get significantly harder.



On the other hand, the attacker may try to follow the “Forgot password” route, as depicted in the activity diagram below:

Diagram

Description automatically generated

In this case, having weak recovery questions that are easy to guess (such as “Your birthday” or “Favorite team”) and not the absence of secondary recovery methods (e.g. mobile phone) makes it easy to reset the password of the victim by the attacker.

**References:**

OWASP (2021) OWASP Top 10 - 2021.Available from: https://owasp.org/Top10/ [Accessed 25 September 2022].

III, (N.D.) Facts + Statistics: Identity theft and cybercrime. Available from: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime [Accessed 25 September 2022].

**Replay to Etkin Post by Mustafa Sibai:**

That was an excellent read. Thank you so much. One thing I would defiantly add is IP address whitelisting and a login monitoring system. This way, if a customer or a user logs in from a new IP address that is unrecognized, an email could be sent to the user asking them to verify themselves and whether it is them that logged in.

Let us say a user logs at 9 AM from the UK. The same user logs in again at 10 AM from China. The only way this is possible is

1. If the user invented light-speed travel and did travel to China within that hour.

2. The user used a VPN to log in from a different country.

3. The user was hacked.

In any of these instances, a verification email would ensure no bad actors took hold of the user account. The problem with though, is what if the user email was compromised? Maybe send a notification on their phone?

At the end of the day, there is not one silver bullet to fix everything.

Security is hard

**Form Post by Gianluca Cannone:**

Even though it is very effective, everyone knows how annoying 2FA is :D Anyway, I agree with you that the end user needs to keep their credentials secure. Your UML clearly shows how important it is to have a 2FA.

**Reply by Mustafa Sibai**

Honestly, I agree with you. When 2FA was first introduced, I was really happy with it. I don't have a single account that does not have 2FA on it. The issue is that after five years or so of using it and having over 20 accounts with 2FA, setting up a new computer or just wanting to access an account quickly is exhausting. Also, having to go through and find the correct 2FA account and type the 6-digit number is exhausting. Sadly it is necessary.

I really like Google and Microsoft's implementation of 2FA. There isn't a need to enter a code, but rather a notification pops up on your phone asking you whether it was you who just signed in or not. Answering that is much better than typing a 6-digit number, but even that gets annoying after a while.

But sadly, it is necessary to keep your accounts secure.

One thing I do and many security experts advise regarding security questions like "what is your birthdate" or "what high school you went to." These questions should not be answered as is. What I mean by that is when you create a security question, and let us say you pick "What is your birthdate?" do not answer with your birthdate but rather answer with a different answer like "UK-EU-World". It would be much harder for an attacker to guess that rather than having your answer your actual birthdate.

Adding small security tips like that when customers create their security question is also a good idea.