Secure2FA

Members :
P. Teja Swaroop (17MIS1003)
Sandeep Kumar

Abstract :

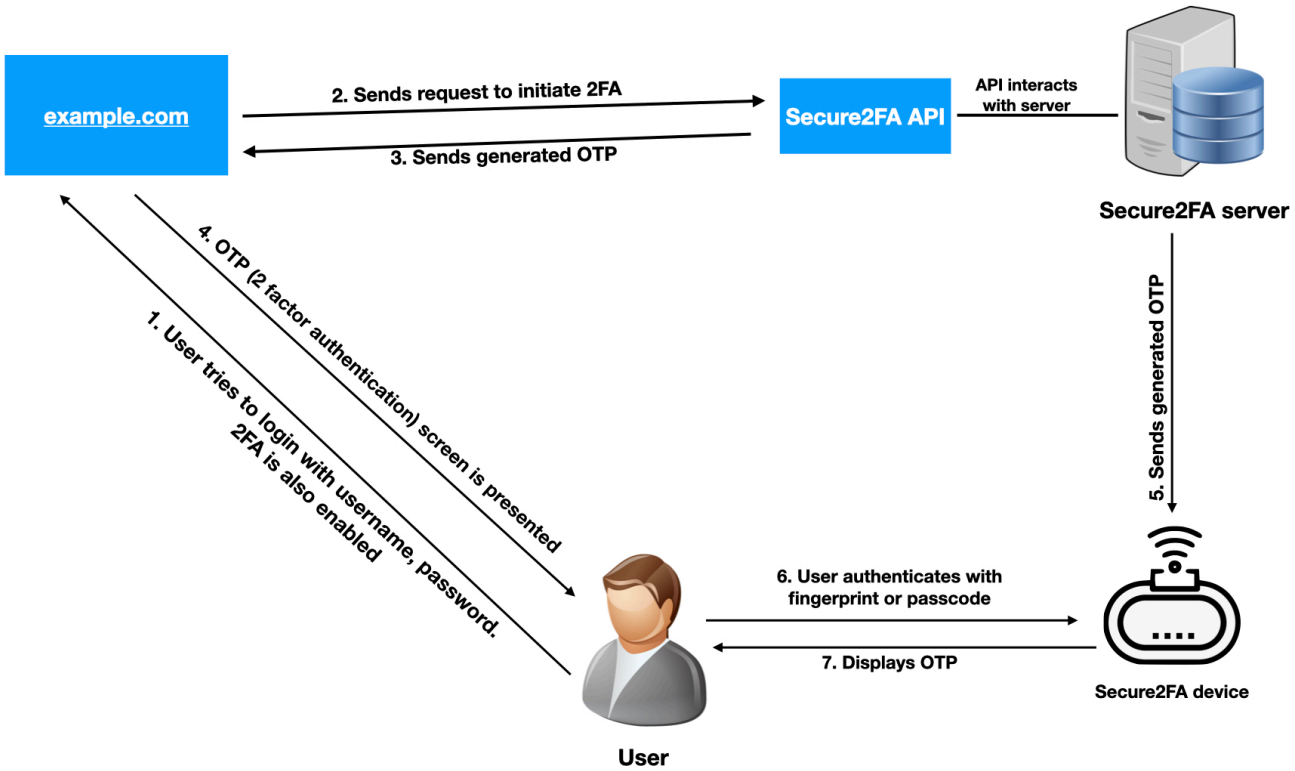
Secure2FA is an innovative way of using IOT in the fields of online privacy, and cyber security. 2FA in Secure2FA stands for 2 Factor Authentication (or multi factor authentication).
Two Factor Authentication, or **2FA**, is an extra layer of protection used to ensure the security of online accounts beyond just a username and password.
For example, when you're making an online transaction using your internet banking, you will need an OTP (one time password) besides your bank username and password, this OTP is randomly generated and ensures that the transaction is authenticated, and is done by the actual bank user and not by any other malicious third party.
So, even if an attacker gets their hands on your username and password, they still can't make transactions from your account because it is protected by 2 factor authentication. This is how 2FA can actually protect your malicious parties.

But, even if you're using 2 factor authentication, that still doesn't guarantee you that you are completely safe, because hackers can find a way to sniff the One Time Password from you, as in most cases, this OTP is actually received on your Mobile or Computer through SMS or Email. A simple demonstration of how hackers can do this - (click on thumbnail to watch the video)

The above video demonstrates how a hacker can bind a malicious RAT (Remote Access Trojan) to an innocent software, and when the victim downloads and executes this software, the hacker gets a backdoor on the victim's device (smartphone, computer, etc). Now that the victim's device is compromised, everything the victim does is recorded. In this case, as you could say, even 2 factor authentication cannot provide complete security as the OTP can also be captured by the hacker.
This is just one of the ways in which a hacker can bypass 2 factor authentication. Anyway, I think I made the point clear that the normal 2FA mayn't be really secure as hackers can easily get access into your device and capture your OTPs.

Our innovation, Secure2FA prevents this.
Secure2FA is an independent device whose only job is to receive an encrypted form of the OTP, authenticate the user (using fingerprint, or just a pass code), decrypt the received OTP, and display it to the user on a small screen. It's also portable so that the user can carry it everywhere, or even use it as a wearable.

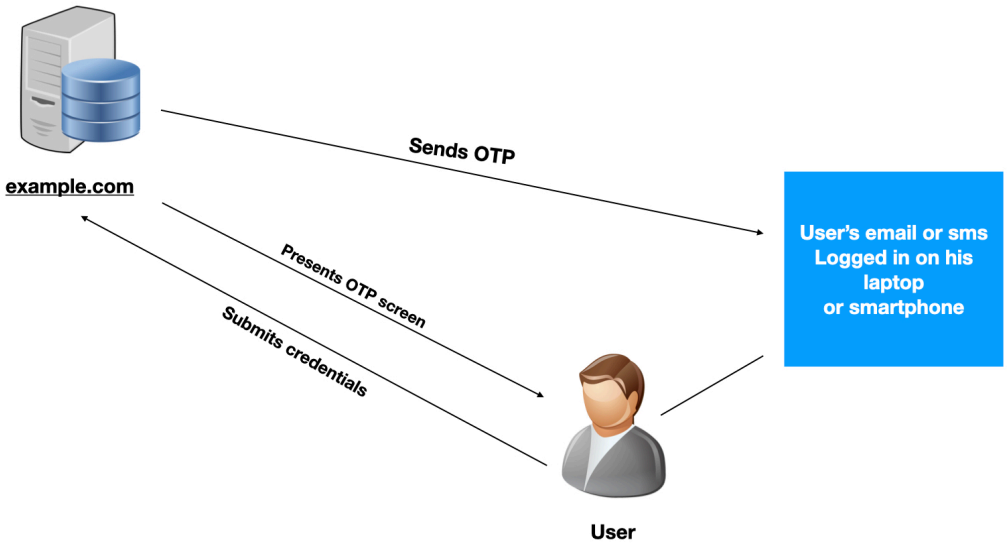
How Secure2FA solves the problem of cyber security threats is simple, since the device is programmed only to do one job i.e., receive, decrypt, and display, it is technically un-hackable. Unlike your other devices like smartphone, PC, etc., hackers cannot get a backdoor on this device. So, when you're authenticating on the Internet using 2 factor authentication, you can be sure that the OTP you're receiving is tamper proof. It cannot be accessed by anyone other than you.



Existing System

Traditional 2 factor authentication : Traditional 2 factor authentication involves the user getting the One Time Password through SMS or Email.

For example, when a user is logging in to **example.com** where 2 factor authentication is enabled, he/she first submits his credentials (username, password) on the website. He then gets presented the 2 factor authentication screen where he needs to enter the one time password. This one time password is sent to the user through email or sms. The user will have to access this OTP from one of his devices (laptop, smartphone, etc). He then enters the OTP into the website's OTP portal, and he will then be successfully authenticated.



Flaws :

1. The devices on which the user is receiving OTP (laptop, smartphone, etc) might already be compromised, and hence the OTP can be grabbed easily as well.
2. The user's email might have been hacked, which leads to the hacker having access to the OTP.
3. Hackers can find a way to social engineer the user and extract the OTP from the user.
4. If the user is fully compromised i.e., if the hackers fully hacked the user (his credentials, and also his devices), it means the hackers can gain access to the user's account.

Secure2FA

Modules of proposed system :

1. **API (Application Program Interface)** : API is the way of communicating with the Secure2FA server. When any website wants to implement secure2fa, they can make requests to the API and get corresponding responses.

2. **Encryption** : The OTP generated by the server is encrypted with the Public key of the Secure2FA client device.

3. **Sender** : A sender program on the server will send the generated OTP to the corresponding Secure2FA device.

4. **Receiver** : A receiver program on the Secure2FA client device receives the data from the sender program (running on server)

5. **Fingerprint Scanner** : A fingerprint scanner sensor will scan the fingerprint data from the user's finger and forwards this to the authentication module

6. **Authenticator** : The authentication module authenticates the fingerprint data inputed by the user and makes sure that the user is allowed to access the device.

7. **Decryption** : The decryption module decrypts the received data by using the private key. The decrypted data is nothing but the received OTP.

8. **Display/Screen** : This module is responsible for displaying the decrypted OTP on the screen of the Secure2FA device.

9. **Clear/Reset** : This module is responsible for clearing the screen and deleting the OTP from the memory of the device.

Protocol Used : CoAP(Constrained Application Protocol)

Block Diagram: