Authentication Strategy Recommendation

Mou Zhang

1. An introduction that explains the motivation for the research

This research is to help technical manger to decide which tech shall be used in an online health care communication and data storage system. The key of this paper is to compare the pros and cons of different authentication strategies, which are used in sending and receiving messages in this online health care communication system. As is known to all, heath care data is very private and needs to highest security levels. Therefore the most suitable authentication strategy is needed.

This health care communication and data storage system contains several essential features, which is listed as below.

- Allows medical practitioners and users to communicate via secure chat
- Allows patients to send pictures to doctors for diagnosis
- Maintains medical records and health insurance data
- Sets up calendar entries for appointments
- Allows patients to use their own devices (e.g,. smart phones)

2. A short discussion of the constraints and considerations that influence the decision

There are several key features when we are comparing among different strategies. These features are the essential standards to choose among the strategies.

The first is the security. As an online health can communication and data storage system, the security is always the most important the problem. As we know, Health data are very secure. If they are leaked to someone else, then the advisement company and hospital may use them to send you advisement and make a lot of money. Also the chat information between medical practitioners and users must also be very secure because they also contains the secure medical data.

The second is the convenience. The convenience here are both for the developers and customers. For the software development engineers, a simple authentication strategy will make them work easier and reduce the chance of being hacked. Also security experts must involve when developing the software to make sure that the security problems are removed. For the customers, we shall not increase the complexity bigly for the security problem. We must leave the login and chatting system as simple as possible. A lot of the users of online health system are old people and most of them are not very familiar with ne technologies. So keeping the software and platform simple is very important.

The third is the scalability. When there are a lot of users, the scalabitilty is very important. As the growth of the numbers of users, we need to keep every users's experience. The communication between patiences and doctors must not be delayed.

Therefore the scalability is very important.

The fourth is the robustness.

3. A succinct description of each strategy under consideration, and

There are several strategies under consideration.

(1)The first is using Kerberos.

Kerberos is very common security strategy nowadays. The famous command ‘kinit’ is useful in many big companies. I used it a lot when I’m interning at Amazon. Kerberos is a network authentication protocol created by MIT, and uses symmetric-key cryptography to authenticate users to network services, which means passwords are never actually sent over the network.

Traditionally the network services always use passwork-based authentication schemes. But in these methods, the transmission of authentication information unencrypted and not sage. Kerberos eliminates the transmission of unencrypted passwords across the network and removes the potential threat of an attacker sniffing the network.

Rather than authenticating each user with password separately, Kerberos uses symmetric encryption and a trusted third party (a key distribution center or KDC) to authenticate users to a suite of network services.

In Kerberos, each user has a unique identity called principal. This principle contains 3 parts: primary, instance or realm. It works as the following steps.

1. The user sends the principal to the KDC
2. KDC searches the that principal in their databases
3. If they find that principal in the database, they gonna create TGT and wraps it in the principal’s user key.
4. When the Kerberos client on the user side receives the encrypted TGT, they gonna decrypt the use key and only use that user key on the client. When the authentication is

(2)The second is using SAML.

SAML is one kind of the XML. It is a assertion. The full name is Security Assertion Markup Language. We can always see is with SSO. The login for enterprise account on zoom at JHU is using SSO.

It works as the following steps.

1. You send a request to access resource from the SP(Service Provider).
2. The SP find that they don’t know you, then It will give you an AuthRequest in HTML Form redirects.
3. Then you need to go to the IDP(Identity Provider) and login to get a credential in HTML Form.
4. When you get the credential from IDP, you can use it to access the service from SP.

(3)The third is using Mutual TLS

SSL/TLS are very famous secure protocals. SSL stands for secure sockets layer. TLS is

an improvement of SSL. It stands for transport layer security. Mutual TLS (mTLS) authentication ensures that traffic is both secure and trusted in both directions between a client and server.
Mutual TLS allows requests that do not log in with an identity provider (like IoT devices) to demonstrate that they can reach a given resource. This is a great advantage comparing with SAML.
What matters in the Mutual TLS is certificate. At first, the client connects to the secure session server will a hello. Then the secure session server sending back a hello together with server certificate and client certificate request. Then the client sends its certificate back and sends the key info with public key. If the server and client verifies the certificate,
(4)The fourth is using Facebook Login
Facebook login strategy is not showed in their website. They only tell us the features and advantages of the facebook login. This is both an advavtage and disadvantage. The good thing is that hackers are not going to find out a way to attck the authentication strategy because they have no idea of how it works. But the bad thing is that the users also don't know what their strategy are, makes it less trustworthy. But I'd say it's a good thing for this online health care communication and data storage system because manager is not an expert in security, and I'm not an expert too. This makes the whole system weaker facing hackers attack if we set the authentication ourselves.

4. A careful articulation of which one is best and *why*.
Taking all these factors into consideration, I ‘d say Facebook login is the best choice. There are several reasons.

The first is that it can combines your personal identity on facebook with your medical data in this app. This helps a lot to identity management and acquiring personal data from users if they permit. More data about the user can help the health system improve user experience and choose the appropriate method that user can afford.

The second reason is that Its safer than common strategy if the manager is not a security expert. Facebook Login is always managed by facebook engineers, and they tend to update it to handle the latest threat. The customers don't need to store their own password in your database. If you use another strategy to connect with your own database, then there is a chance that databases of other apps are hacked. If the customer are using their common password, then this password is leaked and no longer safe. Bad people may use that password to enter your platform and get very secure data from the app. But using facebook login can avoid this problem because facebook have multiple methods to test whether the login is valid.

The third reason is that it has many great features when using facebook login, which are very helpful when we are developing our apps and store our data. For example, it supports Cross Platform Login, which means we can easily use it on IOS, Android and Web. The Gradual Authorization also helps users to keep their personal data secure while saving a lot of time to set different levels of authorization.

The fourth is that It's easy for user to use. You don't need to set up account and remember the long password. You only need to have a facebook account. Everything on facebook account can be share, which will provide you much more convenience for medical appointments and keeping medical record. You can save all your medical data in facebook so you will not lose them.even changing to another health care system.

There are also many problems using facebook login that must be concerned.

1. Someone don't use faceboook. As we know that many people doesn't use facebook, especially the old people. And there are a lot of old people in the health system and cares this much. If they are going to us facebook login, then it feels much more complicated
2. Giving data to facebook. As we know, facebook is not trustworthy for your data. They only gonna use it for advisement and make money. Even though the health care system will not give data directly to facebook, facebook can still know some information using the login information and connection on facebook.
3. Still not a good way for communication via secure chat because facebook will know everything. If chatting with facebook listening and they use these data for advisement, that could be a very big problem.

Even though having these disadvantages, I still think that facebook login is the best authentication strategy for a health system. I believe that convenience is a very important feature for a system with many old users.

Reference

[1] https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/managing_smart_cards/using_kerberos

[2] https://developers.onelogin.com/saml

[3] https://developers.cloudflare.com/access/service-auth/mtls/#:~:text=Mutual%20TLS%20(mTLS)%20authentication%20ensures,can%20reach%20a%20given%20resource

[4] https://developers.facebook.com/docs/facebook-login/

[5] https://www.mutuallyhuman.com/blog/choosing-an-sso-strategy-saml-vs-oauth2/

[6] https://www.techlicious.com/blog/should-you-use-facebook-or-google-to-log-in-to-other-sites/

[7] https://blog.dashlane.com/login-with-facebook/

[8] https://www.theregister.com/2018/05/04/delete_facebook_login/