Effective User Authentication System in an E-Learning Platform

Aeri Lee[a], Jin-young Han[b*], [a]Professor, Department of Computer Education, Catholic Kwandong University, 24 Beomil-ro 579beon-gil Gangneung-si Gangwon-do, 25601, Korea, [b]Professor, Department of Hotel Management, Catholic Kwandong University, 24 Beomil-ro 579beon-gil Gangneung-si Gangwon-do, 25601, Korea, Email: [a]allee@cku.ac.kr, [b*]jyhan@cku.ac.kr

E-learning is a system which provides personalised learning services for anyone, anywhere and anytime with the use of information and communication technology. It is very important in e-learning that a legitimate user should access the learning system for learning and assessment purposes. Therefore, the authentication process is one of the most crucial parts in an e-learning platform. For the authentication, universities or institutions operating the e-learning system are either using the user ID and password authentication or applying ways to strengthen user authentication through a public key certificate and media access control address authentication. However, there are some issues associated with the ID/password-based authentication, namely ID and password leakage or hiring proxy exam takers or proxy attendance by accessing users' own information provided by the user. MAC address authentication contains problems such as allowing an act of cheating through a bypass and having a complicated authentication process in the case of a public key certificate. To resolve these problems, complementary measures need to be sought for the authentication system through secured authentication methods. Thereby, this paper has proposed how to determine whether the user is a legitimate user by using FIDO. As a result of comparison and analysis, it was revealed that security levels remained higher than the existing method, enough to prevent an act of cheating from occurring. In particular, the paper identified the fact that this method promotes a convenient use by users in either a mobile or web environment. The utilisation of this study is expected to serve as a good method for user authentication in the growing e-learning market. A perfect method is expected through further study to restrict proxy attendance by tightening user authentication.

Keywords: *E-learning platform, Authentication, FIDO, Security, Biometric.*

Introduction

E-learning, namely an online learning program, is an educational method which provides educational service for students in the online distance learning environment (Miguel et al., 2015). Over recent years, this new educational method has been expanding its influence with an increasingly growing number of Massive Open Online Course ("MOOC") platform services and their popularity (Xuanchong et al., 2015). Some experts recognise that this e-learning-based online learning system brings lower learning effects than offline learning does. This is because the online learning system may breed an environment that enables proxy attendance or proxy test-taking which allows an unauthorised user to attend and access and test taking while the learner is involved in something else (Assad and Azad, 2009).

A crucial factor in an e-learning environment is authentication. Most of the systems allow students to log into their own space in the e-learning environment through authentication. Their private space consists of assessments, assignments and discussion. The password-based authentication system is the most cost effective of all and is most commonly used. There is a problem associated with this password-based authentication. The password holder has nothing restrictive against anyone who is not willing to keep the password confidential (Rolf, 2013). Authentication fails to function in the following example. If student A notifies student B of his/her password, and student B takes a test with the given password on behalf of student A. To solve this problem, universities or institutions operating an e-learning system are turning to methods dedicated to tightening user authentication through a public key certificate or MAC address authentication along with the ID/password authentication (Asha and Chellappan, 2015). However, in the case of the public key certificate, the user should endure the inconvenience of having to carry the certificate for system access each time and go through a complicated authentication process (Eric and Kazimierz, 2010). When it comes to the MAC address authentication, it may allow a cheater to bypass the authentication mechanism to fall into illegal acts such as proxy test-taking and proxy attendance. This paper proposes effective user authentication methods based on biometric information with the use of FIDO2.0.

Theoretical Background

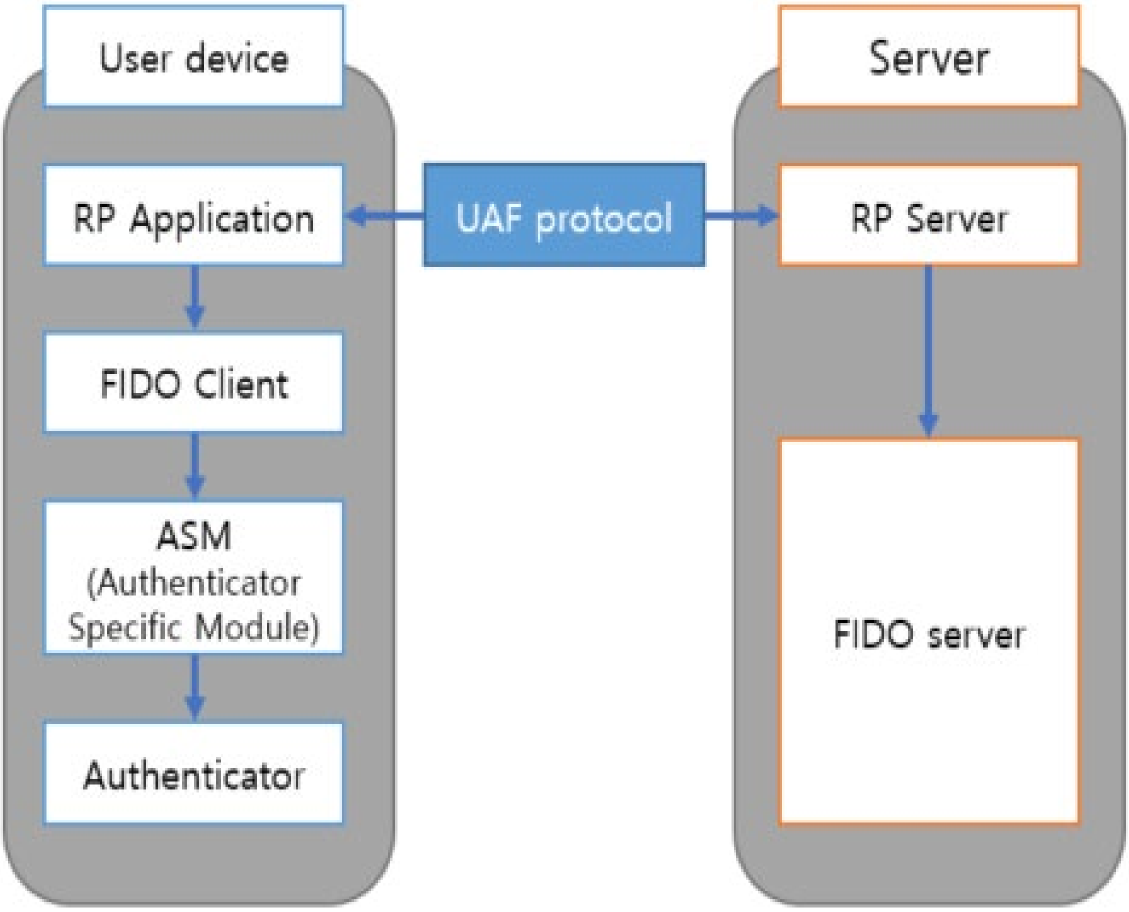
Fast IDentity Online (FIDO), which was developed by the FIDO Alliance, is a new authentication system which defines an open, scalable and interoperable set of mechanisms based on biometric information and a variety of authentication methods, without having to remember a password. Lately, FIDO biometric authentication is emerging as the next-generation authentication system to take the place of a password. FIDO authentication is a set of technology-involved security specifications designed to authenticate a user's identity in an online environment in a convenient secure manner using biometric authentication technology (Salah et al., 2017; Davit et al., 2017).

When it comes to biometric authentication, one would think about biometric authentication provided by mobile devices. At present, most mobile devices are equipped with the biometric authentication mechanism through an easy-to-use authentication application program provided by the manufacturers (FIDO alliance, 2014). This may be mistakenly considered as an authentication such as the FIDO biometric authentication mechanism. The feature provided by the manufacturer includes the automatic typing of an ID/password registered through biometric information which is stored on the device. It is not the authentication system using biometric authentication information and a public key. FIDO 1.0 consists of the Universal Authentication Framework (UAF) protocol which was intended to implement password-less authentication by using biometric data such as voice, fingerprint and facial recognition in the authentication process, and the Universal 2nd Factor (U2F) is a security process allowing the use of two different authentication factors. FIDO 2.0 also consists of the Web Authentication specification and the Client to Authenticator Protocol (CTAP) technology which implement authentication through web application programs (FIDO alliance, 2017; FIDO alliance, 2015; FIDO alliance, 2019) [11].

UAF Protocol

The first model, UAF, refers to technology designed in the FIDO 1.0 version and is used identically to the FIDO 2.0 version. This technology enables authorisation to be authenticated in association with online service based on the authentication method provided by the user device. Using the fingerprint recognition in payment service is one of the leading examples. Figure 1 shows the detailed flow of how the UAF operates. The model structure is largely divided into the user device and web server. The user device consists of the relying party applications in support of providing service and the FIDO client in charge of performing user authentication. The web server is composed of the relying party server and the FIDO server. The RP (relying party) application comprising the user device includes an easy-to-use payment app and a mobile banking app. The FIDO client searches for and calls the authentication system that meets the service authentication policy on the local device. ASM (Authenticator Specific Module), which provides standardised APIs((Application Programming Interface) so that the FIDO client can use the selected authentication system, performs the same role as the device driver. The authenticator performs its core roles of creating and managing security information actually needed for authentication, as well as identifying authentication information entered (FIDO alliance, 2014; FIDO alliance, 2015).

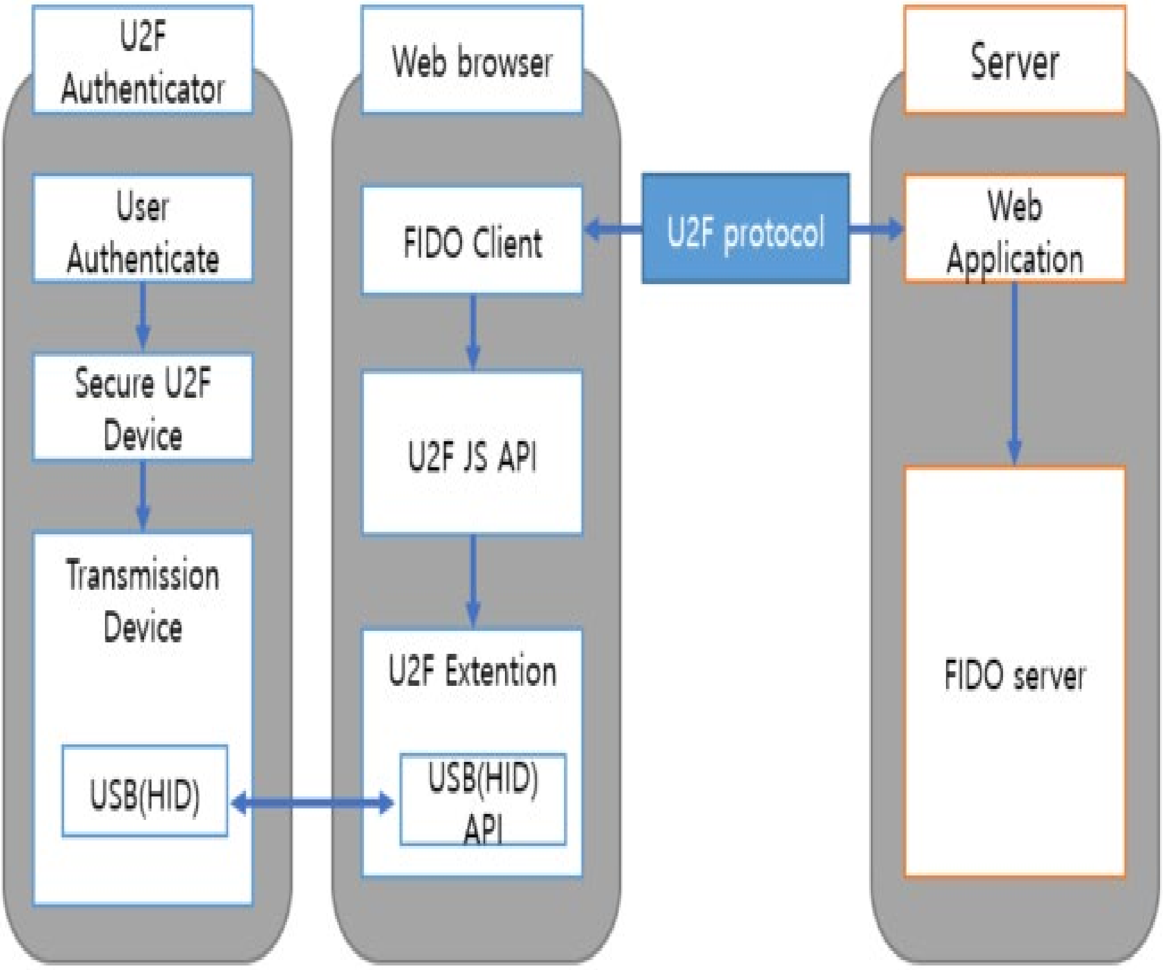
Figure 1. UAF Protocol Architecture



U2F Protocol

The second model, U2F, refers to a method that requires user authentication in the authentication service based on the existing ID and password with the use of an additional device. The additional device comes with a feature of providing a service that simplifies a password without weakening security. Figure 2 demonstrates the U2F protocol structure. A leading example of U2F authentication includes using methods such as Bluetooth, NFC and USB security keys in the secondary authentication (FIDO alliance, 2017).

Figure 2. U2F Protocol Architecture

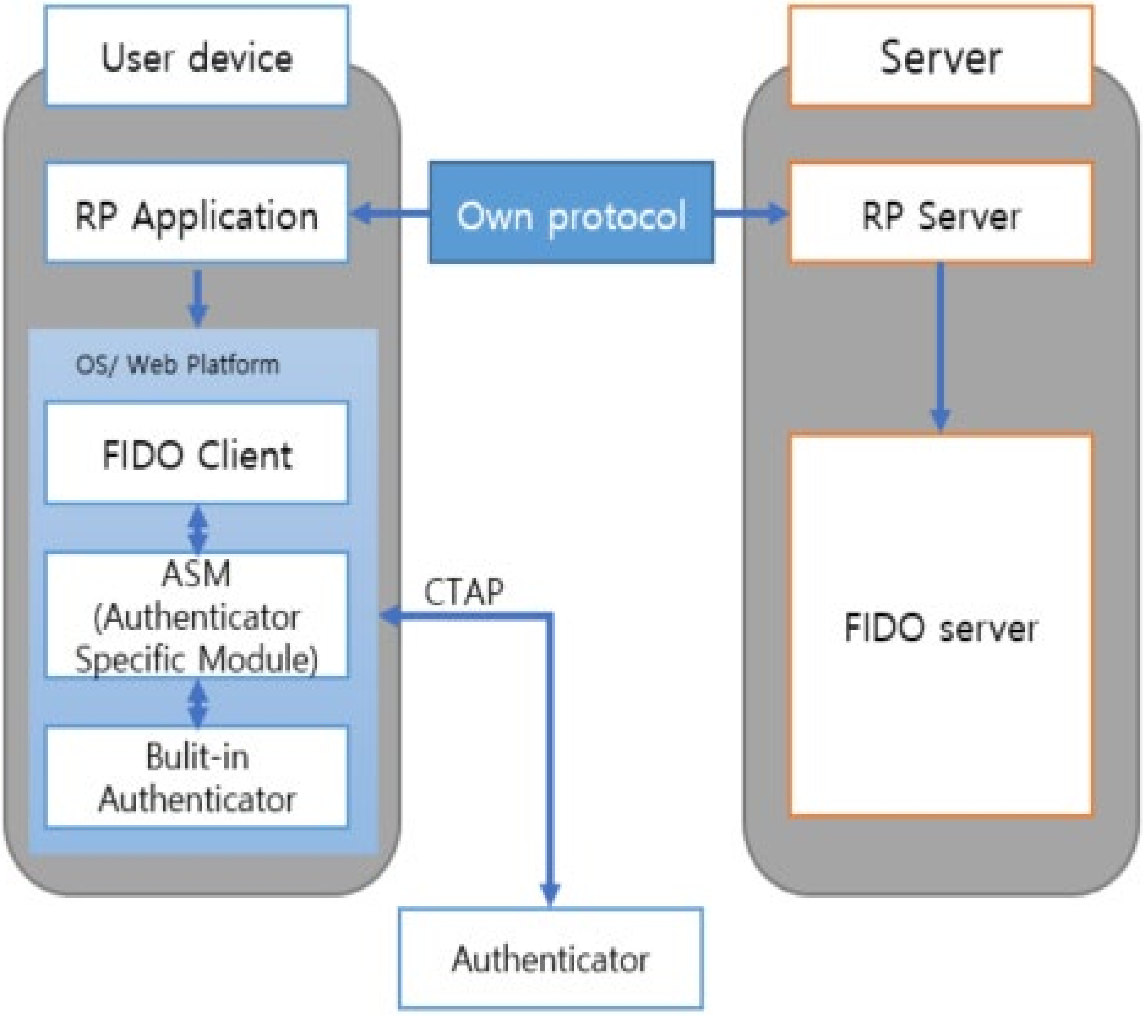


Web Authentication

Web Authentication (WebAuthn) is a standard web API that can be built into the browser and web platform infra for FIDO authentication to be used in an online service. WebAuthn uses public key encryption instead of passwords or SMS text messages to implement registration, authentication and two-step authentication on a website. WebAuthn makes use of the Client to Authenticator Protocol (CTAP) to serve as the authenticator for desktop applications and web services associated with the external device such as a mobile device or a FIDO security key (FIDO alliance, 2015; FIDO alliance, 2019).

The Client to Authenticator Protocol (CTAP), protocols used in authentication methods using an external device, refers to protocols designed to establish interlocking between the authenticator and the operating system or web browser with the use of an external device such as mobile terminals, USB, NFC and Bluetooth. After corresponding protocols took a firm stance as the standard method of interlocking, the UAF enabling biometric authentication only on a terminal itself and the U2F providing the simplified secondary authentication were built as one platform and became applicable to all online services. As shown in Figure 3, FIDO 2.0 and later versions started to apply the CTAP in support of interlocking the subject requesting user authentication and the external authenticator. Using the WebAuthn enables solving critical security issues, such as phishing attacks, data leakage, SMS text messages or other attacks associated with the two-step authentication method. Simultaneously, it improves user convenience significantly as the user finds no need to manage a complicated password (FIDO alliance, 2019).

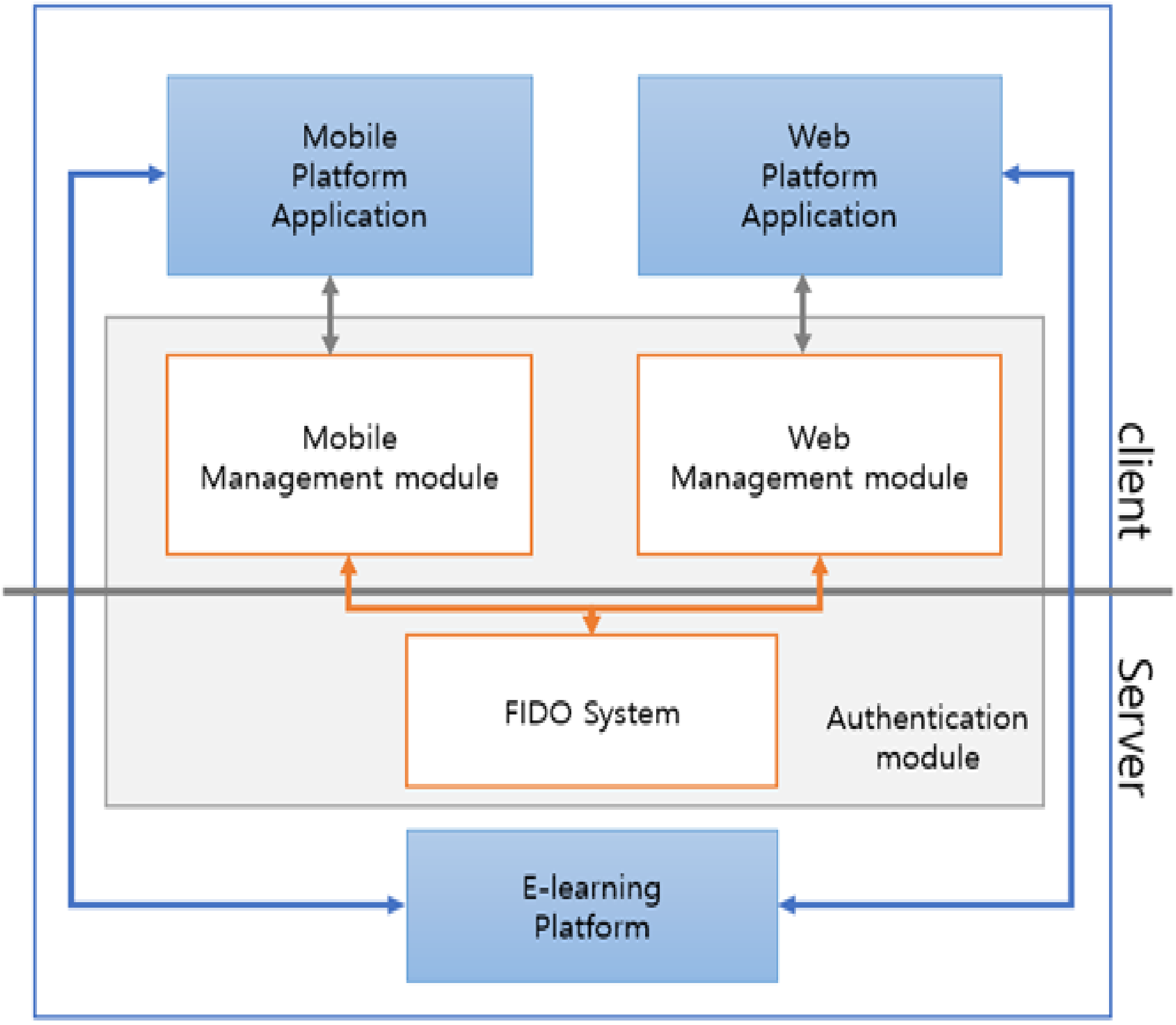
Figure 3. CTAP FIDO 2.0 Architecture



Proposed Method

This Chapter deals with a proposal made about authentication methods in improved e-learning platforms using FIDO. The overall configuration map of the proposed system is shown in Figure 4. The client side allows the mobile/web client in the e-learning platform to integrate with the manager module. The server side has the presence of both the authentication system and the e-learning platform back end. The manager module serves as the role of a mediator between the e-learning platform client and the biometrics recognition authentication system executed in the server. The authentication system in the proposed method is implemented largely in a total of four processes that include registration, authentication, search and deletion.

Figure 4. Proposed Method

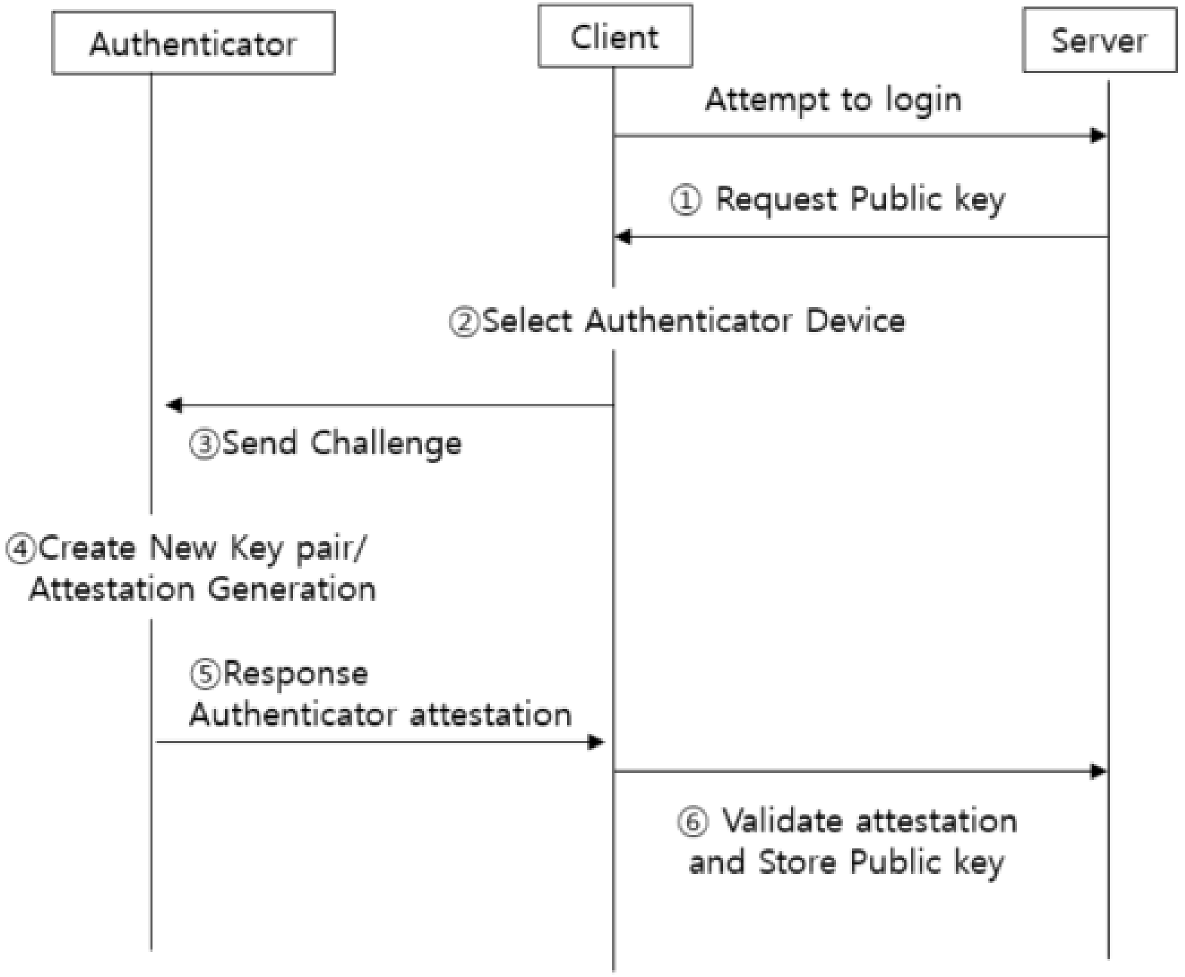


Registration Process

The registration process is a process which allows the first-time service user to go through the user verification through the authentication system and to submit to the server the return value for the value requested from the server via the authentication system for verification. The FIDO 2 registration process usually takes the following order.

First off, it is assumed that the client-server account has been set up in advance and this is not related to FIDO authentication. User identification authentication methods and procedures performed in the setup process can be determined by the server. Figure 5 shows the FIDO registration process.

Figure 5. Registration Process



① The server which has completed the account setup transmits to the client the acceptance policy of the authentication system suitable for service levels and challenge values for signatures to request the registration of a public key to be used in account authentication.

② Upon the receipt of the corresponding request, the client selects the authentication system that best matches the acceptance policy on the server.

③ The client sends the challenge values back to the authentication system.

④ The authentication system in receipt of the requested messages creates a key pair for authentication for the corresponding service before creating the attestation for the purpose of the safe deliverance of a public key for authentication. During this process, the authentication system can include as optional the user authentication on the local side such as biometric authentication.

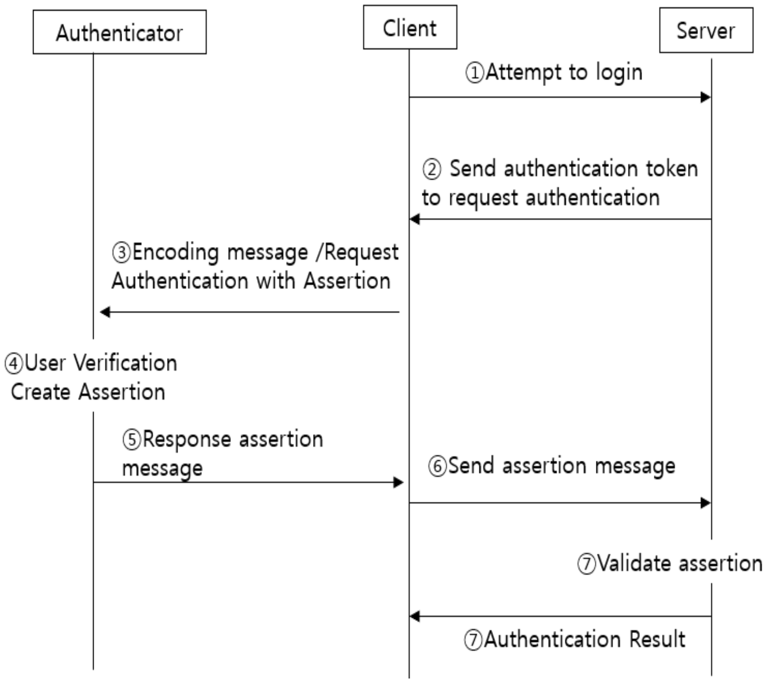
⑤ Set the key handle so that this can be uniquely distinguished in the server-domain part. Then, the authentication system creates an attestation signature with a private key for a verified certificate set at the first production. The next step is to transfer four elements that include the attested signature, the user public key, the key handle and the verified certificate to the server side through the client.

⑥ The service upon receipt of the elements makes use of a public key for verification to first verify the signature for verification delivered from the authentication system using the public key for verification. It is then confirmed that the verified authentication system is consistent before saving the user public key and the key handle to DB(Server's Database).

Authentication Process

Figure 6 shows the FIDO user authentication process.

Figure 6. Authentication Process


Authenticator
Client
Server
①Attempt to login
② Send authentication token to request authentication
③Encoding message /Request Authentication with Assertion
④User Verification Create Assertion
⑤Response assertion message
⑥Send assertion message
⑦Validate assertion
⑦Authentication Result

The client accesses the server and receives the requested message from the server. (This message includes server information such as URLs on the service server and the original signature. The plain text original signature was performed with the FIDO 2 authenticator and can be signed with a user private key when needed.)

① The client in need of authentication for a specific account user accesses the server.
② The server sends a random authentication token to request authentication.
③ The client completes the encoding of the requested message received and delivers it to the authenticator connected to the primary terminal.
④ The authenticator that has received the requested message goes through the authentication process on the local side such as biometric authentication before electronically signing values needed for verification with an authentication private key created in the registration process. It then creates assertion messages together with the security parameter with the inclusion of the values.
⑤ The authenticator encodes the assertion message into a defined type and transfers it to the client.
⑥ The client in receipt of the response message encodes the message into an appropriate type and transfers it to the server.
⑦ The server in receipt of the assertion message verifies it using the public key registered in the corresponding account.
⑧ Once the verification is successful the server identifies the user to be authenticated owns the authenticator with a public key registered in the corresponding account. This is how to take the place of user authentication.

Reference Process

The user needs to check if his/her biometric data has been registered correctly on the server. User registration data is used for authentication through an identification (ID). The user is entitled to identify the reference process by searching the database installed in the authentication server.

Deleting Process

To delete the user, the user can search for an ID used at the time of registration through the database installed on the server and delete all user data (ID, biometric data and etc) associated with this from the database. In addition, the user will need to delete part of a client segmented biometric data template which is also stored.

Effects of the Proposed Model

Traditional user ID/password authentication systems are vulnerable in terms of security. As an example, hackers may steal the user's ID and password with the use of sniffing techniques. However, the authentication-based method or MAC address authentication guarantees security as it installs security modules. The proposed model adopts an external biometric authenticator based on FIDO 2, making it very difficult to leak the user private key stored inside the authenticator. This means its security level is improved when compared to the existing electronic signature for which data is saved to a hard disk using plugins.

In terms of user convenience, users find it convenient to learn once verified with the login system. But, the public certificate system or MAC address authentication system comes with such inconvenience as requesting users to have a public certificate handy or to register MAC address again, e.g. when needing to use a different system. This proposed model is dedicated to keeping the user private key saved securely by combining the existing user certificate with FIDO 2 web standards. In addition to this, the model is regarded to have improved security and convenience in user authentication since it is applicable anywhere under the mobile or web environment in a convenient manner without the need of separate programs for certificate management and keyboard security.

Proxy attendance is the most crucial part in e-learning. MAC address was used to filter the fake users in order to prevent the actual users from requesting others to attend the class on their behalf. This happened quite often when they attended the class both at home and the workplace simultaneously. The electronic signature introduced in FIDO 2 allows the original signature to be created from the server and transferred to the client. Then, the client adds his/her data to the original making it very difficult to counterfeit the original (like a memory hacking) and ultimately prevents proxy attendance thanks to the use of individual's unique biometric data.

Conclusion

This paper has proposed authentication techniques of FIDO-based e-learning platforms using biometric data. The authentication method used in conventional e-learning platforms shows low security levels over a guaranteed usability and low convenience over enhanced security levels. This method also failed to prevent proxy attendance from occurring. As the proposed method adopts an external biometric authentication system, it is very difficult for the user private key saved to the authentication system to be leaked. This method led to enhanced security over the existing electronic signature for which data is saved to a hard disk using plugins. Besides, the security of saving the user private key was secured by combining the existing user certificate and FIDO web standards. Since this model does not need a separate program for certificate management and keyboard security, it is regarded to improve security and convenience in user authentication. In the FIDO 2 based electronic signature, the original signature is created from the server and transferred to the client which then adds his/her data to the original, preventing the forgery of the original such as can occur from hacking. It can also prevent proxy attendance due to the use of individual's unique biometric data. This paper concluded that the system proposed through the comparison and analysis is an effective system that improves security and convenience, further preventing proxy attendance from taking place. The proposed method is expected to enable the convenient and safe user authentication and identification anywhere, as long as the user owns a simplified authentication device through the user authentication method with FIDO standard protocols. This paper will continue on to examine how to enable continuous real-time authentication.

REFERENCES

Asha, S. and Chellappan, C. (2015). Authentication of e-learners using multimodal biometric technology. the Proceedings of the International Symposium on Biomet rics and Security Technologies, IEEE. 2008:1-6. DOI:10.1109/ISBAST.2008.4547640

Assad Moini. Azad M Madni. (2009). Leveraging biometrics for user authentication in online learning: a systems perspective. IEEE Systems Journal.; 3(4):469-476.

Davit Baghdasaryan. Brad Hill. Jeff Hodges. (2017). FIDO Technical Glossary. FIDO Alliance.

Eric Flior. Kazimierz Kowalski. (2010). Continuous biometric user authentication in online examinations. the Proceedings of the 7th International Conference on Information Technologies.: 488-492 .DOI: 10.1109/ITNG.2010.250

FIDO alliance. (2014). FIDO UAF Protocol Specification v1.0. https://fidoalliance.org /specs/fido-uaf-v1.0-ps-20141208/fido-uaf-p rotocol-v1.0-ps-20141208.html.

FIDO alliance. (2015). FIDO2.0 : Key Attestation Format. FIDO Alliance Proposed Standard. https://fidoalliance.org/specs/ fido-v2.0-ps-20150904/fido-key-attesta tion-v2.0-ps-20150904.html.

FIDO alliance. (2017). Universal 2nd Factor (U2F) Overview. https://fidoalliance.org /specs/fido-u2f-v1.2-ps-20170411 /fido-u2f-overview-v1.2-ps-20170411.html

FIDO alliance. (2019). Specifications Overviews. https://fidoalliance.org/specifications/

Miguel J, Caballé S. Xhafa F. (2015). Security in online web learning assessment. World Wide Web 18 Springer. 18(6):1655–1676. DOI:10.1007/s11280-014-0320-2

Rolf Lindemann. (2013). The evolution of authentication. ISSE 2013 Securing Electronic Business Processes, Springer.11–19. DOI:10.1007/978-3-658-03371-2_2

Salah Machani. Rob Philpott. Sampath Srinivas. John Kemp. Jeff Hodges, (2017). FIDO UAF Architectural Overview. FIDO Alliance.

Xuanchong Li, Kaimin Chang , Yueran Yuan, Alexander Georg. (2015). Massive open online proctor: protecting the credibility of MOOCs certificates. Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing, ACM;1129–1137.