ABOUT ENHANCED ACCESS CONTROL USING FIDO2 AUTHENTICATION AND ATTRIBUTES

Zhidovich A., Lubenko A., Vojteshenko I.
Faculty of Applied Mathematics and Computer Science, Belarusian State University
Minsk, Belarus
E-mail: {anton.zhidovich, alexeilubenko02}@gmail.com, voit@bsu.by

In this paper a joint use of the FIDO2 specification and attribute-based access control with support for reading attributes from electronic documents is proposed. Existing solutions and implementation options are reviewed. This provides an opportunity to improve access control methods to information and resources.

Introduction

When building a corporate system, it's necessary to give special priority to the issue of access to system resources and the differentiation of user rights. The key concepts here are authentication and authorization. These two processes are closely interrelated and must be implemented to meet the security and scalability requirements of the information system, while ensuring usability and accessibility for users.

There are various authentication standards, many of which may not provide a high level of security and may be compatible only with a particular class of software or may be proprietary.

I. Relevance of FIDO2 technology

Passwordless authentication allows a user to access an information system without entering a password or answering security questions. Instead, the user provides other form of evidence such as a fingerprint, NFC-chip, or hardware token code [1].

The modern approach to passwordless authentication is the open standard FIDO2, jointly developed by the FIDO Alliance and the W3C consortium. The FIDO2 specification uses public-key cryptography and consists of two groups of standards. One of these is called the W3C WebAuthn standard. The second part is the Client to Authenticator Protocol (CTAP, CTAP1, CTAP2).

The following benefits can be pointed out:

1. Resistance to phishing, MITM, replay attacks;
2. Variety of built-in authenticators with fast secure access;
3. Ease of implementation;
4. Enhanced privacy for users.

See, for example, [2] for a more detailed overview of the FIDO2 specification, its benefits and workflow.

FIDO2 authentication is increasingly used in information systems in different areas. For example, online banking services of such banks as Priorbank, Belinvestbank, Sberbank, and e-mail services like Mail.ru.

II. Attribute-based access control

Attribute-Based Access Control (ABAC) is an authorization model that uses attributes to determine user rights. The key advantage of ABAC is its flexibility. The method can solve a wide variety of access issues with minimal administrative control [3].

ABAC offers a series of benefits, such as:

1. Possibility to construct similar to business concepts rules;
2. No limitation on the complexity of the rules;
3. Rules with dynamic parameters supported;
4. Possibility of filtering the data user has access to.

This authentication model is getting more demanded and finds application in many fields. In [4], the ABAC model is proposed to be used to manage access to emergency patient data. With the designed prototype, the authors evaluated the resulting authorisation system. ABAC is also used in IAM services on such platforms as Amazon Web Services, Microsoft Azure and Okta.

In the ABAC systems anonymous attributes can be used for access decisions. For example, confirmation of age without the need for personal identification.

The joint use of FIDO2 authentication and ABAC can significantly increase the level of flexibility and scalability of a security system. Importantly, these are two different processes, and the FIDO2 specification (specifically WebAuthn) doesn't provide such integration. Consequently, configuring ABAC and FIDO2 together may require additional effort and resources specific to each system. For example, if dynamic attributes (such as location) are in the system, integration with FIDO2 authentication will require the implementation of mechanisms to collect and update this data without violating the requirements of the specification.

III. Electronic identification

The key issue is selecting the appropriate source of user attributes. One suitable option is to use electronic documents that store the issuer's signature.

Electronic identification (eID) is a smart card or biometric passport with an embedded RFID-microchip that contains a biometric identification tool with the holder's data in accordance with the ICAO standard [5]. The following security protocols ensure high level of protection and data integrity:

1. Basic Access Control (BAC) is designed to ensure that card data is only accessed when the card is physically reached.
2. Passive authentication allows the reader to verify eID data authenticity.
3. Chip authentication is designed to protect document data from being altered and cloned.

The use of eID promotes interoperability at the legal, semantic and technical levels, making it an efficient and convenient way of confirming identity in the digital environment.

IV. Existing solutions

The use of the ABAC model based on OAuth2.0 protocol is proposed in [6]. This is a reasonable solution, but in this case there is no way to verify the user data given by the service provider.

In [7], a complete and industry-ready solution for using anonymous credentials with local or remote attestation through a FIDO2 channel is proposed in the form of the FIDO-AC framework, which is an extension of the basic FIDO2 specification. An evaluation of the security and privacy provided by the system and the realisation of a working prototype are also presented.

The essence of the resulting solution is the creation of an additional trusted party - a mediator. This party is responsible for validating the user's data, for example from an eID document.

Thus, the FIDO-AC identifies the following parties to the authorisation process: FIDO-server (relying party), authenticator, client, mediator, FIDO-AC application and eID. The authorisation workflow largely follows the standard FIDO2 authentication process, which is also described in [2]. The FIDO-AC application is designed to perform BAC and to read data from the user's eID. The mediator, in its turn, should check the verification of the data received from the eID, i.e. perform passive and chip authentication. The FIDO-AC access control process is presented in detail in [7].

V. Implementation options

In this section, the use of biometric documents of the Belarus compliant with the ICAO standard is proposed to improve the access control system and ensure user security.

To implement a FIDO server, it's reasonable to use the cross-platform ASP.NET Core. It enables the development of a single solution for both user interface and the web API, and provides extensive deployment and scalability options. To develop a controller that allows the web application to act as a relying party (i.e form FIDO2-compliant queries and verify responses), the component released by Rock Solid Knowledge for the ASP.NET Core 6.0 platform can be used [8]. Web hosting services such as Somee and Google Cloud Platform are suggested for testing and debugging the web application. Also, most deployment scenarios assume containerisation with Docker. For real use, the application is deployed on the company's corporate server.

Currently, desktop and mobile web browsers have built-in WebAuthn API support, so any of them can act as a client. To generate client-side requests and invoke WebAuthn API, the server will send a JS-program.

Since the FIDO-AC protocol does not require physical separation of the mediator and FIDO-AC application sides, they can be merged into a single application. In this case, no concern for the secure connection between the mediator and the FIDO-AC application is required.

Android can be chosen as the platform for the application, in this case the device must have a built-in NFC-sensor to read data from the eID.

In order to realize correct and proper interaction of android device with biometric document, JMRTD-component [9] can be used. JMRTD provides the ability to connect to an eID, retrieve data from it and perform the verification described above, supporting ICAO standard documents.

References

1. Passwordless Authentication [Electronic resource] – Mode of access: `https://www.cyberark.com/what-is/passwordless-authentication/`. – Date of access: 05.10.2023
2. Semantic Approach to Designing Applications with Passwordless Authentication According to the FIDO2 Specification / A. Zhidovich [et al.]. // Open Semantic Technologies for Intelligent Systems – 2023. – № 7. – P. 311-316.
3. Casey K. What is Attribute-Based Access Control (ABAC)? [Electronic resource] / K. Casey // Okta company blog. – Mode of access: `https://www.okta.com/blog/2020/09/attribute-based-access-control-abac/`. – Date of access: 04.10.2023.
4. AC-ABAC: Attribute-based access control for electronic medical records during acute care / Marcela T. de Oliveira [et al.]. // Expert Systems with Applications. – 2023. – Vol. 213, part C.
5. Doc 9303 [Electronic resource] // ICAO. – Mode of access: `https://www.icao.int/publications/pages/publication.aspx?docnum=9303`. – Date of access: 14.10.2023.
6. Belovodov, A. Using attribute-based access control in the OAuth 2.0 protocol / A. Belovodov, O. Laponina // International Journal of Open Information Technologies. – 2023. – Vol. 11, № 6. – P. 182-189.
7. Fast IDentity Online with Anonymous Credentials (FIDO-AC) / Wei-Zhu Yeoh [et al.]. // Proceedings of the 32nd USENIX Security Symposium. – 2023 –P. 3029–3046.
8. RSK IdentityServer [Electronic resource] – Mode of access: `https://www.identityserver.com/` – Date of access: 10.10.2023.
9. JMRTD [Electronic resource] – Mode of access: `https://jmrtd.org/`. – Date of access: 11.10.2023.