BOIDI : Blockchain-based Open ID Infrastructure

ID;2d9fad408689749b4c6b339690c4cad332c216ef6d8d18ac77ea2741b260b89d

Revision 0.2 - November 26, 2017

1. Abstract

Today we are using many online services such as E-mail, SNS, blog, cloud, etc. As we start running new services or using them, the number of account of them increases to be huge for each user to control their statuses, passwords, or security.

Although there are services called Social login, a kind of Single Sign-On; SSO, that enable us to login various accounts by unified ID and password, there are some other problems remaining.

BOIDI is suggested in order to solve these problems. On BOIDI, people can create a unique account which contains common ID and passwords specified for each service easily and safely. Its safety does not depend on application service providers because users' personal information is double-encrypted by both user itself and the providers and to be broadcasted to blockchain. So no information connected to individual user would remain in the providers' storages. Also, the providers can manage data with less concern of leak of personal information and less storage availability.

Enabling BOIDI on consensus between users and the providers would be able to benefit both stakeholders.

2. Keywords

Blockchain, ID, authentication, social login, single sign-on (SSO), password, personal information

3. Issues and Solutions

3.1 Problems of Social Login (and SSO)

Social login is now very popular way for convenient login, however, they have some problems. I'm dealing with only some major problems in this paper.

The first one is that the variety of social login service and their compatibilities. Because we have no consensus that which service is to be standard, we have to manage some accounts to login other accounts. And if you now want to register for an account of application service which certain social login service is available, there might not be the option of social login service whose account you have already gained.

The second one is the security problem. Using social login service sometimes means that you use only one set of ID and password. When someone would succeed in breaching security of those services, your information saved (not only in the breached service, but in all services you have logged in using the breached social login service) would be compromised.

3.2 Issues

Considering present problems, BOIDI is made to respond the following issues;

- How to avoid missing of IDs and passwords.
- How to avoid leak of information from providers of application services or social login.
- How to use online services without permanently trusting their providers to allow them to save our personal information in their own storages.

3.3 Solutions

Solutions which BOIDI proposes for issues in 3.2 are;

- Using truly common and unique ID infrastructure which is based on blockchain and has no single provider to remember users' personal information.
- Double-encrypt the personal information and save it not in the providers' server but in blockchain in order to allow the providers to read it only when a user logs in.

4. Features

4.1 Blockchain

Blockchain is a chain of hash-based proof-of-work[1]. BOIDI use its feature of checkability, disclosing, and time order. Firstly, when a user starts using BOIDI, he/she creates his/her unique ID and broadcast it to blockchain, and then he/she have completed the registration. Soon after registration, ID will appear in a block and disclosed for everyone. At this time, the user need to remember his/her ID and number of block in which his/her ID is stored.

4.2 Registration for Application Service

When a user visit the website of some application service provider using BOIDI and want to register to use the service, they give their ID and encrypted personal information which they want to give or requested by the provider to the provider. The encryption key of this process will be the password to login the service, so the user do not have to allow the provider to save it in their storage. Next, the provider re-encrypt the information and broadcast it to the blockchain, linking to the user's ID. After these process, registration for each service is done and no one without user itself knows the content of the information.

4.3 Logging In to the Service

After the double-encrypted data is broadcasted to blockchain, the user can login to the service with BOIDI. As the user type the common ID and password to the form in the website of service, the service provider search the data which linked to the user's ID on blockchain, and decrypt with provider's key then user's (temporary given) key. After that, the provider load the user's information temporarily without saving it to their own storage. When the user logs out the service, the provider clear all the information they gained include user's password from their servers (which means they use the information only temporarily).

If there is some change of information, the user rewrite the content, then pass it to the provider, and the provider re-broadcast to blockchain. Also, if the user wants to change the password, the user encrypt the information by

---

[1] [Nakamoto, 2008]

new key, then the provider encrypt by their key, and broadcast it. Blockchain having the feature of time order, the provider can recognize which information is the newest when they need to get the information next time.

4.4 Possibility of Attack

Lacking of BOIDI, the providers would have experienced many attacks which leaks personal information of users. It is because that it is obvious that there are valuable information in providers' servers, and attackers can get some money or pleasure by cracking it. But in the BOIDI-enabled world, there would be less possibility of attack for providers because they have no valuable information, which means a lot of personal information, in their own storage, and they are all on the Internet openly. However, encrypted, personal information would never be compromised unless its encryption should be breached.

5. Discussion

Although there are many advantages of enabling BOIDI, there are some tasks we need to work on. In particular, decision of protocol is the most important. The system which avoid providers from saving user's personal information or make that behavior result in disadvantage for the provider must be decided in the protocol.

In addition, saving personal information in blockchain means that no one can delete them from the block. Although they are secured by double-encryption, some users might want to delete completely from the Internet. How to deal with these new problems is the next issue.

Revision History

Rev.0.1	2017-11-17	Initial revision
Rev.0.2	2017-11-26	2nd revision

— End of Document —