

PASSBAY.COM

Free Online Password Manager

White Paper on Passbay Security

Date: April 24, 2007

PASSBAY.COM

All copyrights reserved. Aeware International Limited. Passbay® is registered trademark.

<http://www.passbay.com>



I Summary

Considering about the sensitivity of online password storage service, we understood that the security was the no. 1 question of all that should be concerned. Besides general security measures, special security architecture was utilized, whose effectiveness can be assessed using a quietly simple principle:

The sensitive data can not be accessed freely even by Passbay's staff including developers.

It is not as complicated as it looks to achieve the above target:

- i. to encrypt all the sensitive data according to the password held by Passbay user.
- ii. all the encryption and decryption are executed locally on the user's computer.
- iii. the user's password is strictly used in a limited scope, that is, it only appears in the user's computer.

In that case, no one, including Passbay's staff or other potential attackers, can access the decrypted data even if he/she has the entire database.

II Background Knowledge

1 The BlowFish Encryption Algorithm

Passbay uses BlowFish, designed by Bruce Schneier, as the basic encryption algorithm.

Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Since then it has been analyzed considerably, and it is slowly gaining acceptance as a strong encryption algorithm. Blowfish is unpatented and license-free, and is available free for all

uses.

About BlowFish algorithm, please refer to Bruce Schneier's website:

<http://www.schneier.com/blowfish.html>

2 Adobe Flex 2

Flex Application is a small program written in ActionScript programming language, which can be embedded in HTML page and executed in client end.

Passbay uses Flex Application to deal with the security concerned procedures.

- i. Flex Application adopts SandBox mode which ensures the application can not access user's local resources and can not do harm to user's computer, and this is considered quite secure for internet users. Users don't have to worry about the security issues while using it;
- ii. Flex Application supports cross-platform, that means, end users can use operating systems other than Windows;
- iii. All web browsers in market can support Flash Player, including Internet Explorer, FireFox, Opera and Maxthon;
- iv. Flex Application is mainly in binary form that is different from the scripting languages such as ASP or PHP. It is difficult for attackers to trace the execution of Flex Application, and the webpage analyzing tools or Trojan programs can not steal the protected secrets.

Please refer to the Adobe website for more information about Adobe Flex 2:

<http://www.adobe.com/products/flex/>

III Passbay Password

The Passbay password held by Passbay user is very important in our security architecture. It is the necessary way and the only way to access the user's protected data.

1 How to Protect Passbay Password?

There are two principles for protecting user's Passbay password:

- i. **The password itself or any data from which the password can be recovered is not saved in the server end of Passbay.** Nobody, including Passbay's staffs, can get any user's Passbay password even if they have the entire Passbay database in hand;
- ii. **Passbay password only appears in user's computer, no matter what kind of operations is executed: creation of user profile when registering, logging to Passbay server, changing or retrieving passwords.** It is used in the Flex Application and won't be sent to server end through Internet, even the web pages are not allowed to access Passbay password without explicit confirmation from user.

All operations involving with user's Passbay password will be executed in Flex Application, including:

- i. **To Input Password:** when registering, that is, creating a new account, or signing in, or changing the password, users are asked to input the password(s). In these cases, Flex Application will show edit box(es) to accept user's input;
- ii. **To Display password:** while retrieving the password, the password in plain text and the encrypted password data are also displayed by Flex Application.
- iii. **Encryption and Decryption:** all encryptions and decryptions are executed by Flex Application in terminal end without leaking of users' passwords.

When logging in, user can enable the soft keyboard to input the Passbay password by clicking mouse. This can help avoid the key logging Trojan program.

2 How to Retrieve Passbay Password?

When Passbay user enables the feature of password retrieval, the Flex Application will produce a temporary random secret key to encrypt the

Passbay password and show the encrypted result string to the user. Then user can copy and save this string or ask the Passbay server to send the string as an email to the address provided upon registration. The encrypted result string is embraced with "###". Here is an example:

###C53F FF3B 8751A106D9A291C 4E9CD86061D194C3CB EED5FA3###

Once the user forgets the password, he/she can get the password back by providing the result string to the Flex Application

The Passbay password can be retrieved successfully only when the three conditions below are met:

- i. User enabled the password retrieval feature of his Passbay account;
- ii. User can provide the correct answer to the password retrieval question previously configured;
- iii. User can provide the encryption result string previously produced by Passbay.

(Flow chart omitted)

3 Instructions for Passbay Password

We have done what we can to protect the user's data encrypted with the Passbay password held by the user, and now it is user's responsibility to keep their Passbay password safe. We hope you can our advice as follows:

First of all, choose a good password.

Here a good password must meet two conditions: strong enough and easy to remember. Theoretically, these two conditions are sometimes contradictory, but it is not the case in reality. For examples, the passwords below can be considered as safe:

I's12n&lah: 50% (It's 12 noon and I am hungry)

Myfa'snaisJaSm: 69% (My father's name is James Smith)

Secondly, Change the password regularly.

It is not as trouble as imagined to change a password regularly. It is advisable to change the password once a month. With the great features offered by

Passbay, users are only required to remember the Passbay password to access all frequently visited sites. This helps a lot for users' surfing the internet freely.

IV Protection Of User's Sensitive Data

1 Protection of user's credentials

User's all private data are saved in database after encrypted with a secret key which is created and encrypted using user's Passbay password while user registering. In another word, all data can not be decrypted without user's Passbay password.

(Flow chart omitted)

2 Protection of user's password data: server end

All password data saved in Passbay are double encrypted. Before being sent to server, the password data is encrypted by Flex Application in user's computer, and before being saved in database, the password data already encrypted is encrypted again together with user name and other data items which should be provided to the target websites while logging in.

(Flow chart omitted)

3 Protection of user's password data: client end

User's password string will not be displayed on user's computer screen. The only exception is when user wants to see it. In this case the password will be displayed as a scrambled image to avoid Trojan sniffer.

V Others Security Measures

1 The Security of Data In Transportation

HTTPS protocol is widely used to protect the data in transportation, especially in the case where the highest security level is required, for examples, e-banking and online transactions. While utilizing HTTPS protocol, all data transferred between user's computer and Passbay server are encrypted. No one can access or modify the actual data transferred by sniffer.

Please refer to the below link leading to Microsoft website to know more about HTTPS protocol:

<http://msdn.microsoft.com/workshop/networking/predefined/https.asp>

You can visit the website of COMODO who provided SSL certificate service for Passbay:

<http://www.comodo.com>

2 The Security Of Passbay Server

Our servers are placed in the world class data center with 24 hours a day, 7 days a week secured facilities and high performance network connectivity located in Hong Kong. This can help Passbay to accept worldwide visitors.

If you have any queries about security, welcome to discuss with us:

security@passbay.com