September 2014
Version v1.8

PasswordBox

Thank you for your interest in PasswordBox. On the following pages, you'll find a technical overview of the comprehensive security measures PasswordBox uses to protect your passwords. These processes are vital to achieving our goal of safe-guarding user data while maintaining an overall user experience that is simple and effective.

Our software and systems architecture was built with maximum security in mind from the ground up.

Our Key Security Features Are:

- All passwords and wallet data is strongly encrypted on users' own devices (Client-Side Encryption); no unencrypted password data ever leaves the user's device
- We use AES 256, the strongest encryption available
- The user's Master Password:
  - Is never transmitted over the Internet or the local network
  - Is never stored, either on the user's device or on any server
- Encryption keys are generated from the user's Master Password with a random salt and 10,000 rounds of PKCS5_PBKDF2_HMAC_SHA2
- We use the best available cryptographic code libraries that have been subjected to extensive third-party review
- Passwords can be shared and bequeathed using RSA 2048-bit public-key encryption
- Our servers are hosted in a highly secure data center facility with multiple third-party certifications including PCI-DSS level 1, HIPAA, SSAE 16 SOC 1 Type 2, SOC 2 Type 2, SOC 3, ISAE 3402, and ISO/IEC 27001:2005
- By design, it is impossible for any PasswordBox employee to access users' passwords or wallet data
- In the unlikely event that an intruder could gain access to PasswordBox servers, they would find only strongly-encrypted passwords and wallet data there

The following sections of this White Paper provide further detail on each of these capabilities.

Security Architecture Design

Browser Extension Architecture

In order to provide a high level of security together with the convenience of operating directly from within the user's browser, PasswordBox provides browser extensions that employ the best available, widely peer-reviewed cryptographic libraries to protect user's data. The PasswordBox browser extensions employ the best available cryptographic code libraries for both Javascript and native code.

User Sign Up

During the sign in process, the user generates their own Master Password, which will be used as the basis for the cryptographic keys used to encrypt the user's data. To ensure that the user selects a high-quality Master Password, PasswordBox utilizes the zxcvbn password strength estimation library to provide immediate and realistic feedback to the user on the strength of their chosen password.

Additionally, in case the user's initial choice of password is insufficiently strong, PasswordBox will automatically later invite the user to enhance the complexity of their Master Password.

<u>The Master Password is NEVER stored or saved</u>

- It is never stored on PasswordBox servers
- It is never stored locally on any device
- It is never transmitted over the Internet or any local network

User Sign In

Users are authenticated when they sign in to PasswordBox using their Master Password. This is done without transmitting the Master Password over the Internet. To sign in, the user starts by entering his Master Password, which is used to compute and send an authentication hash, as follows:

1. The user enters their Master Password
2. The standard Password Based Key Derivation Function PBKDF2-HMAC-SHA256 is used, along with a salt guaranteed unique for every account and a large iteration count, to generate an authentication hash
3. The derived authentication hash is sent via SSL to a PasswordBox server for authentication

4. The PasswordBox server computes a bcrypt hash of the PBKDF2 hash received from the client, and uses that to authenticate the user

Data In Transit

All communication between the user's device and PasswordBox is further encrypted at all times with TLS / SSL as an additional layer of security.

The TLS / SSL protocol operates as follows:

- Client and Server negotiate to choose the best cipher and hash algorithm available to each
- Server transmits its digital certificate
- Client verifies certificate is signed by a trusted Certificate Authority
- Client and server negotiate a temporary session key using the Diffie-Hellman key agreement protocol
- Alternatively, if the client doesn't support DH, the client generates and encrypts a random number with its public key and transmits the encrypted number to the server. Both sides use this number to generate the session key
- The new session key is used to encrypt all subsequent traffic between the client and the server

PasswordBox servers properly handle the negotiation of TLS / SSL cipher suites, and are not vulnerable to the BEAST Attack.

Additional security measures are also in place to safeguard the session established between a user's device and PasswordBox servers.

HTTP Strict Transport Security

PasswordBox servers comply with the HSTS specification to allow the user's browser to communicate with PasswordBox using HTTPS only. This security mechanism effectively prevents SSL-stripping attacks in the event that a user connects to PasswordBox from an untrusted network.

Cookie Attributes: Secure and HttpOnly

The secure and HttpOnly attributes are present in all sessions, which in turn ensure respectively that cookies are only sent over secure connections, and that the cookies cannot be accessed over non HTTP(S) methods.

Client-Side Data Encryption/Decryption

When a user has successfully logged in to PasswordBox (as described above), the PasswordBox servers synchronize the user's passwords and wallet data, in encrypted form, to the client. The PasswordBox client must then decrypt the data that was sent to it. This is performed as follows:

1. The user's PasswordBox client receives a local copy of the AES 256-bit ciphertext which was synced through PasswordBox after authentication.
2. The user's PasswordBox client computes the Encryption Key using PKCS5_PBKDF2_HMAC_SHA2":
    1. The user's unique 256-bit salt; and
    2. The user's Master Password
3. When the Key Encryption Key is computed, the user can then decrypt his ciphertext using AES-256 in CCM mode.

When the user adds, changes, or deletes data, the user's PasswordBox client encrypts the data using the same process on the user's own device, and transmits the new ciphertext to PasswordBox.

Sharing Data

PasswordBox is unique in allowing users to share password data securely using a patent pending end-to-end encryption process. RSA 2048-bit and AES 256-bit encryption are used to share the encryption key and to encrypt / decrypt data. When the user chooses to share a password with another user, this works as follows:

1. A fresh 2048-bit key public / private RSA key pair is generated for each user. This is done locally within the user's PasswordBox client upon registration.
2. The user who is the recipient of the shared data will also have their own RSA key. The public key component is exchanged after a user accepts invitation from a friend.
3. A fresh, random AES-256 Shared Encryption Key is generated for each pair of friends.
4. The Shared Encryption Key is encrypted with the recipient's RSA public key.
5. The RSA 2048-bit wrapped Shared Encryption Key, and the symmetrically encrypted shared password, are sent to the recipient.

Password Bequeathing

Password bequeathing enables users to share passwords with pre-selected recipients; but unlike ordinary password sharing the passwords are shared only upon the occurrence of a triggering event.

When Password bequeathing is enabled, the preparations for Password Sharing with the designated users are performed automatically — all passwords are automatically encrypted for the trusted person as they are added to a user's PasswordBox. However, the final step (sharing of the encrypted passwords and the encrypted key) is not performed unless PasswordBox receives a verified notification that the trigger event has occurred.

Extra Security Features

PasswordBox takes security seriously and empowers the user to enhance the security of their account when that is deemed necessary. PasswordBox already has a multitude of features to allow the user to increase their security level, as well as new features like fingerprint authentication that are launching soon.

Benefits of the PasswordBox Architecture

The rapid growth of cloud-based services, coupled with the discovery of significant security weaknesses that can put user data at risk, has demanded heightened awareness and the use of high-level security measures and encryption protocols. Companies that offer cloud-based services have numerous options to choose from when deciding how they will encrypt and protect user data. These options vary in the level of security provided and this choice can have a significant impact on the data security provided to users.

We have carefully designed every aspect of PasswordBox to maximize the security of our users. In this section, we'll highlight some of the benefits of this approach, by comparison to an alternative architecture that is used by many cloud-based services. We'll call this the "Minimal Security Architecture".

The Minimal Security Architecture

A cloud-based service provider may choose to protect user's data with server-based encryption. This requires the use of a provider encryption key, under the service provider's control, to encrypt all user data. This is a straightforward choice from an implementation standpoint, as a single private secret allows the rapid deduplication of data.

This can be valuable if the volume of user data is extremely high. However, in terms of data security, this single private key scenario represents a significant risk for users if the key is compromised either through a hacker attack or the actions of a rogue employee.

In this situation, the most likely attack scenarios are:

1. A rogue employee or external hacker breaks into the Service Provider

2. Unauthorized access allows password hashes or the provider encryption key to be stolen
3. Large-scale password cracking occurs, using hardware assists and specialized software such as oclhashcat-plus, or using time trade-off attacks (rainbow tables)
4. Client accounts are compromised in large numbers

PasswordBox Security Architecture

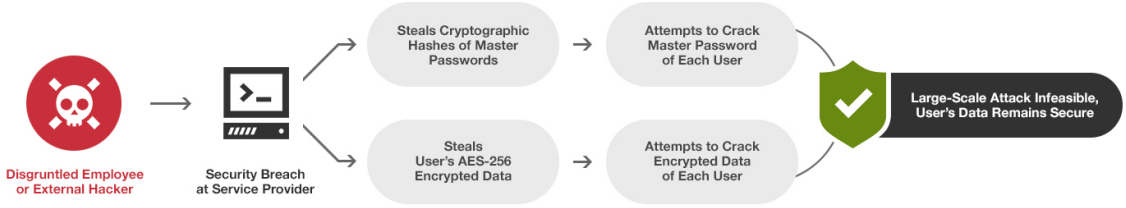
PasswordBox is a client-side encryption solution, meaning that all data is encrypted on the user's computer before being transferred to PasswordBox. Both the data encryption key and the authentication hash are derived on the user's computer from the user's Master Password. The Master Password never leaves the user's computer.

This architecture is much more resilient to attack.

The most likely attack scenarios would occur as follows:

1. A rogue employee or external hacker gains access to PasswordBox servers
2. The attacker either:
    1. steals authentication hash and tries to guess the Master Password; or
    2. takes the user's AES 256-bit encrypted data and tries to retrieve the user's passwords.

Even in the unlikely event that this scenario were to occur, the attacker would face the laborious, resource-consuming task of a brute force attack attempt on each user's AES user data files separately. And as PasswordBox employs the PBKDF2 algorithm, with more than 10,000 iterations, the encryption keys used to protect users' data have high complexity.



Even using a high-output machine, the time it would take to break a well-chosen Master Password used to protect PasswordBox user data is beyond most hackers' capabilities.

The use of PBKDF2, and the emphasis by PasswordBox on assisting users in employing strong passwords (such as using a combination of 4 Diceware words), results in a scenario in which an attack would be impractical at best.

Even with the best security architecture, security can never be perfect. While PasswordBox has chosen extremely stringent security protocols, other user-generated risks remain a factor. If a user's computer is compromised — such as through theft, or through the introduction of key-logging software or other malware — then no password-based security method can guarantee the prevention of data theft or piracy. As a result, the user always retains the final responsibility for protecting their devices against unauthorized access. But barring this risk, a PasswordBox user is still significantly more secure than someone who is storing sensitive login data in files on their desktop, or using the password-saving feature found on most browsers, or using cloud-based password services with inferior architectures.

Operational Security

PasswordBox was designed and built with high security standards. This includes not only our software, but PasswordBox's technology infrastructure and operational model.

Corporate Security Policy

The PasswordBox Security Policy clearly defines roles and responsibilities, management's engagement towards security, the corporate security requirements with which every employee must comply, and technical standards for secure software development, server and network hardening, etc.

PCI Compliant Data Center

Although PCI compliance is a regulatory requirement that is mainly imposed on merchants who store, process or transmit credit card data, our data center complies with the Payment Card Industry Data Security Standard (PCI-DSS) in order to ensure that strict security controls are applied and users' privacy is ensured. The

same level of controls that are typically employed to protecting financial and credit card data are enforced to safeguard user data confidentiality.

Server Hosting

All PasswordBox servers are located in a highly secure datacenter facility with 24/7 security guard presence and biometric security for entry. This data center has received the following Certifications and Third-Party Attestations:

- Validated as a Level 1 Service Provider under PCI-DSS
- Certified against the Common Security Framework (CSF) from the Health Information Trust Alliance (HITRUST) and has been certified for HIPAA compliance
- SSAE 16 SOC 1 Type 2, SOC 2 Type 2, SOC 3 and ISAE 3402 reports, demonstrating the viability of the security control program over time.
- Received a certificate of approval for our control program against the ISO/IEC 27001:2005 standard for Information Security Management Systems.

This secure facility also provides the following logical security services:

- IP Reputation Management
- Log Monitoring and Management
- Intrusion Detection System
- Vulnerability Management
- Application and Database Server Isolation
- Web Application Firewall
- Best of breed next-gen Firewall with egress and ingress filtering
- DDOS/DOS protection

Third Party Security Testing

PasswordBox conducts quarterly security audits, including penetration testing performed by a world-renowned penetration tester. We also perform software code reviews before every major release and have personnel continuously monitoring for potential threats and vulnerabilities.

Network Architecture — Application and Database Server Isolation

PasswordBox operates a 3-tier network with strictly demarcated security zones, exposing on the Internet only the necessary services, and properly segregating the Application Servers and Database Servers.

Secure Admin Access

Role-Based Access Control is enforced on all PasswordBox systems. By default, no access is granted to any employee. Privileges are granted solely according to operational need and at the least level of privilege necessary to perform the duty. All access to our infrastructure requires VPN access with two-factor authentication to enhance security and ensure accountability for all administrative activities.

Log Management and Monitoring

A log management and monitoring solution is in place to detect and prevent unauthorized access to PasswordBox systems. All logs are centralized to safeguard their integrity and allow correlation of events for enhanced monitoring.

Server Hardening

The web servers, the databases and the operating systems are all hardened according to NIST and CIS (Center for Internet Security) best practices.

Change Management Process

A formal Change Management Process is enforced in order to minimize the risk of corruption of the production environment. The process ensures that all changes are approved and tested prior to being deployed in production.

Patch Management

All servers and applications are kept up to date with the latest tested patches in the production environment. Prior to deployment, all patches are tested in pre-production and development environments to ensure continuous availability of the production environment.

Web Application Firewall

All Web traffic is inspected to detect and block attacks such as XSS (Cross-site Scripting) and SQL Injection.

DDOS Protection

Layer 3, 4 and 7 DOS protection is in place to safeguard resources and bandwidth for legitimate customer traffic.

IP Reputation Management

An IP reputation management system is in place to quickly compare source IP addresses to known and dangerous reputation lists in order to instantly deny access to known attackers.

Making Complex Security Processes Seem Simple

Throughout the design and development process, the PasswordBox team has shared the mission to deliver a product that offers a simple, intuitive user experience while at the same time providing users with an extremely comprehensive and effective data security solution. Security is becoming increasingly important for users of cloud services, but users are rightly unwilling to significantly sacrifice convenience and ease of use for increased security. At PasswordBox, it is our mission to deliver a product that enables users to benefit from both convenience and high security.

PasswordBox performs many complex security functions in the background, as described throughout this White Paper; but by design the user need not be aware of these processes. For most users, PasswordBox is a simple, easy, and effective way to securely store and share their passwords. More technically sophisticated users can more fully appreciate the lengths to which PasswordBox goes to protect their confidential data; but both groups benefit fully from the high levels of security and convenience that PasswordBox delivers.