Security White Paper April 2018

Contents

Introduction

KeyKong is a password manager made for humans. Simple, private and safe. We wrote this document to give you a clear sight of what we do to protect everything you store on KeyKong, knowing all the details may let you free to enjoy it without any doubt.

[NOTICE]
From now on this document will proceed with technical detailed language that may not be comfortable for all readers.

Overview

KeyKong gets you covered with the following features:

Encrypted Data

All your data is stored under a real secure encryption system using strong keys, this means that your real data is never stored anywhere, every encryption or decryption happens exclusively on your own device.

Zero-Knowledge

Since the encryption and decryption happen exclusively on your device, we never actually receive your real information, only an encryption of it. This means no one inside KeyKong or even our servers has access to your data.

Secure Transport

Data is always encrypted in travels between devices and servers by Transport Layer Security (TLS). Your data never travels without being encrypted first.

Cryptosystem

KeyKong's application, servers, and architecture thoroughly follow the main design principle: no access to user raw data (passwords, notes, usernames).

Every storing, transporting, encoding or logging operation made by our application servers won't have any access to unencrypted information.

The Key Password

When creating a new account, users are prompted asked to create a Key Password (This password can be changed later in the app).
The Key Password is only accepted as secure when it passes the minimal strength established, this is very important to have a real security cryptographic key.

All the strength requisites are automatically asked while the Key Password is being created. The Key Password must be memorized or registered in a secure location, like a physical safe combination. If lost, there is no way to recover it.

For your security, the Key Password is never stored on our servers, your device or sent over the internet.

The Key Password is derived to generate the main encryption key, which will be used in the encrypt/decrypt processes. The derivation from the user's Key Password uses thousands of iterations of a derivation function PBKDF2 with SHA512 and a user’s unique salt value.

How We Authenticate

The Authentication Token is required for a user to access his/her account. This token is based on the Key Password and the process of authentication starts with its derivation, then this Token is sent over TLS to our servers.

On the server side, it is hashed and compared to a previously stored value, if there is a match, the authentication will be succeeded.

How we Secure Data on Client

All encrypted data stored on servers are synced when the user enters KeyKong, then the app decrypts it using the following process:

- KeyKong app requests user's data to the server, encrypted with AES-256 in CBC mode;
- The main Encryption Key is derived from the user's Key Password, using PBKDF2 with SHA512 and a user's unique salt value;
- The main Encryption Key is used to decrypt the Collection Password (which is a secure random 128 bits key) for each collection;
- The Collection Encryption Key is derived from the user's Collection Password, using PBKDF2 with SHA512 and a user's unique salt value;
- KeyKong will use the Collection Encryption Key to decrypt the user's encrypted data using AES-256 in CBC mode.

Every time you create, update, or remove any item, KeyKong will use the same process to re-encrypt data on your device. KeyKong will always sync data to our servers so we can ensure backup strategies and let data available for your other devices.

Principle

We implement the security design principle of least privilege and separation of duties in our software architecture. We also use tools to analyze violations of this principle.

Cryptographic Primitives

KeyKong uses primitive cryptographic algorithms in our protocols to provide the best available security:

Our servers only store encrypted data, so in a hypothetical situation event where the server's data was stolen, a possible decryption process would take too much computing resources to brute-force keys and this process would take several years to make any sense. It's just not worth the thief's time.

Communications Security

Every request made by KeyKong app to its servers is encrypted by SSL/TLS connections. To ensure we use the best practices for TLS, we take the following measures:

- Select the best Cipher Suites;
- Eliminate Mixed Content;
- Secure Cookies;
- Use a reliable CA;
- Exclusive TLS communication;
- HTTP Strict Transport Security (HSTS).

KeyKong servers are kept up to date with constant security testing. We also implement a series of server-side mitigations to detect TLS attacks.

How We Build Our Software

Least-privilege

- AES-256 in CBC mode;
- PBKDF2 with SHA512 ;
- bcrypt KDF.

Third Party Validation

Every module or library used in our application is submitted to automated module validation and internal team review.

Disclaimers

- No payment information is stored on our servers;
- None of your raw data will be stored on our servers;
- KeyKong won't store or save your Key Password anywhere;
- Software changes or updates won't interfere with your data.