Gpass Security Whitepaper

November 29, 2016

INTRODUCTION

Gpass is from SplashData, a company that has a well-established track record of delivering password management and security solutions to millions of individual and business customers since 2000. Our infrastructure and security team includes people who've played lead roles in designing, building, and operating highly secure cloud based systems. Our long experience has taught us that maintaining security is an ongoing process. So we work closely with the best partners we can find -- like Amazon for hosting and Stripe for payments -- that focus exclusively on maintaining leadership in their particular areas of security expertise. Most importantly, we respect your privacy and the security of your records. Everything we do at Gpass is built around that respect and designed to maintain your privacy and security. We would never do anything with your data that we wouldn't be proud to tell the world about.

Millions of users trust SplashData and its security product SplashID to easily and reliably store, sync, and share sensitive information across devices. Gpass brings that same simplicity a google user, with advanced features. But although designed as an easy-to-use tool for password management, Gpass is also designed to keep important information secure. To do this, we've created a sophisticated base infrastructure. In this paper, we'll detail this infrastructure and our back end policies -- as well as the options available to user -- that make Gpass such a great solution for getting things done productively and securely.

As you continue to learn more about Gpass, we recommend you also review our Terms and Privacy Policy.

PRODUCT FEATURES

With Gpass, all your passwords and other sensitive information is organized and easy to find. Here are some key features (and this list is always growing):

- My Safe – store your personal records
- Favorites – access your favorite records
- Records – store your information into records
- Import & Export
- Mobile and desktop client apps
- Browser extensions
- Backups

AUTHENTICATION

First step with Gpass is creating an account. Creating an account is free. You can sign up yourself using your Google account.

SECURITY ARCHITECTURE

Despite our easy-to-use interface and apps, Gpass is backed by a robust architecture to ensure fast, reliable, and secure operation. We're continually evolving our product and architecture to speed data transfer, improve reliability, and adjust to changes in our users' environments.

In this section, we'll explain how data is transferred, stored, and processed securely. Gpass is designed with multiple layers of encryption, network configuration, and application-level controls that are all distributed across a scalable, secure infrastructure. Gpass users can access records and folders at any time from the desktop, web, and mobile clients. All of these clients connect to secure servers to provide access to records, allow sharing with others, and update linked devices when records are added, changed, or deleted.

Security design

Gpass uses security mechanisms that go beyond traditional encryption to protect user data. Gpass's security architecture is based on secrets known only to our users. We use AES 256-bit encryption and employ the user's Google token as the key to the encryption mechanism. This token is never stored on Gpass servers and must be provided by the user via a valid google session to decrypt the records.

Encryption library

Gpass makes use of the php mcrypt library. We believe in the power of open source and trust its proven model over time and by different vendors. Gpass uses the Rijndael cipher with CBC mode encryption. It has proven to be a reliable model, and we have used it successfully on other products with widespread user bases.

System architecture

The Gpass system architecture was designed with a modular approach. The Authentication Module has its own database for authentication only. It is completely independent from Encryption and the only requirement for Encryption is providing a valid google session specific for each user.

Our flexible design also allows the Encryption Module to be updated or even replaced depending on requirements. The API Service combines the Authentication and Encryption Module (but also other elements such as Account Management and Logging) and offers their functionality as a set of API calls that can be used by different clients such as the Gpass web client and native apps.

APPLICATION AND DATA SECURITY

The Gpass service can be utilized and accessed through a number of application interfaces. Each has security settings and features that process and protect user data while ensuring ease of access. Security of the client applications that access Gpass data is of equal importance to us as the security of the core application. Meanwhile, Gpass sync mechanisms ensure fast, responsive anywhere access to data across devices.

- Gpass web application - allows users access to their records through any modern web browser.
- Gpass Windows and Mac applications - The Gpass desktop application is a powerful sync client that gives users full access to their Gpass records. Offline access on desktop apps is in development.
- Gpass mobile applications - The Gpass app is available for iOS and Android, allowing users to access all their records on the go. The mobile app also supports favoriting of records. Offline access on mobile apps is coming soon.
- Gpass Chrome browser extension - allows users to view Gpass records directly on the extension's interface. Users can also auto-fill and auto-login to websites.

Data in transit

To protect data in transit between Gpass apps and our servers, Gpass uses Secure Sockets Layer (SSL) / Transport Layer Security (TLS) for data transfer, creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. File data in transit between a Gpass client (desktop, mobile, API, or web) and servers is always encrypted via SSL/TLS. For end points we control (desktop and mobile) and browsers, we use strong ciphers and support perfect forward secrecy and certificate pinning.

Additionally, on the web all authentication cookies are secure and enable HTTP Strict Transport Security (HSTS) with include subdomains enabled. To prevent man-in-the-middle attacks, authentication of Gpass front-end servers is performed through public certificates held by the client. An encrypted connection is negotiated before the sync of any records and ensures secure delivery of data to Gpass apps.

Data at rest

Gpass records at rest are encrypted using 256-bit Advanced Encryption Standard (AES). Records are stored in multiple data centers in discrete blocks. Each block is fragmented and encrypted using a strong cipher. User data is encrypted using the user's google token. User's data is encrypted using the token. Neither the user's token or any other key is stored on our servers.

Certificate pinning

Gpass does certificate pinning in modern browsers that support the HTTP Public Key Pinning specification, and on our desktop and mobile clients in most scenarios and implementations. Certificate pinning is an extra check to make sure that the service you’re connecting to is really who they say they are and not an imposter.

Framework security

The framework chosen to develop our system is Laravel. It is a modern PHP framework built with security in mind.

Laravel uses Eloquent as its ORM to access databases. This minimizes the risk of SQL injection. It also provides a templating engine to protect against XSS attacks, and CSRF protection is automatically enabled for all forms.

RELIABILITY & INCIDENT RESPONSE

Reliability

A security system is only as good as it is reliable, and so we've developed Gpass with multiple layers of redundancy to guard against data loss and ensure availability. Daily backups are performed on all data. Gpass uses Rackspace systems that are designed to provide 99.99% durability. This feature, beyond protecting user data, ensures high availability of the Gpass service. In the event of a failed connection to the Gpass service, a client will gracefully resume operation when a connection is re-established. Records will only be updated on the local client if they have synchronized completely and successfully validated with the Gpass service. Load balancing across multiple servers ensures redundancy and a consistent synchronization experience for the end user.

Incident response

We have incident response policies and procedures to address service availability, integrity, security, privacy, and confidentiality, including:

- Prompt response to alerts of any unusual activity
- Determination of the severity of the incident
- If necessary, execution of mitigation and containment measures
- Communication with internal and external stakeholders, including notification to customers
- Gathering and preservation of evidence for investigative efforts
- Documentation and analysis to develop triage plan and long term remediation plan

Business continuity

We maintain a business continuity plan (BCP) to address how to resume or continue providing services to users — as well as how to function as a company — if business-critical processes and activities are disrupted. Our BCP identifies internal and external threats and specifies how people, processes, and infrastructure will be mobilized to prevent and recover from disruptions.

Disaster recovery

To address information security requirements during a major crisis or disaster impacting Gpass business operations, we maintain a disaster recovery plan. The Gpass Infrastructure team reviews this plan annually and tests selected elements at least annually. Relevant findings are documented and tracked until resolution. Our Disaster Recovery Plan (DRP) addresses both durability and availability disasters. A durability disaster is complete or permanent loss of primary metadata data centers, or lost ability to communicate or serve data from metadata data centers. An availability disaster is defined as an outage greater than 10 days, or lost ability to communicate or serve data from storage service/data centers. We define a Recovery Time Objective (RTO), which is the duration of time and a service level in which business process or service must be restored after a disaster, and a Recovery Point Objective (RPO), which is the maximum tolerable period in which data might be lost from a service disruption. We also measure the Recovery Time Actual (RTA) during Disaster Recovery testing, performed at least annually. Gpass incident response, business continuity, and disaster recovery plans are subject to being tested at planned intervals and upon significant organizational or environmental changes.

Data centers

Gpass corporate and production systems are housed at Amazon (AWS EB). Amazon is responsible for the physical, environmental, and operational security controls at the boundaries of Gpass infrastructure. Gpass is responsible for the logical, network, and application security of our infrastructure. Connections are protected through an IDS and Cisco firewall, which are configured to offer offer highest level of security and monitoring. Gpass severely restricts access to the environment to carefully screened individual IP addresses and employees.

SUMMARY AND FURTHER INFORMATION

Gpass offers an easy-to-use password management tool to help google users while providing the security measures they require. With a multi-layered approach that combines a robust back-end infrastructure with a customizable set of policies, we provide businesses a powerful solution that can be tailored to their unique needs. To learn more about Gpass, visit our website or get in touch with us at help@gpass.io

Website - https://gpass.io