CryptPad Whitepaper

The Insecurity Incentive

Cybersecurity is a critical and growing need for enterprises of all size. While the global cybersecurity market is expected to grow from USD 137.85 Billion in 2017 to USD 231.94 Billion by 2022 [1], the annual occurrence of reported data breaches is also on the rise, having grown from 419 in 2011 to 1,093 in 2016 [2]. Clearly either enterprises are not doing enough or what they *are* doing is not working.

IT providers must compete on features and cost so security suffers.

At CryptPad, we believe that the fundamental problem with cybersecurity is caused by an adverse economic incentive. Namely, IT software providers are incentivized to provide the most measurable value at the lowest cost. Any effort which expended for any other objective degrades the competitiveness of the software provider. Therefore, we believe it is safe to assume that commercial software will always be less secure than its users are lead to believe.

The Need-to-Know Solution

CryptPad compartmentalizes sensitive information.

Need-to-know security is a proven industry standard for mitigating risk of employee data theft. CryptPad is the only office productivity tool to provide collaborative editing with *need-to-know security* for mitigating the risk of leaked data from breaches of IT infrastructure.

CryptPad escapes the insecurity incentive because it does not attempt to directly make IT infrastructure more secure. Instead, CryptPad builds *defense in depth* by **compartmentalizing sensitive data with cryptography**, this way it is able to multiply the effect of your existing information-security protocol.

Unlike many data encryption solutions, CryptPad's cryptographic layer is bound to its discretionary access control such that **the keys to decrypt an asset are available only to the people with the right to access it**. There is no unencrypted central server or database which can be hacked or leaked.

XWiki SAS, Société par Actions Simplifiée au Capital de 37560 Euros
35/37 RUE BEAUBOURG 75003 PARIS FRANCE, RCS Paris B 477 865 281
Tel: +33 1 45 42 40 90

CryptPad runs in any modern web browser, using **100% client-side encryption**. Sensitive material typed in a CryptPad document is **never sent to the CryptPad server unencrypted**. CryptPad uses **256 bit security** with a variety of well tested modern cryptographic algorithms:

- TweetNACL.js
- **Salsa20/Poly1305** - Pad content is authenticated and encrypted to protect against people without a link.
- **Ed25519** - Encrypted pad content is signed so that people with a *read only* link cannot make changes.
- **Ed25519** - Authenticated communications with the server.
- **Curve25519** - Contact requests to create encrypted chat sessions.
- ScryptAsync.js
- **Scrypt** - Deriving a strong encryption key from username and password.

Simplicity and Ease of Use

Using CryptPad is just like using any other web application. When a user logs in, the encryption keys are derived from the user name and password using the scrypt key derivation function and then stored in the web browser's *localStorage*.

Giving access to a CryptPad document is as easy as sharing the link. You can also create a link which provides *read only* access to a pad, allowing you to publicize your collaborative work while still being able to edit it.

Whenever you access a pad, it is automatically added to your CryptDrive. Later on you can organize it in folders with **intuitive drag and drop**. When you're done with a pad, you can just drag it into the trash bin.

Productivity With CryptPad

CryptPad can help you become more productive in your projects by enabling fast and efficient collaboration, consider the following scenarios:

- Meeting minutes
    1. Appoint a scribe to document decisions made in your meeting.
    2. With collaborative editing every participant can see the minutes as they're written, you're assured that there is agreement on the wording.
    3. When you're done, you can share a *Read-only Link* amongst interested parties or publish the content.

- Collaborative document authoring
    1. Make a rough draft of the document in a pad.
    2. Share with stakeholders who can make changes, raise issues and discuss on the content.
    3. When the content is finalized, send the pad to a secretary who can format it into an official document.

- Fast feedback collection
    1. Have an impromptu meeting with a customer or stakeholder? Open a pad.
    2. Write down whatever information they share which might be actionable.
    3. Find your pad later and organize items for investigation and action.

- Have a special use case ?
    - CryptPad is organized into *apps*, we can help you create an app for pads specific to your line of business.
    - Any editor which runs fully on the client side is a candidate for packaging as a CryptPad app.
    - **Whatever app you use, it's the same cryptography under the hood.**

References:

1. http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html
2. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

Credits:

- https://pixabay.com/en/garlic-garlic-cloves-vegetables-1914116/
- https://commons.wikimedia.org/wiki/File:Jenga_distorted.jpg