CryptPad; end-to-end encrypted collaborative office suite

David Benqué
Project Lead

Presented by: RESEARCH @ ECLIPSE & OW2
Yes, you can have both

Collaboration

Privacy

CryptPad
Lorem Ipsum


Dolor Sit Amet


Donec at neque laoreet

Efficitur magna sed, ullamcorper metus. Proin vitae efficitur odio. Aliquam aliquam ullamcorper nibh sit amet interdum. Praesent dapibus, eros ac volutpat consectetur, quam turpis venenatis ante, quis volutpat lacus mi a urna. Quisque eu arcu at mauris condimentum cursus.

Quisque porta
# Markdown

The book in your hands is about the behavior and culture of "computer hackers". It collects a series of essays originally meant for programmers and technical managers. The obvious (and entirely fair) question for you, the potential reader, to ask is: "Why should I care?"

- lists
- of
- stuff
- and
- more-stuff—

The essays in this book did not invent such a fundamental advance, but they do describe one: open-source software. **the process of systematically harnessing open development and decentralized peer review to lower costs and improve software quality**. Open-source software is not a new idea (its traditions go back to the beginnings of the Internet thirty years ago) but only recently have technical and market forces converged to draw it out of a niche role. Today the open-source movement is bidding strongly to define the computing infrastructure of the next century. For anyone who relies on computers, that makes it an important thing to understand.

I just referred to "the open-source movement". That hints at other and perhaps more ultimately interesting reasons for the reader to care. The idea of open-source has been
# CryptPad

- open source
- encrypted in your browser
- the server cannot read anything

You can write your slides in markdown

This is a dodo
Which topping is the best?

- Mushroom
- Cheese
- Ham
- Pineapple

Please explain why

Character limit: 0/1000
Hello!
<table>
<thead>
<tr>
<th></th>
<th>sepal length</th>
<th>sepal width</th>
<th>petal length</th>
<th>petal width</th>
<th>species</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5.1</td>
<td>3.5</td>
<td>1.4</td>
<td>0.2</td>
<td>setosa</td>
</tr>
<tr>
<td>2</td>
<td>4.9</td>
<td>3</td>
<td>1.4</td>
<td>0.2</td>
<td>setosa</td>
</tr>
<tr>
<td>3</td>
<td>4.7</td>
<td>3.2</td>
<td>1.3</td>
<td>0.2</td>
<td>setosa</td>
</tr>
<tr>
<td>4</td>
<td>4.6</td>
<td>3.1</td>
<td>1.5</td>
<td>0.2</td>
<td>setosa</td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>3.2</td>
<td>4.7</td>
<td>1.4</td>
<td>versicolor</td>
</tr>
<tr>
<td>6</td>
<td>6.4</td>
<td>3.2</td>
<td>4.5</td>
<td>1.5</td>
<td>versicolor</td>
</tr>
<tr>
<td>7</td>
<td>6.9</td>
<td>3.1</td>
<td>4.9</td>
<td>1.5</td>
<td>versicolor</td>
</tr>
<tr>
<td>8</td>
<td>5.5</td>
<td>2.3</td>
<td>4</td>
<td>1.3</td>
<td>versicolor</td>
</tr>
<tr>
<td>9</td>
<td>6.5</td>
<td>2.8</td>
<td>4.6</td>
<td>1.5</td>
<td>versicolor</td>
</tr>
<tr>
<td>10</td>
<td>5.7</td>
<td>2.8</td>
<td>4.5</td>
<td>1.3</td>
<td>versicolor</td>
</tr>
<tr>
<td>11</td>
<td>6.3</td>
<td>3.3</td>
<td>4.7</td>
<td>1.6</td>
<td>versicolor</td>
</tr>
<tr>
<td>12</td>
<td>4.9</td>
<td>2.4</td>
<td>3.3</td>
<td>1</td>
<td>versicolor</td>
</tr>
<tr>
<td>13</td>
<td>6.6</td>
<td>2.9</td>
<td>4.6</td>
<td>1.3</td>
<td>versicolor</td>
</tr>
<tr>
<td>14</td>
<td>6.3</td>
<td>2.8</td>
<td>5.6</td>
<td>1.8</td>
<td>virginica</td>
</tr>
<tr>
<td>15</td>
<td>7.6</td>
<td>3</td>
<td>6.6</td>
<td>2.1</td>
<td>virginica</td>
</tr>
<tr>
<td>16</td>
<td>4.9</td>
<td>2.5</td>
<td>4.5</td>
<td>1.7</td>
<td>virginica</td>
</tr>
<tr>
<td>17</td>
<td>7.3</td>
<td>2.9</td>
<td>6.3</td>
<td>1.8</td>
<td>virginica</td>
</tr>
<tr>
<td>18</td>
<td>6.7</td>
<td>2.5</td>
<td>5.8</td>
<td>1.8</td>
<td>virginica</td>
</tr>
<tr>
<td>19</td>
<td>7.2</td>
<td>3.6</td>
<td>6.1</td>
<td>2.5</td>
<td>virginica</td>
</tr>
<tr>
<td>20</td>
<td>6.5</td>
<td>3.2</td>
<td>5.1</td>
<td>2</td>
<td>virginica</td>
</tr>
</tbody>
</table>
Lorem ipsum dolor sit amet


Suspendisse aliquet metus risus


Nam maximus sed erat at finibus.
CryptPad
Collaboration suite
end-to-end encrypted and open-source
A) What normally happens

1) Send

SERVER

2) Convert

3) Receive

BROWSER

.docx  .odt

INTEROFFICE
B) With INTEROFFICE

1) Receive converter

2) Convert

.docx  .odt
CryptPad Blueprints

Figure 3: Key derivation for CryptPad.

CryptPad: End-to-End Encrypted Collaboration Suite
CryptPad Team @ XWiki SAS
Version: 1.0.0 (Changelog in Appendix A)

Abstract. Collaborative document editing has grown popularity over the last decades. This has been driven by the ease of use of online platforms compared to workflows requiring participants to mail versions back and forth and reconcile changes. However, common tools such as Google Docs or Microsoft’s Office 365 come with an impact to their users privacy. The server hosting these services can access all stored documents and actively modify or passively read their content.

In this paper, we present the cryptographic design of CryptPad, a web-based, end-to-end encrypted, collaborative real-time editor for a variety of document types. We show how we use cryptography to protect against attacks in an honest-but-curious threat model. We present multiple dedicated schemes that use a mix of asymmetric and symmetric encryption, as well as signing, to allow fine-grained access control, private messaging, and signatures. Despite the common perception of documents or user data.

Since CryptPad’s initial release in 2014, the feature set has grown from a simple editor to a full-blown set of multiple applications including forms, spreadsheets, presentation slides, kamban boards, and whiteboards. Nowadays, CryptPad also features additional collaboration utilities such as calendars, teams and simple chats.

CryptPad is an open source project with both client and server code available and licensed under the GNU Affero General Public License version 3.0 (AGPL). This means that anyone with the ability to do so is free to use, host, and modify the software as long as any modifications are available to the users under the same terms. CryptPad is developed by XWiki SAS, a company based in Paris, France that has been making open source software since 2004. The development has been funded by European funding bodies such as BPI France, the NLNet Foundation, NGI Trust, and Mozilla. Source Support.

https://nlnet.nl/project/CryptPad-Blueprints/
CryptPad AUTH

- Single Sign On
- Multi-factor authentication

https://nlnet.nl/project/CryptPad-Auth/
OpenDesk

- Diagram application
- Nextcloud integration

https://nlnet.nl/project/CryptPad-Auth/
Hello Cryptpad

This is nice. Change here.. This is fun..

Another change...

Hello Cryptpad

This is nice. Change here.. This is fun..

Another change...
Cloud de Confiance

Sovereign Office Suite partnerships and subsidies

Full suite of apps

End-to-end encrypted

Real-time editing and collaboration

cryptpad.org
David Benqué
David.benque@xwiki.com
@dbenque:matrix.xwiki.com

David - Project Lead
Yann - Privacy Engineer
Wolfgang - R&D Engineer
Faye - Cryptography Engineer
Fabrice - Cryptography Engineer
Mathilde - Community & Support
Zuzanna - Developer
Diana - Junior Developer
Daria - Junior Developer

Ludovic - XWiki CEO