An introduction to Clipperz

Table of contents

Summary

Clipperz has been developing its eponymous online password manager since 2005, gaining a solid reputation among security experts.

Now we are ready to add new substantial features and turn this robust password manager into a general purpose online safe box where users can store and securely share their most precious information and documents.

Clipperz brings state-of-the-art cryptography to the average user without the hassles of cryptography based products. Clipperz looks and behaves like a regular web app, but hides a strong Javascript cryptographic engine entirely built and executed within the browser. Clipperz is the most advanced and secure **host-proof web app**, with a paranoid focus on learning nothing about its users and their data.

In order to avoid storing readable data on the server a host-proof web application encrypts and decrypts the data inside the browser. The keys for all encryption processes are derived from a passphrase that never gets sent to the server.

The new Clipperz will introduce two features that are key to expand its value as a tool for protecting privacy and ultimately freedom:

1. **Document encryption**
   Users are no longer limited to storing passwords, but they can use Clipperz to encrypt, store and retrieve any confidential and sensitive document.

2. **Secure sharing**
   Users can share passwords or documents with other Clipperz users without the need of other communication channels or trusting third parties.

These two new features will turn Clipperz into something much more powerful than a super secure storage for passwords: Clipperz will actually become an almost invisible set of tools for protecting and sharing sensitive data.

Being able to protect information is crucial in our everyday life, but even more if you happen to live in a repressive country. Clipperz is therefore designed for an hostile environment where nothing can be trusted.

To serve the most wide audience it has very limited requirements in terms of technology: any device with a decent browser and an ordinary Internet access. No installation of local software is required, not even a browser plugin. Just a plain browser.

Anonymity is an important component of the security architecture of Clipperz. In fact, linking encrypted data stored on Clipperz server to a real identity widens the range of potential risks. Attackers could gain information about the plaintext and target the cryptography defending the data and, more likely, they could enact social engineering strategies. The security perimeter will be much larger and more difficult to protect. That's why Clipperz doesn't want to know its users!

We are submitting this proposal in order to be able to complete the design and implementation of the aforementioned two new features.

What problem does Clipperz address?

There are billions of people living under a constant Miranda warning: anything they say could be used against them, in a court or even in some extrajudicial investigation and context.

A large chunk of the world population is risking their lives because of their religion, sexual orientation, political beliefs, honest intellectual interests, … These people need to protect themselves, their family and friends. Quite often this translates to protecting and sharing sensitive information.

Clipperz will provide a convenient solution to this need, a web app that is capable to:

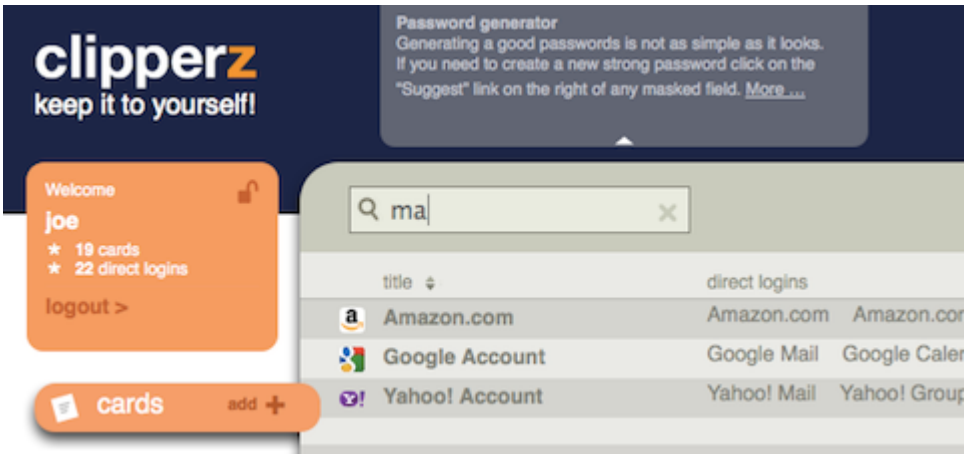
- encrypt texts and documents
- store them in encrypted form on a remote server
- share them securely with other users

Thanks to its radical **host-proof architecture**, Clipperz learn nothing about its users and their data.

Clipperz lowers the barrier to cryptography, bringing high-level encryption standards to the web. And therefore empowering users. Clipperz enables non-technical people to securely and anonymously store and sharing sensitive data without trusting a third party.

Not Google, not the government, not the ISP. Isn't that revolutionary?!

More technical details on the security architecture are available here.



How is it solved today?
And, what are the limitations?

Depending on the specific conditions and needs, there are multiple approaches to protecting, storing and sharing sensitive data. Using some kind of cryptography-based product is quite common. As Esther Dyson once said:

> *"Encryption is a powerful defensive weapon for free people. It offers a technical guarantee of privacy, regardless of who is running the government. It is hard to think of a more powerful, less dangerous tool for liberty."*

However **cryptography is hard**. Using software for encrypting data is complex and cumbersome, it requires to be installed, updated and maintained. Furthermore, if you need to securely share data, you most likely need to generate keys, manage certificates, register with a CAs, …

And hiding the use of crypto tools from authorities is even harder. This is extremely important because, under authoritarian governments, simple ownership of encryption software is enough to rise suspects or outright illegal.

A web app has a much smaller footprint and countermeasure to obfuscate its use are widely available (e.g.: TOR networks). Using cryptography through web apps is probably the best approach in many situations, if not the only options.

When people cannot rely on cryptography they often resort to in-person meeting for exchanging information using physical objects (paper, USB pen, …). This is of course more dangerous and less effective.

Some may be tempted to skip encryption and use "the cloud" for storing and sharing their data. This is a very risky approach. Cloud infrastructures are gradually shifting toward monopolies that are often unable to resist to pressures from governments, no matter how democratic or repressive they are.

Clipperz development plan

We want to build upon the code base of current Clipperz password manager and turn it into a general purpose online safe box where users can store their most precious information and **documents** in an encrypted form. And adding **sharing capabilities** at the same time.

This requires designing and implementing two new main features:

1. **Document encryption**
   Currently Clipperz organize data in "cards" that contain a small set of related information which structure can be configured by the user (Example: url-username-password). However text fields are good enough to store web credentials, credit cards data or PGP keys, but cannot answer all needs. We would like to add the ability to attach files to each card (example: passport data along with a scanned copy of the passport itself).
   Advancements in Javascript engines make dealing with average documents quite possible. Today we can run military-grade encryption routines right in the browser, and we can expect to encrypt a 10MB documents in a few seconds. Clipperz asynchronous implementation of AES is already very fast and can definitely handle average size documents. Moreover HTML5 allows the files to be encrypted locally without loading them to Clipperz server first.

2. **Secure sharing**
   Sharing is the most requested feature since the early days of Clipperz. It turns a simple encrypted storage service into a secure communication channel. It's really going to change the way people see and use Clipperz. We are going to build a whole public-key system within Clipperz, but we will mask all complexities to the user that will just need to share an authorization token with counterparts in order to open a secure sharing channel right within the web app interface.
   Groups of activists, journalist/informats, regular families living in non democratic countries, … there are plenty of situations where exchanging encrypted data and documents could be vital.
   Besides plain 1-to-1 sharing, users will also able to define more complex sharing policies (Shamir secret sharing, event triggered sharing, ...).

The new features will be implemented in a way that the "pure web nature" of Clipperz will be preserved, no additional software (browser plugins, local clients, …) or external hardware devices (tokens, dongles, …) will be required.

What challenges will you confront during this effort?

1. **Complex security architecture**
   The two new major features described above, require to expand the set of crypto primitives available in the underlying cryptographic library. Therefore there are risks in the implementation of new encryption algorithms and the overall design of the cryptographic architecture.
   In order to maintain and hopefully improve the current security levels, we will need the support of qualified specialists.

2. **Usability and user experience**
   We strongly believe that accessibility and ease of use must be treated as security properties and therefore Clipperz interface should be designed to be accessible indiscriminately to all cultures, languages and age groups. The new features should play nicely with the current responsive design that makes Clipperz convenient to use on any device, from large desktop screens to smartphones small displays.

Who will care and what will the positive effect be?

Clipperz is a tool for everyone, but people in repressive countries will benefit the most from it. While it could be convenient and wise for people living in democratic countries to protect their most important data (not just passwords), it could be lifesaver for people living under authoritarian governments.

Clipperz is much easier to use (and therefore more likely to be used) than setting up PGP or establish an OTR-encrypted connection or encrypting the whole hard disk with TrueCrypt. This convenience could lead to a broader reach and regular use.

- **Activist groups**
  Encryption doesn't solve every surveillance problem, but it could make life much easier for groups of activists that are able to integrate encryption in their daily routines, both for data at rest and data in motion between members. The ease of use of a web app like Clipperz reduce the risks of relying on less secure storage solutions and communication channels.

- **Reporters and whistleblowers**
  Clipperz make it easier to establish a secure asynchronous communication channel between two parties. A journalist could therefore use Clipperz to securely receive confidential documents from an informant without the need to use encrypted email or settiong up more complex solutions.

- **Dissidents, freethinkers, …**
  People in these categories are subject to government and social pressures. Clipperz provide them with a place where to store credentials and documents that could be dangerous to expose.

- **Families living in authoritarian countries**
  Family members can use Clipperz to store access credentials (bank accounts, safe deposit boxes, …) and important documents. This could be very important in emergency situation and when direct communications between members is not possible (e.g.: arrest by police, dispersed because of armed conflicts, natural disasters, …).

Since all accounts are completely anonymous, users could create multiple accounts on Clipperz and prepare a deceiving strategy if forced by authorities to reveal their Clipperz credentials.

Risks and limitations of Clipperz

1. **Browser crypto criticisms**
   The openly debated limitations of browser cryptography (mostly related to code delivery) are more an opportunity than a risk. Browser manufacturers are already building basic crypto functionalities directly in the browser and the W3C Working Group just released the first draft of Web Crypto API. Therefore we can expect to have soon tools to overcome these limitations.
   Clipperz built the first open source, robust and fast Javascript library of cryptographic primitives in 2005. We want to keep contributing to build the "web security stack". Brendan Eich said:

   > *"the web stack is never perfect, but it always catches up, and it has the broadest reach."* (source)

   And when we talk security the "broadest reach" is a crucial factor …

2. **Speed and size constraints**
   Encryption/decryption processes in the browser are slower than native solutions, but Javascript engines are quickly catching up. Today our AES routine can encrypt a 10MB document in under a minute, but it still can't tackle a 1GB file. But as soon as W3C Web Crypto API will be available even this constraints will be removed.

3. **Authorities**
   Online services can be shut down by authorities that could intervene at many levels (domain, DNS, ISPs, …). To counter this risk Clipperz took several different actions:

   a. it provides any user with the ability to run a personal instance of Clipperz from his own server (formerly known as Clipperz Community Edition) using the open source code;
   b. **moved out of the USA** all the technical infrastructure (app servers, web server, DNS server, …) to enjoy higher level of privacy and freedom of speech protection;
   c. registered the domain **clipperz.bit**, reachable using a decentralized DNS service based on the Namecoin blockchain.

More information about Clipperz

Other security features

Both document encryption and secure sharing will of course play nicely with the current set of features, more specifically:

- **offline copy**
  Once you start using Clipperz to protect and share sensitive data, being offline means being disconnected by your most precious bits of information. This is why we included the offline copy feature from the very first release. It means the user can dump the whole content of her account to a local hard disk or USB drive and create a read-only portable version of Clipperz to be used when no Internet connection is available. The offline copy is just a single HTML file that contains both the whole Clipperz web application and user's encrypted data. It is as secure as the hosted app since they both share the same code and security architecture. And provide the same user experience too.

- **OTP, one-time credentials**
  for secure access from insecure devices
  A one-time passphrase works like a regular Clipperz passphrase, but it can be used only once. If the same passphrase is used again at a later stage in a login attempt it will be rejected and the login process will fail. Each one-time passphrase is 32 character long and it guarantees at least 128 bits of entropy.
  OTPs are an excellent choice to prevent attacks from keyloggers and spyware. They guarantee secure access from insecure devices and public terminals, such as those found in Internet cafes and libraries.

- **password generator**
  Humans generally do poorly at generating random data, that's why Clipperz provides a cryptographically strong random password generator based on the Fortuna algorithm.

Clipperz is a single page app and can run from a local file

The whole Clipperz application is retrieved with a single page load. HTML, JavaScript, CSS, encoded images, … are all loaded into the memory of the browser before credentials are entered in the signin/signup form. Clipperz does not automatically reload during user interaction with the application, nor does control transfer to another page. This kind of web apps are usually called single page app (SPA).

There is a very good reason to design Clipperz as a single page app: if additional chunks of source code were downloaded from the server after the login phase, the user wouldn't have any chance to verify the security of a web application. Therefore in Clipperz not a single line of Javascript is moved to the browser after a successful user authentication.

Being a SPA, Clipperz may be executed from a local file using the file URI scheme. This gives users the ability to download and verify the Clipperz code once and then run the file locally without downloading a new copy every time they need to use the online service. Leran more here.

Clipperz is an open source project

Clipperz is the sponsor of 2 open source projects: the Javascript Crypto Library and of course the very Clipperz Password Manager web app. Both projects are hosted on GitHub.

There's been a lot of debate by security practitioners about the impact of open source approaches on security. Clipperz stays on the side of security expert Bruce Schneier when he says:

> *"In the cryptography world, we consider open source necessary for good security; we have for decades. Public security is always more secure than proprietary security. For us, open source isn't just a business model, it's smart engineering practice."* (source)

And along the same lines is Vincent Rijmen, co-author of the AES algorithm:

> *"Not only because more people can look at it, but, more importantly, because the model forces people to write more clear code, and to adhere to standards. This in turn facilitates security reviews."* (source)

Here is a short description of these projects:

- **Javascript Crypto Library (license: BSD)**
  The Javascript Crypto Library provides web developers with an extensive and efficient set of cross-browser cryptographic functions. The library aims to obtain maximum execution speed while preserving modularity and reusability. This is the very library that Clipperz web app is built upon. It currently includes:
  - AES-256, symmetric encryption;
  - Fortuna, a strong pseudo-random number generator;
  - SRP, a verifier-based authentication protocol;
  - SHA-2, hash function.

  New crypto primitives will be included as a byproduct of the development of the new features objects of this proposal: ECDH,

- **Clipperz Password Manager (AGPL license)**
  This project is for those interested in inspecting the code behind the Clipperz online vault or run a local instance of it.
  We want to enable as many people as possible to play with our code, so that people can start trusting it (the code, not its developers). In order to allow users not just to inspect the Clipperz code, but also analyze the traffic it generates between client and server, we had to provide an easy way to locally deploy the whole web application.
  Users can choose among multiple backends (PHP/MySQL, Python/AppEngine, …) or you contribute their own.

Please note: all the development required for the implementation of document encryption and secret sharing will contribute to these two open source projects.

Contributions are very welcome and we received quite a few along the years. In order to avoid jeopardizing the ownership of the code base, Clipperz requires every developer to sign the Clipperz Contributor Agreement. This enables a single entity, Clipperz Srl, to represent the aggregated code base.

The fraudulent wire transfers case and Iceland

Since June 2013 Clipperz has been under an uncanny attack, more precisely Giulio and I, as individuals, are the target of the attack. Neither Clipperz infrastructure nor user encrypted data stored on Clipperz have been exposed to any risk.

A long story short: someone is hacking online banking accounts of tens of Italian small companies and individuals in order to send large wire transfers to the bank account of Clipperz. What's more astonishing is that all transfers are larger than 10K€, that is above the daily limit allowed by almost any bank for automatic processing. Chances for such orders to go undetected and executed are almost nil. The only effect they are obtaining is putting a dozen district attorneys at work, each of them independently investigating Clipperz.

In the past months we spent quite a lot of time answering questions from Italian authorities. There are yet no formal charges against us, but it's not completely unlikely that a single district attorney could order the seizure of Clipperz assets as a "pre-trial precautionary measure".

Our main goal now is to protect Clipperz, its users and their data. We are not doing anything illegal, but allowing people to better protect their most precious bits of information. We are determined to fight in order to prevent anyone from destroying Clipperz just by signing a paper.

As a first measure we moved our technical infrastructure from the US to Iceland, where we can already enjoy stronger protection while waiting for the completion and approval of the Icelandic Modern Media Initiative [IMMI], a jurisdiction to provide even further protection of freedoms of expression and information.

Clipperz.is domain is registered with the nice folks at 1984.is that also manage our DNS records, while the servers running both the Octopress website and the actual password manager app are hosted on Greenqloud.

More details are available on the Clipperz blog.

Organization profile

Clipperz is a project by Marco Barulli and Giulio Cesare Solaroli. We are both based in northern Italy and have been studying and working together for 10+ years in a few startups and software related projects.

Giulio is the sole developer, taking care of all the technical issues: from host configuration, database setup, coding both backend and frontend, monitoring tools, performance tuning, etc…

Marco is involved in designing the product and the security architecture, while being in charge of the administration and business development tasks. Both are providing customers supports to users and are active members of the Clipperz forum.

Giulio Cesare Solaroli
All things software + information architect + UI and UX designer
http://it.linkedin.com/in/gcsolaroli

Marco Barulli
Product and business development + crypto apprentice
http://it.linkedin.com/in/mbarulli

Clipperz srl was established as an Italian resident limited liability company in November 2005.

Clipperz track record

During the past 7 years Clipperz never experienced a security breach, not even a security glitch. The online service has been incredibly stable with extremely limited unscheduled downtime. The service is currently used on a daily basis by about 10K users. Total registered users are more than 100K.

During the 7 years Clipperz has been receiving unsolicited donations from over 1200 unique users and supporters (averaging at of 400€/month) from 51 different countries. The detailed financial statements of Clipperz are available on the website.

Current Clipperz audience

Being an anonymous service we have very limited information about the composition and segmentation of Clipperz users. However since we've been accepting donations (via Paypal, bank wire and bitcoin) for a few years, we came to know a significant portion of our users (over 1,200 unique donors).

The first conclusion is that, as of today, most of Clipperz users are technologists of some sort: security experts, cryptographers, developers, system administrators, scientists, … Many work for renowned universities (Stanford, Harvard, Cambridge, Lousanna, IIT, Cornell, ETH Zurich, MIT, …) or top technology companies (Google, IBM, Mozilla, …).

Since we announced support for Bitcoin, Clipperz has been attracting crypto currencies activists and got a good coverage in forums and dedicated websites (e.g.: [Coindesk]).

Public speaking

Giulio and Marco are sometimes speaking at conferences.

- Marco: "Bitcoin, the taste of things to come", Shift Conference, Bologna, February 2014
- Giulio: "How to build single page applications in Javascript", JS Day, Verona, May 2013
- Giulio: "Zero-knowledge web applications", Lift Conference, Geneva, February 2008

Selected reviews

- CoinDesk, Clipperz Password Manager Only Accepts Bitcoin, December 2013
- Gizmodo, These Password Managers Keep Your Everything Safe, January 2012
- MacWorld, Clipperz helps manage passwords for free, September 2012
- TidBITS, Clipperz Does the Impossible: A Safe Online Password Manager, February 2010
- IT Innovators, Marco Barulli interviewed by Jon Udell, November 2009
- Jon Udell's blog, Talking with Marco Barulli about zero-knowledge online password management, November 2009
- Ajaxian, Clipperz and zero-knowledge online password management,November 2009
- Slashdot, Richard Stallman and Clipperz Promoting Freedom In the Cloud, July 2008
- InfoWorld, RMS & Clipperz offer freedom in the cloud, June 2008
- Wired.com, Keeping Hosted Data Secure from Its Host, April 2008
- Clarìn, Tus claves maestras, a lugar seguro, November 2007
- Mashable, Clipperz Launches Online Password Manager and Virtual Safe, July 2007
- Lifehacker, Store passwords online with Clipperz, April 2007