Project Report

2012-2013

project.crypto.cat

year in review

The Cryptocat Project's goal of bringing private, encrypted and accessible instant messaging to the masses was never perceived as easy. We were beset with new technologies and a seemingly impossible challenge. Striking a balance between security and accessibility has been one of the most difficult challenges in computer security for years before Cryptocat was conceived.

Last year was the first entire year that Cryptocat had for itself, and the year where we started making great progress. Spring and Summer saw Cryptocat presented at conferences from New York City to Rio de Janeiro. In Autumn we released Cryptocat 2, the first major revision of our software. Cryptocat was encouraged and criticized, met with skepticism and praise. For a project trying to tackle such difficult problems, this was our best case scenario.

Cryptocat is now used by thousands daily. It has found a surprisingly broad user-base, from transgender counselors to journalists. We're achieving our goal to make private communications accessible.

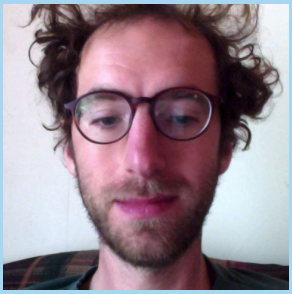
Cryptocat is being built so that anyone can chat on the Internet without being surveilled, even if they're not a computer scientist. It works in your browser, it's colorful and it has a cat. This is what we've accomplished in 2012, and what we're looking to do in 2013.

Nadim Kobeissi,
Lead Developer

team

Nadim Kobeissi
Lead Developer

Nadim released the first version of Cryptocat in May 2011 and handles most of the project's design and engineering.



Arlo Breault
Core Library Developer

Arlo develops and maintains a large portion of Cryptocat's encryption libraries.

Daniel Faucon
Core Volunteer

Daniel joined Cryptocat after discovering a vulnerability in its encryption scheme.

Elisabeth Gill
Translations Coordinator

Elisabeth coordinates between dozens of translators to keep Cryptocat accessible in more than thirty languages.

notable volunteers

Jacob Appelbaum Joseph Bonneau, Griffin Boyce, David Dahl, Arturo Filasto, Tom Lowenthal, Fabio Pietrosanti

Thanks to everyone that helped make Cryptocat better!

our research

What Is Cryptocat?

Cryptocat is an instant messaging client that offers encrypted chat within any browser. Our goal is simple: Have an instant messaging platform that anyone can access and use, regardless of technical expertise.

Cryptocat aims to leverage both the ease of use and accessibility afforded by web applications and the security provided by client-side cryptography to offer group instant messaging, encrypted file sharing, and more. Everyone deserves the right to private communications, whether they are a journalist with no advanced computing skills or a transgender activist wishing to discuss their issues in private. Cryptocat wants to make private communications accessible for everyone.

Cryptocat is open source, free software released under the GNU Affero General Public License. We rely on an open development standard, use open encryption designs and specifications and operate under constant peer review. Our software is available in 32 languages and is used by tens of thousands around the world.

Why Privacy Matters

Cryptocat is developed by privacy advocates, for privacy advocates. Big Data providers such as Google and Facebook continue to amass huge amounts of personal information without providing any guarantee of privacy, while encryption remains largely inaccessible. This means that a lot of what you do online is susceptible to governmental or corporate interception. Cryptocat aims to bridge the gap for those who need easily accessible encrypted communications.

Who Uses Cryptocat?

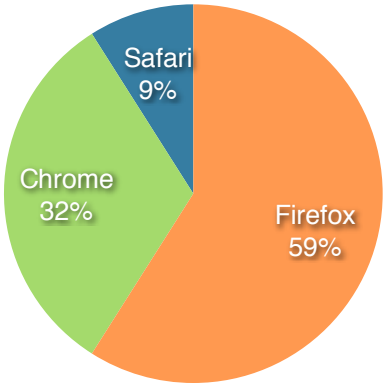
Friends and Family: Cryptocat means to be as accessible as any other web Instant Messaging platform, while also offering a transparent layer of security. This makes it an ideal alternative to invasive services for talking with friends and family.

Media, Journalists and Nonprofits: These organizations regularly require private communications, but often deal with parties that aren't ready to set up and use conventional encryption software. Cryptocat makes it easy for your nonprofit to communicate with its clients privately.

usage statistics

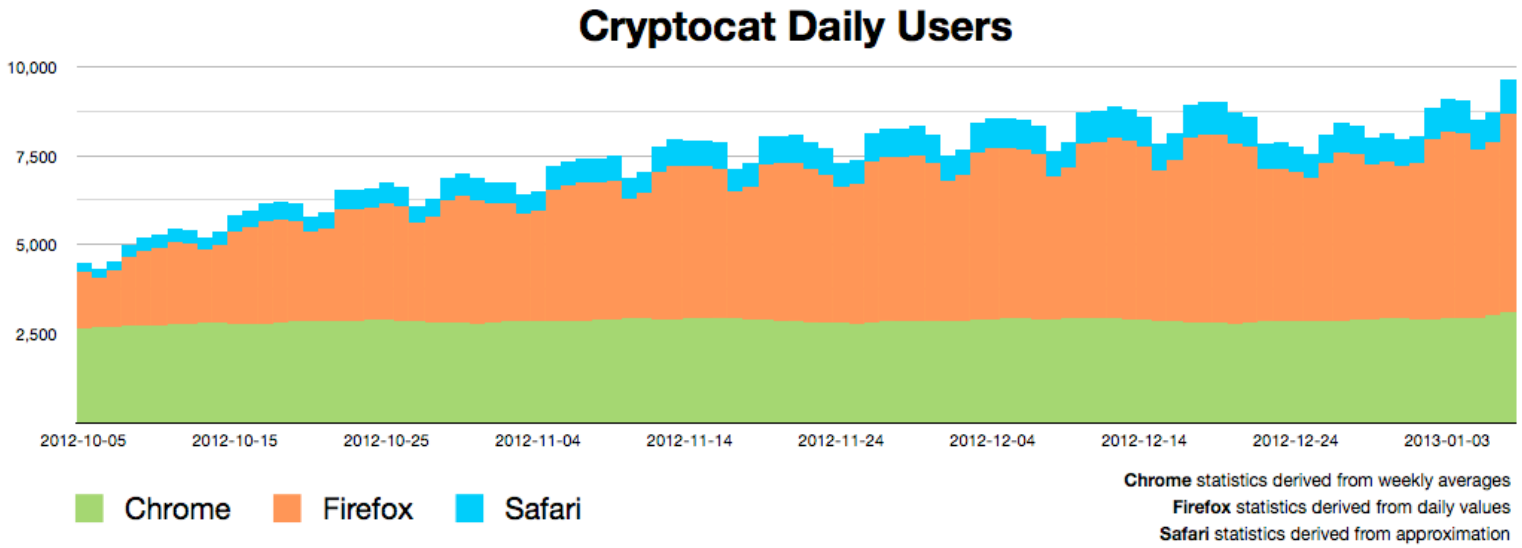
In September, we released Cryptocat 2.0, a major revision that works entirely as a browser plugin. This introduced delivery challenges, namely that Cryptocat had to be available as a special package for each browser. Surprisingly, Cryptocat adoption *increased* under the browser plugin model.

In October, Cryptocat saw nearly doubled into more than 8,000 users had been available for Chrome Cryptocat for Firefox in 2012 the Firefox client instead. As of clients are launched from within October's 20% figure.



4,000 daily users. This statistic daily in December. While Cryptocat since 2011, the introduction of resulted in most users switching to 2013, almost 60% of Cryptocat Firefox browsers, a sharp rise from

Due to our commitment for user privacy, we have not employed methods to monitor usage metrics in depth. We do however plan to develop privacy-preserving anonymous metrics in 2013, which we hope will give us further insight into how and where Cryptocat is being used without endangering user privacy.



languages

Cryptocat had its translation API completely rewritten in 2012, introducing support for full-app translation coverage and right-to-left languages. Using this new API, Cryptocat was translated into 32 languages, making our software language-accessible in a large variety of countries (delineated above.) We hope to keep our translations steadily updated as we introduce new features. Cryptocat is available in the following languages:

- English
- Arabic
- Basque
- Bengali
- Catalan
- Chinese (China)
- Chinese (Hong Kong)
- Czech
- Danish
- Dutch
- Esperanto
- Estonian
- French
- German
- Greek
- Hebrew
- Irish
- Italian
- Japanese
- Khmer
- Korean
- Latvian
- Norwegian
- Persian
- Polish
- Portuguese
- Russian
- Spanish
- Tibetan
- Turkish
- Urdu
- Vietnamese

awards and mentions

Cryptocat has received a tremendous amount of media coverage in 2012. This has been very helpful for our project due to it attracting volunteers, programmers, experts, auditors and users. While the media has sometimes exaggerated the reach of our research, we are thankful towards everyone who took the time to write about Cryptocat.

"Cryptocat has a simple, countercultural goal: people should be able to talk on the Internet without being subjected to surveillance." — **The New York Times**

"Cryptocat is deceptively simple for a web app that can save lives, subvert governments and frustrate marketers." — **Wired**

"16th Annual Webby Awards Honoree, Social Media Category." — **Webby Awards**

"Wall Street Journal Data Transparency Award for Outstanding Data Control Project." — **Wall Street Journal**

"Cryptocat works inside a web browser and enables people to chat online via encrypted instant messaging."— **BBC News**

"One of the best Google Chrome apps currently out there." — **Business Insider**

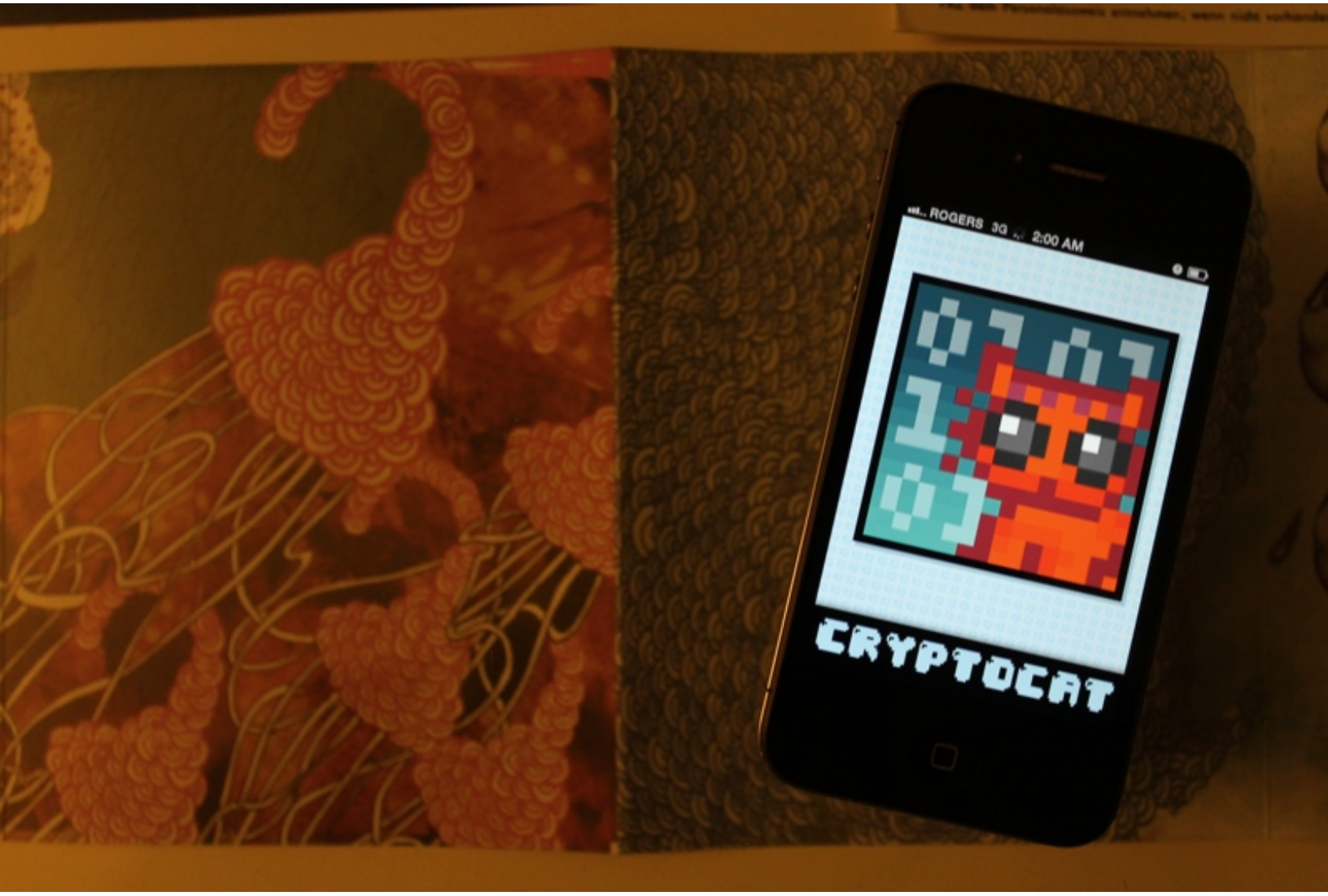
"Cryptocat brings extra-secure communication to web chat, especially in places where conversations might be watched." — **Ars Technica**

"Cryptocat may turn out to be the Web's easiest way to communicate with strong encryption." — **Forbes**

"The beauty of Cryptocat is its simplicity." — **PC World**

"Cryptocat creates an encrypted, disposable chatroom on any computer with a web browser." — **Lifehacker**

coming soon: mobile apps



Beginning May 2013, the Cryptocat Project plans to roll out mobile applications for iPhone and Android, offering free and open multi-party chat on mobile devices. These applications will connect users seamlessly with existing desktop and laptop Cryptocat users. Cryptocat Mobile will include push notifications, message delivery confirmation, and more mobile-specific features.

In addition to iPhone and Android, we are looking forward to testing Cryptocat on Mozilla's upcoming Firefox OS for mobile phones and expect a platform release in late 2013.

2013: proposed deliverables

A lot of research was done in 2012. The Cryptocat Project has accomplished software, outreach and other deliverable goals, and we're looking for doing more in 2013.
In 2012, we had deliverables including project development, mobile development, threat modeling, auditing, documentation, outreach and software development. This year, we're going in the same direction, with new goals and more experience.

We want to achieve more in terms of research, software development, documentation and outreach. We're looking for organizations to support, sponsor and fund our work. Here's what we would like to work on.

Documentation and Outreach

Translations Fund Establishment

So far, the Cryptocat Project has not had any dedicated funds for soliciting translations, translation coordination and verification. This has forced us to rely on volunteers who work in their free time. When we're ready to release new Cryptocat features, we need to make sure they are translated into 32 languages (including obscure languages such as Tibetan) before they can be released.
Relying on volunteers for translations means that we sometimes deal with unreliable results. More importantly, we deal with substantial delays to new releases. It's important that the Cryptocat Project establishes a translations fund in order to secure reliable and timely translations for future versions.

User Field Guide

The Cryptocat Project would like to publish a colorful, accessible field guide which can be used to introduce and train individuals worldwide on using Cryptocat. The field guide would rely on symbols (images, drawings, graphs) more than on language, therefore breaking possible linguistic and cultural barriers. The guide would be useful in teaching basic privacy principles to communities worldwide, including journalists and human rights workers.

Field Training Program

In addition to our field guide, the Cryptocat Project would like to establish a field training program which would allow members of the project to travel and visit organizations worldwide in order to give basic privacy, security and anonymity training involving Cryptocat as well as other software (such as Tor.) Cryptocat is already supported by an international

and multilingual team, and we believe a field training program would not only help promote online privacy worldwide, but also help us understand how to better develop our own software.

Privacy Policy

Cryptocat currently lacks a formal privacy policy regarding the circumstances under which our software is delivered and the data collected during download and usage. Formulating and publishing a legally valid privacy policy is necessary.

Research and Development

Anonymous Usage Metrics

Cryptocat has so far gathered only very basic usage statistics. This is due to our commitment to user privacy. We do, however, want to develop anonymous usage metrics that can help us learn more about how, and where, Cryptocat is used without endangering the anonymity or privacy of our users. Learning more about Cryptocat's usage will help us discover how to best improve and adapt our software and also discover potential censorship attempts with higher accuracy.

Better Authentication Using SMP

Currently, the only possible method to authenticate the identity of fellow participants inside a Cryptocat conversation has been via public key fingerprints. We would like to expand this to include SMP (the Socialist Millionaire Protocol) which allows secure authentication using an easier, more natural question/answer process. SMP is already part of the Off-the-Record protocol (which Cryptocat uses,) but our software currently lacks an interface for this feature. The interface will need to work with our 32 languages, including right-to-left languages.

Permanent Key Storage

Cryptocat currently does not store user keys on the client side, forcing users to regenerate encryption keys every time they use Cryptocat. This is not only a time-consuming process, but also results in the reset of the user's authentication fingerprints, forcing re-authentication. We would like to implement permanent key storage in a safe manner in order to make Cryptocat easier to use and authentication less painful.

Multi-Party Off-the-Record

The Cryptocat Project would like to obtain funds to hire researchers in order to improve the state of current standards used for multi-party encrypted instant messaging. We intend to build upon the existing Off-the-Record specification in order to publish the first Multi-Party Off-the-Record protocol, which may very well find uses beyond Cryptocat.

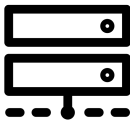
USENIX Research Paper

The Cryptocat Project would like to present its work at USENIX (USENIX Security 2013, FOCI 2013) in order to establish an academic presentation for its research and draw in more peer review and expert discussion. FOCI (*the Free and Open Communications on the Internet Workshop*) has especially been an excellent resource for the discussion and advancement of research in privacy and communications research.

Better Chrome OS Integration

Cryptocat is currently the *only application* for Chrome OS that offers encrypted instant messaging. This is an excellent opportunity to focus on better integration and catering towards Chrome OS. We would like to investigate Chrome OS features and formalize a beta testing process specific to Chrome OS.

IM Network Interoperability



We would like to investigate allowing Cryptocat to connect to other social networks (such as Google Talk) in order to allow encrypted conversations with friends and contacts on those networks. It would be important to implement this without allowing the Cryptocat network access, even theoretically, to the user's credentials on other IM networks. Such a goal is considered possible, but however will require significant redesign of the user interface and underlying code.

Firefox OS App

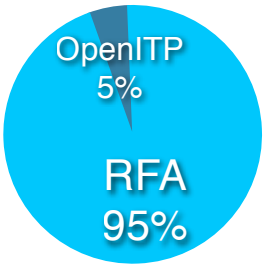
The Cryptocat Project has been closely assisted by volunteers from Mozilla which have aided in the Firefox implementation. Mozilla has also sent us a test device for their upcoming Firefox OS. We would like to implement Cryptocat to function natively on this new and promising mobile platform which targets developing economies.

User Interface Personalization

Cryptocat users have frequently demanded a more customizable user interface, including control over font size and color schemes. The rationale for this has ranged from increasing readability and usability to simply making the software more fun to use. We believe this feature to be important for both reasons of increased usability as well as making Cryptocat more appealing to users on a personal level.

2012: our sponsors

Funding Distribution



Cryptocat was sponsored in 2012 mainly by **Radio Free Asia's Open Technology Fund**, with some minor support from **OpenITP**. Funding from OTF and OpenITP has propelled a lot of the innovation and hard work we've managed to perform in 2012. The Open Technology Fund was instrumental in helping us lay the groundwork for the Cryptocat Project, including a project website, threat model, software audits, documentation and outreach. OpenITP helped with funding the implementation of cryptographic protocols. Our total funding from both parties amounted to $100,000 USD.

We are infinitely thankful for the serious and necessary support our sponsors have given us.

RFA OPEN TECHNOLOGY FUND

"Cryptocat was created through vision, devotion and most importantly, a desire to help others communicate safely. The need and potential impact of this tool has been demonstrated by its growing user base, an expanding community of volunteers/contributors and a rising number of requests for integration and collaboration. Cryptocat has been user-localized into more than 30 languages in the past 8 months alone. Cryptocat embodies a core Open Technology Fund principle: developing open and accessible technologies that support human rights and foster open societies."
— **Libby Liu, President, Radio Free Asia**

OpenITP Internet Tools Project

"The Cryptocat Project handled our funding arrangement with transparency and an obvious sense of responsibility to promise less than they delivered. We look forward to supporting their work again in the future."
— **James Vasile, Director, OpenITP**

Thank you!