Introduction

Cryptocat aims to offer private, end-to-end encrypted communications in an accessible platform for everyone. However, a quick review of the domestic policies of world nations reveals a strong correlation between repressive human rights records and tendency towards Internet censorship.

Cryptocat's potential at achieving a secure but accessible communication platform for the mainstream (including journalists and human rights activists) can therefore be endangered by Internet censorship efforts within the countries in which those individuals operate. In this report, we investigate a selection of censorship circumvention techniques which the Cryptocat Project may deploy in order to not allow repressive Internet policies to pose a threat to Cryptocat achieving its purpose: computer software promoting human rights and the freedom to connect.

While this is a detailed report, it focuses on being accessible and easy to understand for both technologists and other individuals involved in human rights initiatives.

Censorship Circumvention Technologies

In this report, four methodologies are discussed:

1. **Deployable Cryptocat Servers**: Anyone with minimal computer networking knowledge can deploy and manage a standard Cryptocat service for their community including an easy to use administrative interface and localization capabilities.
2. **Cryptocat Hidden Services**: Theoretically allow *any website on the Internet* to secretly harbor the capability to maintain Cryptocat sessions. The extreme difficulty in differentiating between regular web traffic and Cryptocat traffic makes it difficult for censors to track down these hidden nodes.
3. **Cryptocat Plug-and-Connect Open Hardware**: Cryptocat mini-servers, tiny enough to ship in a letter-sized bubble envelope. Gives organizations inside repressive regimes a ready-to-use, plug-and-play style Cryptocat service.

4. **mpOTR, a Universal Protocol**: By universalizing the Cryptocat protocol into becoming the first ever implementation of Multi-Party Off the Record, the Cryptocat technology itself becomes *transferable to any Instant Messaging client.* mpOTR makes it so that even in the case of Cryptocat being knocked completely off the Internet, the encryption technology it provides remains accessible in a sizable variety of Instant Messaging clients worldwide.
5. **Seamless Compatibility with the Tor Network**: Tor[1] provides an accessible free software solution that unifies both censorship circumvention and Internet monitoring/ wiretapping. Seamless integration with the Tor Project allows Cryptocat to tap into the potential of the most promising anti-censorship Internet anonymity project on the Internet.

Deployable Cryptocat Servers

What is it? Easy to deploy server software that can be dropped into any web server to provide both a Cryptocat client (accessible through any web browser) and Cryptocat server capabilities. The server may be connected to via its web client and also through browser apps (such as Cryptocat Chrome) or mobile apps (such as Cryptocat for Android.)

What can it fight? A wide spread of Cryptocat servers is a standard, natural method of combating the selective censorship of Cryptocat servers, and also allows for the setup of private, localized or otherwise customized Cryptocat servers for specific organizations or needs.

What interesting features does it have? At present, Cryptocat servers are even easier to deploy than leading blogging software such as Wordpress[2] and require less dependencies. In the near future, a web-accessible server administration interface will be introduced, with the possibility of keeping anonymous usage metrics (sent to the Cryptocat project) as well as automatic update notifications and more.

When will it be ready? Cryptocat server code is available with installation instructions and source code on the Cryptocat code repository at <https://github.com/kaepora/cryptocat/>.

[1] https://torproject.org

[2] http://wordpress.org

Cryptocat Hidden Services

What are they? A variant of the deployable Cryptocat servers designed to integrate seamlessly into popular websites. Cryptocat hidden services allow the websites to provide the capacity of acting as Cryptocat chat servers, while simultaneously masking Cryptocat conversation traffic as regular traffic from the eyes of Internet surveillance agents. These nodes are therefore difficult to detect, and therefore (also depending on the website in question) difficult to censor.

What can they fight? In the case a system is implemented to automatically identify and censor Cryptocat servers according to their network usage fingerprint, Cryptocat hidden services would be more difficult to detect due to their traffic's high similarity to regular connectivity to an inconspicuous website.

What interesting features will they have? Integration with Cryptocat browser apps and plugins, that enable the detection and sharing of Cryptocat hidden services between friends.

When will it be ready? We hope to have a methodology outlined for the architecture and development of Cryptocat hidden services within October 2012.

Cryptocat Plug-and-Connect Open Hardware

What are they? Tiny little computers that we can ship anywhere. As big as a deck of playing cards, their small size means they can probably get past the borders of repressive regimes. Journalists, human rights workers just plug them into their network, and the servers instantly provide a Cryptocat service accessible to everyone on the network.

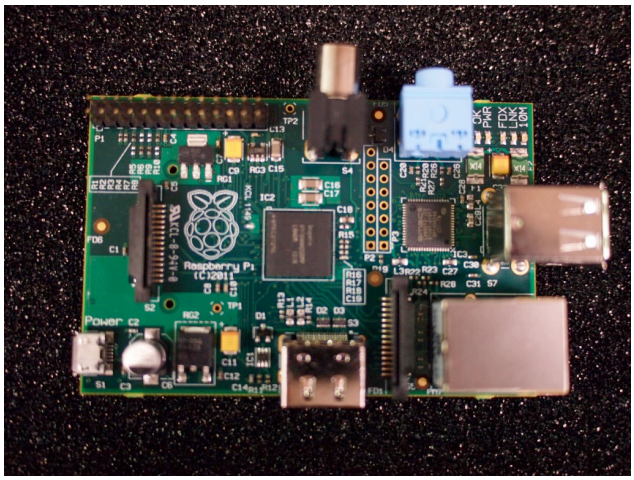
What can they fight? Even if the entire Internet is cut off from a nation-state (as Mubarak did to Egypt for a brief spell in January 2011,) small organizations will still be able to rely on an internal network of communication that is still accessible from their browsers, computers and mobile phones, that is run locally and that offers accessible end-to-end encryption. Even if the plug-and-connect server is seized by authorities, it will not contain any record of the conversations, connections or any other identifying information.

What interesting features will they have? An accessible control panel for administration and setup, the capacity to gather anonymous usage metrics, automatic update notifications, and more. Instead of using a hard drive, the servers will depend on an SD card, allowing for better storage flexibility and security. Furthermore, the establishing of a network of Cryptocat mini-servers around the world opens wealth of yet-uninvestigated possibilities.

When will they be ready? Test units will be ready in July 2012. We plan to offer units for sale for NGOs and media organizations (at a very affordable, less-than-$99 cost per unit) by September 2012.

What will they look like?

Cryptocat mini-server in case. Finished units will be branded with the Cryptocat logo, not shown here.



Cryptocat mini-servers will use the Raspberry Pi (http://raspberrypi.org) open hardware for its affordable cost, small size and impressive hardware capabilities.

mpOTR, a Universal Protocol

What is it? While the current Cryptocat encryption protocol is openly documented and available in its own specification design document[3], we plan to evolve the current protocol to be the first ever multi-party encrypted chat system to match the requirements of the Multi-Party Off the Record

[3] https://project.crypto.cat/documents/spec/spec-rev1.4a.pdf

(mpOTR) specification written by Ian Goldberg et. al.[4] This will guarantee Cryptocat a wider body of academic study as a secure cryptographic system, while also bolstering its Internet censorship resistance.

What can it fight? Once mpOTR is implemented for the first time, the protocol can be ported to any Instant Messaging client on the Internet. This means that even if Cryptocat is purged entirely from the Internet, its complete and utter eradication would still be survived by the same multi-party encrypted chatting protocol being accessible in other Instant Messaging clients, such as Pidgin[5] or Adium[6]. Cryptocat's chatting protocol will become a standard for all other Instant Messaging systems to adopt, thus permeating the Cryptocat system throughout the Internet.

What interesting features will it have? Encrypted conversations with a virtually unlimited number of parties simultaneously. Encrypted file and photo sharing. Is compatible with any Instant Messaging software that implements the protocol.

When will it be ready? We hope to have mpOTR implemented in Cryptocat and specified in a protocol design document by September 2012.

Seamless Compatibility with the Tor Network

What is it? The Tor Project[7] provides the most well-researched, academically sound volunteer-run Internet anonymity and censorship-circumvention network in the world. Tor can provide Cryptocat with a powerful, all-included layer of censorship circumvention, which Cryptocat can maximize the potential of by:

A. Running a Tor Hidden Service (currently available at <http://xdtfje3c46d2dnjd.onion>) and running Tor compatibility testing with both Cryptocat servers and clients upon every release.

B. Implementing a Cryptocat app for Firefox, to be included by default in the Tor Browser Bundle[8] which provides a one-click Tor-connected browser.

---

[4] http://www.cypherpunks.ca/~iang/pubs/mpotr.pdf

[5] http://pidgin.im

[6] http://adium.im

[7] https://torproject.org

[8] https://www.torproject.org/projects/torbrowser.html.en

C. Implementing Tor compatibility within Cryptocat apps for mobile phones.

What can it fight? Tor has proven capable of circumventing Internet censorship in China, Iran and other countries with a repressive Internet record, even when attacked directly by cyber-intelligence authorities. Seamless integration with Tor guarantees that any Tor user is automatically a potential Cryptocat user regardless of the Internet censorship threat.

When will it be ready? Tor compatibility will ship with every Cryptocat server and client ever released. The Cryptocat plugin for Firefox will be designed to ship with the Tor Browser Bundle, and is expected to be finished by September 2012.