

# Mega.nz: A Technical Write-up

## Brief Overview

During Q1 of 2012, one of the most popular websites for file sharing, MegaUpload, was shut down by the United States government. Founder Kim Dotcom (yes, his legitimate last name is pronounced like “.com”), within the year founded Mega.nz, another file share network.

Mega.nz however is vastly different from MegaUpload. Unlike former file share giant MegaUpload, Mega.nz is not a public file share website, and instead is a private network using AES encryption. It also includes chat features, file transfers and video chat.

While still highly debated in the community as a viable option for secure file transfer and communication, scrutiny has developed over the years on the validity of Mega.nz’s and Kim Dotcom’s ethics over the years.

## Functionality

Mega.nz has a primary feature and a few secondary features. The primary feature is the encrypted file storage/sharing. This was the overall intent of the program early on; however other secondary features were later added. This includes the encrypted chat, encrypted video chat, encrypted purchases, encrypted voice chat, as well as plugins for Chrome, Firefox, and IOS security plugins.

Mega is available on IOS, Android, Windows, Mac, Windows Phone and Blackberry.

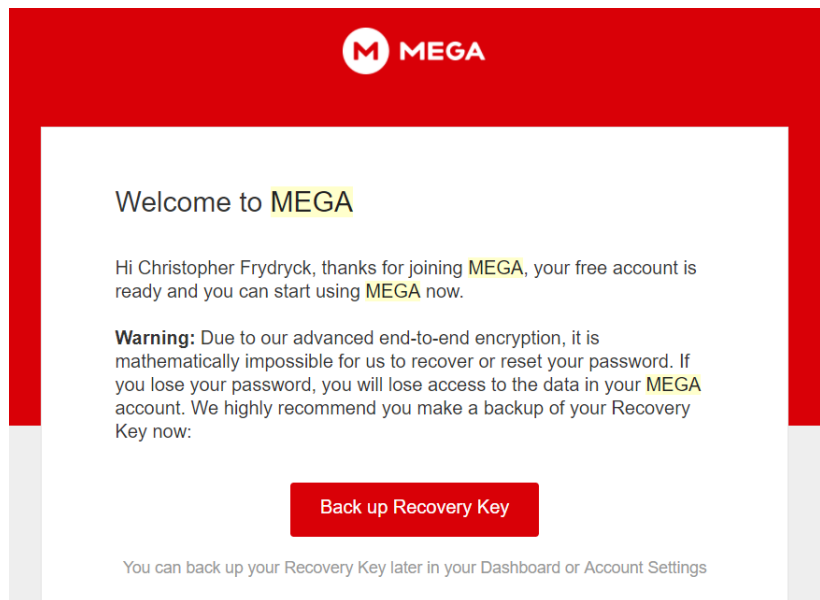


Figure 1

Setting up the tool is quite simple. Upon signing up (with minimal information may I add), there will appear a prompt to activate the account through the email provided. Upon verifying, you will have access to your private key through AES encryption. Note: once the account is created, the algorithm cannot be cracked by Mega.nz and it is recommended you make a backup recovery key (see figure 1).

There are also several different account options. The free option does not compromise your security or make your account at a greater risk. The pay accounts allow:

- Larger cloud storage capacity
- Larger transfer storage capacity
- Greater transfer quota
- Password protection settings
- File expiration settings













 PRO LITE	 PRO I	 PRO II	 PRO III
4.99 € /month	9.99 € /month	19.99 € /month	29.99 € /month
 200 GB STORAGE  1 TB TRANSFER	 1 TB STORAGE  2 TB TRANSFER	 4 TB STORAGE  8 TB TRANSFER	 8 TB STORAGE  16 TB TRANSFER

Figure 2

In regard to specific settings to be attended to, there are a few security features that can be considered. The first of which is under file management, giving the user to wipe all data after logging out, or encrypting the data. This will be wiped from the server and history of the user's data. Another setting is the cancel account button. If your account is canceled, it is wiped forever, and will never be recoverable. This is similar to losing your password, since it is stored on your private key. If forgotten or deleted, your account is lost forever.

## Encryption

Mega.nz is encrypted on the client-side with AES encryption methods. This is important since it is encrypted before it reaches the server. Dotcom in his boisterous fashion stated, "If servers are lost, if the government comes into a data center and rapes it, if someone hacks the server or steals it, it would give him nothing," while talking about the encryption being AES on the client side. This is similar to DES, but with a larger bit key and fits on the symmetric key platform with Twofish and Blowfish. This is much faster at encrypting data than asymmetric encryption, but that does not leave Mega.nz invulnerable.

In November 2016, a hacker group by the name of Amn3s1a had successfully accessed source code from the admins of Mega as well as chat directories, the Chrome browser tool and even a private RSA key. The group exclaimed that the software was vulnerable and that a piece of software that lacks being entirely open-source is a vulnerable piece of software. While many of the claims were disputed by Mega on the information collected, the group said they will wait for the right time to release the data.

The vulnerability was in an escalation of privilege attack. It was an attack based on access control that allowed the user to spoof themselves and grant themselves administrative abilities. They had done this on the server side, granting them access to private keys that can decrypt information. This became an issue for the overall integrity of the data provided to the server, even if it was previously encrypted on the server side. This is because the key is what truly keeps the data private, and their access to the private key gave them permission that should have never been granted in the first place.

Settings the user has access to with encryption are limited since Mega is not entirely open source. The user does have access to have data behave differently, and can either have it encrypted or wiped from

their servers. This way, if a breach occurred, the data does not exist and has been overwritten. Another feature is the ability to back up your key since that is the only way to enter your account without a password. This private key is important for the user to back up, otherwise their account may merely exist in limbo forever if unrecoverable. This is a great possibility since Mega does not have access to passwords for users if they forget the account information.

## Security Role

The CIA triad (confidentiality, integrity and accessibility) play a key role in Mega's design. Typically, a vulnerable design fails to fulfill one of the three in the triad. Without noticeable vulnerabilities, Mega would be considered confidential due to its client-side encryption, the integrity would be considerably strong due to the more complex AES encryption (instead of DES), and accessibility is quite easy for the user to access their data by visiting Mega.nz. It seems like a slam dunk when it comes to security, but there are definitely a few issues.

During the conception of Mega, the software had bugs that threatened the integrity of the software's confidentiality. While fixed swiftly, there was an evident XSS (cross site scripting) hole and a poor hash function that allowed a user to skip access control and exploit sensitive data on users. This issue is a huge one since it would ultimately destroy all three parts of the CIA triad. Confidentiality would lack due to others having the information shared among the private servers, integrity would be destroyed since it was bypassed by an XSS hole, and accessibility could lack if the users maliciously deleted the accounts and the information along with it. It is a security nightmare.

Early on they also had to adopt a system that required stronger passwords. This would help prevent brute force attacks from outside attackers from harming the integrity of the company's mission statement. Otherwise, Mega would share similar traits to Google Drive or Dropbox.

The final issue within the first week was a weak random number generation for the keys produced. This is a problem since a pattern could be noticeably studied and break the account of anyone who was vulnerable to the WebKit's `crypto.getRandomValues()` method. Ultimately this was another integrity issue with the software.

However, with a strong system, this tool can play a major role in the CIA triad. In an ideal scenario, it would keep data confidential between those who own it and those who had data shared with them. This also could be susceptible to man-in-the-middle attacks, but we are viewing this in an ideal scenario. It also could improve the integrity portion of the CIA triad. It would remain invulnerable and strong through the encryption and the private key of each individual user. This would help prevent outside attackers from entering without the longevity of an asymmetric encryption system. As for accessibility, if the other two are held to the highest standards, we should have an ease of accessibility for the user to access their files in a feasible manner. However, this is in an ideal world where bugs, vulnerabilities and malicious intent do not exist.

Since we do not live in a world that would make security pointless, there are certain attacks that Mega.nz would prove itself a worthy challenger against the everyday hacker or hacking group. One attack would be a man-in-the-middle attack. Since data is encrypted on the client-side and it requires

data to be sent to only specific certificates, it would make a man-in-the-middle take a lot more difficult since they would have to break into the server infrastructure to successfully poise themselves as Mega. Another attack Mega is good at handling is rainbow road attacks. This is because the data for accounts does not exist on a rainbow table. Instead, it is hashed, salted and not granted access to anyone to access. Even if the government were to require the information for a certain account to be handed over, the company does not have access to the data. This secure, but unmonitored approach is what has left Dotcom in scrutiny with the law in the past. He cannot and will not comply with the law on these matters because the data does not exist. Hence, a rainbow road attack would be unable to execute properly.

## User Considerations

Mega.nz serves a purpose outside of Google Drive or Dropbox that users may gravitate towards. Firstly, it seems more secure than other cloud storage/file sharing options. While Google Drive and Dropbox both have security measures themselves, they are not encrypted on the client-side, nor are the alternatives to Mega.nz as generous with their free plans. While many people disregard security more than they should, Mega's approach to giving 50gb of free data storage is incredibly generous compared to Google Drive's 15gb and Dropbox's 2gb.

Mega is designed to allow a mass encrypted communication chain between verified certificates that allows users to feel more secure about the data transfer. I say "communication chain" since sharing data is still a way of communication, as well as their integration of chat abilities and video calls. It would work well for private situations where data is meant to remain private (IE: a business or legal documents).

However, there are a few weaknesses to consider with the software. One is account security. While data is quite secure, accounts are almost too secure that if a backup private key is not made. Since this is more technical than usual, it is very possible that this software would not be recommended for those who are not literate in technical terms. Even the settings seem a little confusing for users, and one can tell that the settings were written by a programmer. For instance, we see a setting for "number of parallel upload connections." This would be incredibly confusing to a user not literate in the world of technology or the internet of things. This hurts the overall availability of a user to utilize the settings to their full capacity since the confusion factor is at play here.

Another example of a shortcoming with the software is the broad confusion of what Mega.nz truly is. Is it a file share? Is it a cloud storage? Is it a messenger? It seems like it has too many purposes that can confuse the user. This makes many of the settings and even the security features arbitrary for your daily usage. This then begs the question, why not use Google Drive or Dropbox for file sharing or text someone to message them? Unlike Dotcom's predecessor, MegaUpload, Mega seems to be more of a five inch shallow pond, dipping its feet into everything instead of focusing on one topic. This raises security issues that give attackers more doorways into the cracking a vulnerability that inevitably exists after too many features are implemented.

Luckily there is little risk in using Mega.nz. Unlike other security software, Mega has no way of formatting/encrypting your hard drive, Mega cannot brick your computer, it is malware free (according

to Kaspersky anti-virus and is more secure than the typical software on the market. However, the risk in this software is forgetting your password (elaborated earlier multiple times) and deleting data. For instance, if data is deleted from the recycling bin it is unrecoverable. So if data is important and held on Mega, make sure there is a backup key and all data is where it should be before emptying the recycling bin, or your availability will be compromised.

## Bibliography

Graeber, Charles. "Megaupload Is Dead. Long Live Mega!" *Wired*. Conde Nast, 18 Oct. 2012. Web.

Kerr, Dara. "MegaUpload Rises from the Dead as Mega." *CNET*. CNET, 18 Oct. 2012. Web.

"MEGA." *MEGA*. N.p., n.d. Web.

Protalinski, Emil. "Kim Dotcom's Mega to Launch Browser-based Encrypted Video Call and Chat Service 'soon'." *VentureBeat*. Venture Beat, 29 Dec. 2014. Web.

Rouse, Margaret. "What Is Privilege Escalation Attack? - Definition from WhatIs.com." *SearchSecurity*. SearchSecurity, 10 Nov. 2010. Web.

"What Is an XSS Hole? - Definition from Techopedia." *Techopedia.com*. N.p., n.d. Web.

Whittaker, Zack. "Hackers Say They Took Mega.nz Source Code and Admin Logins." *ZDNet*. ZDNet, 21 Nov. 2016. Web.