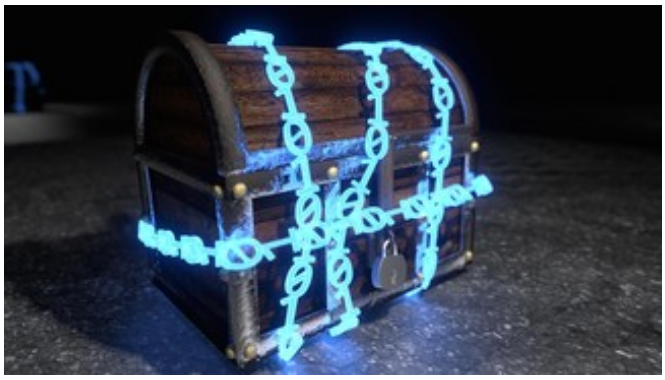
A digital safe for sending confidential documents

3 October 2014, by Cécilia Carron



Credit: EPFL Caillet Jamani

To secure the storage and transfer of documents, two post-docs at EPFL have recently developed three solutions. The solutions use encryption to render documents inaccessible to anyone who does not possess the secret code chosen by the user.

To make you documents inaccessible to a third party, two post-doctoral fellows at EPFL have created a start-up called Di55erent around three data security solutions. The solutions are based on the clever but intuitive ideas of locking files in a safe or breaking them apart like a jigsaw puzzle, also referred to as key-based encryption and files-splitting, respectively. Only the person in possession of the right key can decrypt the puzzle pieces and reconstitute the original file.

MakeSends performs secure files transfers. The service encrypts the user's files on the browser itself using a secret code selected by the user. "Once encrypted, the contents of the files cannot be accessed by anyone, not even us," states Radhakrishna Achanta, one of the co-founders. This is because cracking a well-chosen code takes a long time. It is similar to trying to open a safe by going through every possible combination of digits: it can be done, but it takes years. The level of security is similar to that of online banking, which requires two-level authentication. To reconstitute the document, the user has to enter the correct password, which is transferred by the sender via SMS or telephone.

The service is extremely easy to use. The user simply uploads a file, enters the email addresses of the sender and receiver, chooses a secret code, and clicks on "Send." There are already several other approaches to keep online files safe. Some of them encrypt files during transmission, while others encrypt the data once it arrives on the storage server. "These schemes have their weaknesses," explains Thomas Lochmatter, the other co-founder. "In the first case, the files are only encrypted during transmission, which means that they can be read before of after they are sent which is not secure enough, apart from being suscesptible to " man-in-the-middle " attacks.. In the second case, the company that stores the files has access to them. That means that its employees can read them."

This "digital safe" also keeps data out of the hands of government authorities. According to the revelations in the American media in 2013, the National Security Agency and FBI has access to user data including chat conversations, images, videos, emails, and other documents stored by the nine largest IT companies. " Our solution provides end-to-end security, from the sender to the receiver, making files illegible for all others who do not possess the secret code ", the founders emphasize.

Building on the technology used for MakeSends, the start-up has developed two other solutions that provide data privacy protection to the users. The first one, swi5t is a software solution that encrypts files before placing them on a cloud server by first enveloping them in a secure HTML file. The other product, uKeepIt, first splits each file into multiple

pieces, much like a jigsaw puzzle, and encrypts and stores each fragment on one or several clouds. Only users that have the password can find the pieces and put them together again.

Provided by Ecole Polytechnique Federale de Lausanne