Circular all-or-nothing: A new approach to protect data from key exposure

7 February 2019, by Ingrid Fadelli

An attacker possessing the key and all but one data fragment is not able to decrypt even a small portion of the initial data. Credit: Kapusta, Memmi & Rambaud.

A team of researchers at Telecom ParisTech has developed a new method to protect encrypted data against key exposure. Their algorithm, presented in a paper pre-published on arXiv, transforms, fragments and disperses data so that it remains protected, unless all storage nodes are compromised.

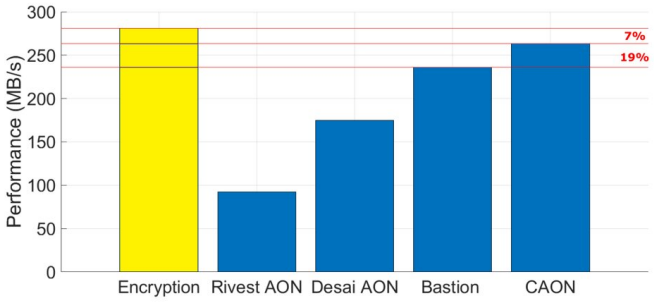
"Nowadays, we observe two things," Katarzyna Kapusta, one of the researchers who carried out the study, told TechXplore. "On the one hand, the popularity of data outsourcing is still growing. On the other hand, every two months, we witness a major data breach exposing users' data. Attackers are becoming more and more powerful. They are sometimes able to acquire encryption keys using bribery or coercion. In such situations, simply encrypting data may not be enough."

According to Kapusta, an encryption method is only as good as the key generation and management strategy employed by individual users. In collaboration with her colleagues Gérard Memmi and Matthieu Rambaud, she hence set out to develop a more effective method to protect encrypted user data against malicious attacks.

"We propose a set of methods that combine encryption with data fragmentation and dispersal," Kapusta said. "They aim at reinforcing data confidentiality in order to protect against an attacker that was able to acquire the encryption keys."

Classical symmetric encryption algorithms work by encrypting data into a ciphertext using an encryption key that needs to be kept secret. This means that if the encryption key is found by an attacker, data becomes vulnerable.

All-or-nothing transform (AONT), also known as the all-or-nothing protocol, is an encryption method first introduced by Ronald L. RIvest in the late 1990s. It works by transforming input data into a ciphertext so that it can only be decrypted when the ciphertext is complete.



A performance benchmark, comparison between CAON and other techniques, simple encryption (AES-NI in CTR mode, yellow) is used as the baseline. Credit: Kapusta, Memmi & Rambaud.

"All-or-nothing encryption reinforces data confidentiality by protecting the data against weak or leaked encryption keys," Kapusta explained. "It produces a ciphertext that can be only decrypted when it is complete. Fragments of such ciphertext are resistant against a situation of key exposure: It is not possible to decrypt the portion of the data inside one fragment without the rest of the fragments, and this even if the encryption key is

known. Encrypting data using an AON, then fragmenting and dispersing the obtained ciphertext reinforces data confidentiality."

When combined with data fragmentation and dispersal, AONT approaches can protect data from attackers who acquire the encryption key but are unable to gather all data fragments. However, as they require at least two rounds of data encryption, these methods typically result in a significant decrease in performance. The study carried out by Kapusta and her colleagues addresses the limitations of existing AONT approaches, introducing an alternative method called circular all-or-nothing (CAON).

"Classical symmetric encryption is the main component of each all-or-nothing method protecting against less powerful attackers without the knowledge of the encryption keys," Kapusta said. "The protection against more powerful attackers possessing the keys is achieved by combining the encryption with a component creating dependencies between data inside of the ciphertext that will protect against the key exposure. In older AON methods, this component is a pre-processing step, while in recent AON, these dependencies are created after data encryption. CAON belongs to the second group of AON, as it applies a linear transform over the encrypted data. This transform 'exclusive-ors' blocks of data in a chaining way – each block is exclusive-or with its predecessor, and the first block that does not possess a natural predecessor is exclusive-ored with the last one."

The key difference between CAON and other AON approaches is that the former only requires a single XOR operation per data block, which is the minimum possible in terms of additional processing. This makes it significantly faster than existing AON approaches, including Bastion's scheme, a recently devised method that protects fragmented data against key exposure using a single round of data encryption and linear post-processing transform.

"CAON enables the protection of outsourced data against key exposure without leading to a performance burden," Kapusta said. "The overhead coming from the post-processing transform applied over encrypted data is almost negligible. Previous AON were slow and therefore not practical."

In the future, CAON could protect online user data against key exposure attacks. For instance, it could be integrated inside modern distributed storage systems or multi-cloud solutions, offering greater confidentiality without the costs typically associated with AONT encryption methods.

The team is now working on new methods combining encryption, fragmentation and data dispersal that could be applied to cloud computing or IoT edge computing. More specifically, they are planning to release a fine-grained open source implementation of CAON.

More information: Circular all-or-nothing: revisiting data protection against key exposure. arXiv:1901.08083[cs.CR]. arxiv.org/abs/1901.08083

All-or-nothing encryption and the package transform. dl.acm.org/citation.cfm?id=740733