A plea for paranoia

Today massive amounts of data are generated, processed and stored on computers and servers throughout the world. Big data. In the Bitcoin system (blockchain) data is copied intensely to provide authenticity. Storing data has become a huge and important business. The important issue for security in this context is that data cannot be deleted *anymore. This calls for higher security, this calls for long-term security.*

Symmetric encryption is often said to be the workhorse in cryptography. Public- key techniques are used to exchange keys, but the encryption of the bulk of data is usually done with symmetric encryption systems such as the AES. It is widely believed that AES is a good symmetric encryption system, and it has been predicted that encryptions using AES with 256-bit keys will be safe until at least 2040.

Cloud storage is gaining more and more popularity. Providers have large storage centers where customers upload their data, e.g., Amazon S3. The customer can later access the data, possibly multiple times, but is no longer in control of where the data is stored. The providers might have many different servers which could possibly be located in many different countries.

At the same time massive amounts of sensitive data needs to be stored. Companies and governmental agencies need to store personal data about their employees, medical data, financial data etc. Hospitals and doctors store private data about their patients. If such data are to be stored “in the cloud”, then it is natural for the parties to ensure that the data is encrypted properly. Some providers of cloud storage also offer encryption, e.g., in Amazon S3 customers can encrypt their data using a pre-installed encryption system, right now using AES with 256-bit keys, or they can define their own encryption system.

Cloud storage introduces a new angle to the world of encryption, namely how to get long-term protection of data using encryption, or what could be called *long-term encryption*. The problem is that although the customer can ***upload*** data to the cloud, and ***retrieve*** it again, she cannot ***delete*** the data from the cloud. Taking AES as an example again, the above-mentioned prediction that AES encryption is safe (only) for 20 years from now, means that this type of encryption is by far not strong enough for all applications of cloud storage.

LRK 2019.