Encryption method takes authentication to a new level

30 September 2016

Credit: VTT Technical Research Centre of Finland

VTT Technical Research Centre of Finland has developed new kinds of encryption methods for improving the privacy protection of consumers to enable safer, more reliable and easier-to-use user authentication than current systems allow.

The method combines safety, usability and privacy protection, when, until now, implementing all three at the same time has been a challenge.

"Our method protects, for example, the user's biometric data or typing style," says Senior Scientist Kimmo Halunen.

In biometric authentication, the risk is that a person's permanent biometric identifiers, which cannot be changed, leak out of the database. VTT's method stores data in the database in an encrypted form and all comparisons between measuring results and the database are conducted using encrypted messages so there is no need to open any biometric data at this stage of the process.

VTT integrates new kind of encryption methods, such as homomorphic cryptography and secure exchange of cryptographic keys, to known measuring methods of typing styles.

The traditional authentication based on passwords has proved to be weak, since users mostly select weak passwords, and hackers often succeed in stealing quite large password databases. Recently, companies such as Dropbox and Yahoo have fallen prey to such data breaches.

In addition, new types of user environments, such as smart devices, cars, and home appliances, create challenges for user authentication with the help of passwords.

VTT is now looking for a partner for further processing and commercialisation of this method, which could be available to consumers within a year or two.

Provided by VTT Technical Research Centre of Finland