Algorithms improve how we protect our data

May 4 2021

Prof. Yongjune Kim, DGIST Credit: DGIST

Daegu Gyeongbuk Institute of Science and Technology (DGIST) scientists in Korea have developed algorithms that more efficiently measure how difficult it would be for an attacker to guess secret keys for cryptographic systems. The approach they used was described in the journal *IEEE Transactions on Information Forensics and Security* and

could reduce the computational complexity needed to validate encryption security.

"Random numbers are essential for generating cryptographic information," explains DGIST computer scientist Yongjune Kim, who co-authored the study with Cyril Guyot and Young-Sik Kim. "This randomness is crucial for the security of cryptographic systems."

Cryptography is used in cybersecurity for protecting information. Scientists often use a metric, called 'min-entropy', to estimate and validate how good a source is at generating the random numbers used to encrypt data. Data with low entropy is easier to decipher, whereas data with high entropy is much more difficult to decode. But it is difficult to accurately estimate the min-entropy for some types of sources, leading to underestimations.

Kim and his colleagues developed an offline algorithm that estimates min-entropy based on a whole data set, and an online estimator that only needs limited data samples. The accuracy of the online estimator improves as the amount of data samples increases. Also, the online estimator does not need to store entire datasets, so it can be used in applications with stringent memory, storage and hardware constraints, like Internet-of-things devices.

"Our evaluations showed that our algorithms can estimate min-entropy 500 times faster than the current standard algorithm while maintaining estimation accuracy," says Kim.

Kim and his colleagues are working on improving the accuracy of this and other algorithms for estimating entropy in cryptography. They are also investigating how to improve privacy in machine learning applications.

More information: Yongjune Kim et al, On the Efficient Estimation of Min-Entropy, *IEEE Transactions on Information Forensics and Security* (2021). DOI: 10.1109/TIFS.2021.3070424