HARVEST NOW, DECRYPT LATER

Harvest Now, Decrypt Later

It is now inevitable that the encryption algorithms used to secure vital data across the world – from defence and banking to infrastructure and air travel - will be breached. With the escalation in computing power enabled by quantum technology, the question is not if, but when potentially devastating breaches will occur.

With 'harvest now, decrypt later' hacking strategies currently in progress, criminals are banking on the power of quantum computing to allow them to unlock huge data resources. The onus is on companies not just to consider the future quantum threat but to determine how best to protect current resources today.

Paul German, CEO, Certes Networks, explains the risk associated with bulk encryption strategies and the importance of crypto-segmentation in reducing criminal exposure to data in a post-quantum world.

Quantum Leap

Quantum computing is edging ever closer to reality, with venture capitalists investing almost $1.02 billion in quantum computing start-up companies this year alone. While there is huge excitement around the step change in AI performance, for example, that quantum compute power could unleash, the security implications are potentially devastating.

Security experts globally expect quantum computers to herald the breach of the asymmetric cryptography used globally to secure everything from defence to infrastructure. While classical compute power would take billions of years to execute Shor's Algorithm, which is proven to break the encryption methods currently in place, the arrival of a quantum computer of sufficient size and complexity totally changes the game.

For companies reviewing security strategies, this post-quantum security threat is not in the future; it is not about considering how to respond as and when quantum computing becomes available. Criminal organisations globally are embarking upon mass data harvesting & breach schemes today on the basis that even though the information cannot be immediately decrypted, at some point in the future, access to quantum compute power will unlock these information resources. Systems are at risk - not in the future, but today.

Time & Data

While securities bodies across the world, including Open SSL, are working hard to develop new quantum-proof algorithms, no organisation can afford to wait. Changes need to – and moreover can - be made today to safeguard current data resources and reduce the decryption risk posed by quantum computing. What is required is both a change in mindset and a change in technical approach to the solutions already available.

A key step is to minimise the value of 'harvest now, decrypt later' strategies by reducing the amount of 'usable' data collected during a breach. During many recent attacks, criminals have been able to spend months collecting data – and although it is encrypted, they had the time (often months) to access vast data sets. This enabled them to build up enough knowledge about the encryption algorithm being used to know that, once they have the opportunity to use quantum computing, they will be able to break the key and have full access to the entire data resource.

The priority today to is to institute data securities policies that radically reduce the time and data available to criminals.

Crypto-segmentation

Many organisations are starting to adopt micro-segmentation as part of their data security policies. While this is a step in the right direction, unless they are also applying cryptography, ultimately data harvesting is still very real threat.

It is also vital to recognise the inherent risk associated with the bulk encryption model: using the same encryption key, however strong, to protect all data resources is not a robust policy. Once in, a criminal has one data set to work with; one encryption key to identify.

The concept of crypto-segmentation, however, is based on a far more nuanced approach to protecting data, defining different data classes for each data type and protecting each class with its own encryption algorithm and encryption key.

> *Criminal organisations globally are embarking upon mass data harvesting & breach schemes today on the basis that even though the information cannot be immediately decrypted*
>
> **Paul German, CEO, Certes Networks**

In addition to creating multiple data classifications, regular rotation of the encryption keys used for each class will also hugely limit a criminal's time with any data set. If keys are being rotated every hour, for example, anyone capturing the data has minutes, not months, to work on a data set. That means minutes to understand the data; to determine which data packets belong to which data classification; group the data sets together to create a sample; identify the encryption used for each data class and then reverse engineer the keys. Plus, with very small sample sizes in each data class, it becomes incredibly difficult to crack the keys being used.

Incorporating New Standards

The next generation of post-quantum encryption standards are being developed. But this is a challenge that will never disappear – especially for security agencies that are required to retain data for decades. With the phenomenal growth in computer power, tomorrow's ground breaking algorithm will be easy to break in five, ten, 20 years' time – however smart the algorithm, no organisation can risk the reliance on one encryption key.

Bulk encryption is inherently flawed, which means organisations must maximise the value of an array of standard encryption algorithms. Using crypto-segmentation and key rotation is an important step; significantly increasing protection against the quantum threat even with current encryption algorithms. As and when new post-quantum encryption standards are introduced, they can be incorporated into this model to maximise the organisation's protection.

Conclusions

This threat is not the future; it is happening today. 'Harvest now, decrypt later' breaches are occurring right now. Quantum compute services in the cloud are offering criminals the chance to buy a slice of quantum power. Algorithms will continue to evolve and improve; criminals will continue to gain access to ever more powerful computers. By creating multiple data classes and using regular key rotation, not only is the limited data set harder to decrypt but it also likely to offer far less value; value outweighed by the enormous cost of quantum compute power.

Contact Certes Networks

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

CERTES NETWORKS

Tel: 1 (888) 833-1142
sales@certesnetworks.com

www.certesnetworks.com