SANDBOXAQ™

SoftBank

Safeguarding Telco Data in Japan

As the world progresses toward the quantum era, quantum computers will create new opportunities for SoftBank and other telecommunication providers to deliver better, faster and more innovative services and solutions.

However, quantum computers will also pose a serious risk to the entire global telecommunications industry, due to their predicted ability to break existing Public-Key Cryptography (PKC) standards. Every security-conscious organization will need to transition to Post-Quantum Cryptography (PQC) algorithms, which are expected to be standardized by the National Institute of Standards and Technology (NIST) within the next two years and will be mandated for use by most governments.

SoftBank took a bold step towards protecting its customers by exploring PQC, the next generation of quantum-resistant encryption algorithms. Specifically, SoftBank partnered with SandboxAQ to rigorously test several new PQC algorithms, in conjunction with its existing cryptographic protocols, to determine their impact on network security, performance and other potential benefits.

After a thorough evaluation, SoftBank was satisfied that a hybrid cryptographic solution, composed of both classical and quantum-resistant algorithms, would provide the best protection for its users and customers while maintaining network performance and regulatory compliance. SoftBank's determination to migrate to PQC demonstrates its global leadership, vision and dedication to its customers, and will give it an advantage in the global telecommunications marketplace.

Partner
SoftBank Corp.

Industry
Telecommunications

Products & Services

Provision of mobile communications services, sale of mobile devices, provision of fixed-line telecommunications and ISP services

Consolidated Organization Size

49,000+

Country
Japan

Website
https://www.softbank.jp

Continuous Security Enhancement

Telecommunication companies like SoftBank are a prime target for threat actors, due to the high volume of sensitive business and consumer data crossing their networks and stored in their databases. To protect its customers, SoftBank strives for continuous security enhancements and threat evaluation.

As the global development of quantum computers progresses, SoftBank's R&D team noted the potential threat posed by these systems. Recognizing that it will only be a matter of time before quantum computers can break current encryption protocols such as RSA and elliptic curve cryptography (ECC), they grew increasingly

concerned that the existing cryptographic security would not be adequate to protect their customer's data against quantum-based attacks. They also became aware of Store Now Decrypt Later attacks (SNDL), in which threat actors exfiltrate and store encrypted data until fault-tolerant quantum computers are available to decrypt it. Some experts believe this could be as soon as 2030.

SoftBank made assessing quantum risk a priority, including exploring and developing internal competency on PQC to protect its networks and customer data from quantum attacks. According to the World Economic Forum, more than 20 billion devices worldwide will need PQC upgrades in order to become quantum-resistant, making this transition a once-in-a generation shift in the global cybersecurity environment.

How SoftBank Leveraged SandboxAQ

SoftBank worked with SandboxAQ engineers to stress-test various communication channels and evaluate the impact of each PQC algorithm on network performance and security. A central goal was to arrive at the best approach for SoftBank to integrate the new PQC protocols into their existing security architecture, without sacrificing performance.

Using AQ Benchmark, the joint SoftBank/SandboxAQ team compared the network performance of existing elliptic curve-based encryption protocols against several of the new quantum-resistant PQC protocols approved by NIST.

They created different scenarios for a number of web traffic patterns, such as gaming, web page loading, media sharing, and content streaming. They ran tests for each algorithm, recording metrics such as latency, connection success, CPU load, memory utilization, and others. The number of connections per second were ramped up until a failure point was reached. The team also conducted stress tests on handset devices and servers. After several months of testing, SoftBank gained a better understanding of its cybersecurity posture and how well its infrastructure would handle migrating to quantum-resistant cryptography.

Insights

When cryptographic protocols are deployed in data transmission infrastructure, they can place a significant load on communications and cause latency problems, resulting in poor quality and lower throughput. In general, the heavier the encryption, the greater impact it has on data transmission.

One primary insight SoftBank gained was that lattice-based PQC algorithms were significantly better than other alternatives. While lattices have been used in mathematics for centuries, it was not until the 1990s when they started being used to construct cryptographic schemes. The past two decades have seen a tremendous evolution in lattice-based cryptography schemes, and NIST recently selected several lattice-based algorithms for possible PQC standardization.

The team also tested a hybrid cryptographic approach combining both new and existing algorithms. They found that a combination of structured, lattice-based PQC algorithms and non-PQC (classical) algorithms performed well across all traffic types and communication channels in the test scenarios. The hybrid approach allows SoftBank to guard against future quantum threats with only a marginal increase in overhead costs. It also allows SoftBank to maintain regulatory compliance and interoperability with other partners through the use of Federal Information Processing Standards-mandated classical algorithms.

> "SoftBank continues to focus on research and development in security technologies as well as network technologies to provide comfortable, safe and secure infrastructure services."
>
> - Ryuji Wakikawa, Vice President, Head of Research Institute of Advanced Technology, SoftBank Corp.

Conclusions

After a thorough and successful evaluation, the joint team determined that migration to PQC is ready to commence. The next step will be to define a specific set of security requirements and choose the most appropriate PQC algorithms and protocols. This will provide a further opportunity to refine the company's cryptographic inventory and measure performance.

"SoftBank continues to focus on research and development in security technologies as well as network technologies to provide comfortable, safe and secure infrastructure services," said Ryuji Wakikawa, SoftBank Corp. Vice President. "By leveraging our partnership with SandboxAQ and their expertise in quantum and quantum-safe technology, we will continue to promote the early implementation of quantum-safe networks. In particular, we expect that the need for quantum-safe networks will increase as the development of quantum computers progresses, especially among organizations that deal with information assets with long lifetimes, such as medical data or critical intellectual property."

About SoftBank

SoftBank Corp. (TOKYO: 9434) provides telecommunications services and combines them with advanced technologies to develop and operate new businesses in Japan and globally. SoftBank Corp. has 39 million mobile subscribers and 8 million broadband subscribers in Japan. Through its group customers, such as Yahoo Japan Corporation, PayPay Corporation and LINE Corporation, the company serves 86 million online media users, 51 million smartphone payment users and 92 million communication app users. With this strong business foundation and compelling number of customer touchpoints, SoftBank Corp. is expanding into non-telecom fields in line with its 'Beyond Carrier' growth strategy while further expanding its telecom business. Also, by fully harnessing the power of 5G, AI, IoT, Digital Twin, Non-Terrestrial Network (NTN) solutions, including High Altitude Platform Station (HAPS)-based stratospheric telecommunications, and other key technologies, SoftBank Corp. aims to realize the "Implementation of Digitalization into Society".

In recognition of its ESG initiatives, SoftBank Corp. was selected for inclusion in the Dow Jones Sustainability Indices, FTSE4Good, 2022 Constituent MSCI Japan ESG Select Leaders Index and other leading global ESG investments indices.

About SandboxAQ

SandboxAQ is an enterprise SaaS company, providing solutions at the nexus of AI and Quantum technology (AQ) to address some of the world's most challenging problems. SandboxAQ's Security Suite includes cryptographic inventory and crypto-agility solutions to help government agencies and corporations protect their most sensitive data, ensure long term cyber resilience and remain compliant with new government regulations. The company's core team and inspiration formed at Alphabet Inc., emerging as an independent, growth-capital-backed company in 2022.

SANDBOXAQ™