TYCHON

carahsoft.

7 Reasons You Need to Upgrade to Post-Quantum Cryptography Today

Thank you for downloading this TYCHON resource! Carahsoft is the public sector distributor for TYCHON solutions.

To learn how to take the next step toward acquiring TYCHON's solutions, please check out the following resources and information:

For additional resources:
carah.io/TYCHONResources

For upcoming events:
carah.io/TYCHONEvents

For additional TYCHON solutions:
carah.io/TYCHONProducts

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
TYCHON@carahsoft.com
844-445-5688

To purchase, check out the contract vehicles available for procurement:
carah.io/TYCHONContracts

7 Reasons

You Need to Upgrade to Post-Quantum Cryptography Today

1
Harvest Now, Decrypt Later Attacks

2
The Shor's Algorithm Threat

3
Long-Term Security & Compliance

4
NIST Standardization & Industry Adoption

5
Business Continuity & Future Proofing

6
Hybrid Cryptography

7
PQC Readiness & Classical Security Enhancement

The Urgency of PQC Adoption

The advent of quantum computing presents an unprecedented threat to current cryptographic systems, necessitating a swift transition to Post-Quantum Cryptography (PQC). This white paper discusses the critical importance of upgrading to PQC, including the strategic use of hybrid cryptography, to ensure long-term data security in the face of emerging quantum threats. With NIST's recent announcement of a timeline for deprecating current cryptographic standards, including ECDH and X25519, the urgency of this transition has become even more apparent.

1. "Harvest Now, Decrypt Later" Attacks

Adversaries, particularly nation-states, are actively capturing encrypted data today with the expectation of decrypting it in the future using quantum computers. This strategy, known as "harvest now, decrypt later," poses a severe threat to sensitive information such as military secrets, financial transactions, and personal data. Even if an organization improves its security measures in the future, previously harvested data remains vulnerable.

2. The Shor's Algorithm Threat

Current public-key cryptography relies on the computational difficulty of factoring large numbers and solving discrete logarithms. Shor's algorithm, when implemented on a sufficiently powerful quantum computer, can efficiently break these cryptographic schemes. This development means that widely used encryption methods like RSA and ECC will become obsolete once quantum computers reach the required scale.

3. Long-Term Security and Compliance

Organizations with long data retention requirements, such as those in banking, healthcare, government, and legal sectors, face a particular challenge. As quantum computing advances, the risk to long-term data increases exponentially. Moreover, regulatory bodies are beginning to mandate the adoption of PQC, making compliance a critical aspect of organizational cybersecurity strategies.

4. NIST Standardization and Industry Adoption

NIST has made significant progress in standardizing PQC algorithms, selecting Kyber for encryption and Dilithium, Falcon, and SPHINCS+ for digital signatures. Leading tech companies like Google, AWS, IBM, and Cloudflare are already testing or deploying PQC solutions. Organizations that delay adoption risk falling behind in security capabilities and may face increased vulnerability.

5. Business Continuity and Future Proofing

The transition to PQC is a complex process involving upgrades to software, hardware, network protocols, and certificates. Organizations that start early gain a significant advantage in terms of security and operational continuity, positioning themselves as leaders in data protection and technological foresight.

6. Hybrid Cryptography: A Safe Transition Path

Hybrid cryptography, which combines PQC with traditional methods like RSA or ECC, offers a smooth and secure transition path. This approach allows organizations to maintain compatibility with existing systems while gradually introducing quantum-resistant algorithms.

7. PQC Readiness and Classical Security Enhancement

Many PQC algorithms, such as Kyber, offer performance advantages over traditional cryptographic methods. Implementing PQC can enhance an organization's overall security posture, providing resilience against both classical and quantum threats.

NIST's Timeline for Deprecating Current Standards

NIST has set a clear timeline for transitioning away from current cryptographic algorithms:

- By 2030, NIST will deprecate RSA, ECDSA, EdDSA, DH, and ECDH algorithms.
- After 2035, these algorithms will be completely disallowed.

Specifically, for ECDH and X25519:

- These algorithms will be deprecated by 2030.
- They will be removed as standards by 2035.

This timeline underscores the urgency of transitioning to post-quantum cryptography and has several implications:

1. Accelerated Transition: Organizations must expedite their adoption of post-quantum cryptographic solutions.
2. Widespread Impact: The deprecation affects a broad range of cryptographic applications.
3. Hybrid Approaches: During the transition period (2030-2035), hybrid cryptographic schemes may be necessary.
4. Long-term Data Protection: Data encrypted with soon-to-be-deprecated algorithms may become vulnerable.

How to Prepare Today

To prepare for the post-quantum era, organizations should:

1. Conduct a thorough assessment of cryptographic dependencies.
2. Begin testing PQC implementations.
3. Closely follow guidelines from NIST, NSA, and industry leaders on PQC migration strategies.
4. Implement hybrid cryptography solutions where possible.
5. Develop a comprehensive quantum-safe transformation strategy.

Conclusion

The transition to Post-Quantum Cryptography is a critical step in ensuring long-term data security and business continuity. With NIST's timeline for deprecating current standards, including ECDH and X25519, the need for action is more pressing than ever. Organizations must act now to protect their sensitive data from both current and future threats. By embracing PQC and hybrid cryptography solutions, businesses can safeguard their digital assets, comply with emerging regulations, and position themselves as leaders in the new era of quantum-resistant security.

About Tychon

Learn More: tychon.io

Tychon LLC is a software company founded by former U.S. Department of Defense cybersecurity experts. TYCHON, our core product, is the world's first advanced endpoint analytics and remediation platform designed to be the "gold source" for enterprise endpoint data. It provides the ability to search, visualize, remediate, and monitor security concerns across all endpoints within one powerful interface. TYCHON delivers a flexible endpoint management query and response tool that gives administrators and incident responders complete control of their systems.

TYCHON Quantum Readiness is an Automated Cryptography Discovery & Inventory (ACDI) tool designed specifically to help agencies meet the requirements of the Quantum Computing Cybersecurity Preparedness Act. It delivers a comprehensive cryptographic inventory and a prioritized inventory of vulnerable information systems.