THE IMPACT OF QUANTUM COMPUTING ON ENCRYPTION

Technical Brief - April 17, 2025

PULSAR
SECURITY

WEI
CYBERSECURITY

Purpose

To evaluate the emerging cybersecurity threat posed by quantum computing to widely deployed cryptographic systems and to provide recommendations for risk mitigation through proactive planning and cryptographic agility.

Background

Modern encryption, particularly public key cryptography, relies on the computational difficulty of problems like integer factorization and discrete logarithms. Algorithms such as RSA, Diffie-Hellman, and ECC (Elliptic Curve Cryptography) underpin most digital security, including TLS/SSL, VPNs, digital signatures, and secure email.

Quantum computing introduces a fundamentally different computational model that threatens to render these cryptographic systems obsolete. Algorithms like Shor's and Grover's offer exponential and quadratic speedups over classical counterparts, enabling quantum computers to break RSA and ECC in feasible timeframes.

Cybersecurity Implications

- **Data Confidentiality:** Encryption protecting long-term sensitive data (e.g., personal health records, state secrets, financial assets) is vulnerable to 'harvest now decrypt later' attacks.
- **Authentication and Trust:** Quantum enabled compromise of digital signatures undermines the authenticity of software updates, certificates, and blockchain integrity.
- **Legacy Risk Exposure:** Systems with long life cycles (e.g., embedded devices, critical infrastructure) may remain vulnerable for decades if not retrofitted with quantum-safe cryptography.

The information contained in this document is confidential, privileged, and only for the intended recipient

Technical Impact Analysis

Threat Vector	Current Status	Quantum Risk
RSA (2048-bit)	Secure under classical models	Broken via Shor's algorithm
ECC (256-bit)	Secure under classical models	Broken via Shor's algorithm
AES (128-bit)	Secure, with reduced strength under Grover’s	Requires doubling key size

---

Industry Response & Strategic Recommendations

1. **Adopt Crypto Agility**
   - Ensure systems can transition to new cryptographic algorithms without architectural overhauls.
   - Avoid hard coded or static crypto implementations.
2. **Monitor Post Quantum Standards**
   - Follow NIST’s Post-Quantum Cryptography (PQC) initiative.
   - Begin testing finalists such as CRYSTALS-Kyber (key encapsulation) and CRYSTALS-Dilithium (signatures).
3. **Implement Risk Based Prioritization**
   - Inventory data and systems with long-term confidentiality needs.
   - Prioritize updates for systems exposed to long-term interception threats.
4. **Engage in Quantum Readiness Planning**
   - Establish a transition roadmap for migrating to quantum resistant protocols.
   - Include vendor assessment and lifecycle management as part of security architecture planning.

The information contained in this document is confidential, privileged, and only for the intended recipient

Key Takeaways

- Quantum computing will render traditional encryption obsolete. Preparation must start now.
- Organizations should adopt a layered, crypto agile security model.
- Monitoring PQC developments and vendor readiness is essential for future proof cybersecurity strategies.
- The cost of inaction could be retroactive data breaches, unauthorized access, and systemic trust erosion.

Conclusion

Quantum computing is not merely a theoretical concern; it is a credible, near-future threat to global cybersecurity. Forward leaning organizations must evaluate their cryptographic posture, adopt agile frameworks, and prepare for a new era of encryption resilience. Transitioning to post-quantum cryptography will be a defining challenge, and opportunity of the next decade in information security.

The information contained in this document is confidential, privileged, and only for the intended recipient