WHITEPAPER

Encrypted Data Today May Be Public Information Tomorrow

How Xiid SealedTunnel™ Delivers Post-Quantum Security

The cybersecurity landscape faces a potentially catastrophic, looming threat: **"Harvest Now, Decrypt Later" (HNDL)** attacks. Malicious actors exploit this strategy by stockpiling encrypted data, confident that advancements in computing, including quantum computers, will allow them to decrypt it later and gain access to valuable information. Xiid addresses this challenge with Xiid SealedTunnel™, a groundbreaking solution that safeguards communication channels with Zero Knowledge Networking and post-quantum cryptography.

The Threat Landscape: Harvest Now, Decrypt Later (HNDL) Attacks

Today's Encryption is Insufficient

It goes without saying that encryption is important. The world has long embraced the reality that unencrypted data is, essentially, public information, so we accordingly secure everything from top secret government data to our individual web browsing activity.

For specific, high-priority targets, nation states may invest in attempts at undermining encryption and cryptography generally. These attempts are sometimes successful, such as with the "Flame" malware's MD5 collision attack.[1] However, the risk to most businesses and individuals from malware like Flame is often limited. If the standard encryption mechanisms used by the world at-large were to suddenly be broken, it would create a catastrophe of unimaginable proportions. Closely-held proprietary secrets, emails, files, phone calls, and more would all be compromised.

Encryption algorithms are assumed safe because they are designed to make it impossible for "normal" computers to ever break them.

1 https://www.wired.com/2012/05/flame/

Quantum computers defy this assumption and put nearly all encrypted data at risk.

Harvest Now, Decrypt Later Isn't Science Fiction

Quantum computers will be able to break most asymmetric (public-key) encryption and some of the symmetric encryption methods in use today within the next 5-15 years, and not even newer protocols like TLS1.3 are completely safe.[2]

Nation states and large hacking groups may employ a technique called Harvest Now, Decrypt Later in which encrypted data is intercepted today and stored, to be decrypted in the future once quantum computers are able to do so.[3]

HNDL attacks pose a significant risk to a wide range of data, including:

- **Personal Identifiable Information (PII)**
  Sensitive details such as names, addresses, and social security numbers.
- **Financial Records**
  Bank account information, credit card details, and transaction history.
- **Intellectual Property**
  Trade secrets and proprietary algorithms.
- **National Security Secrets**
  Classified information critical to a nation's safety.

Just as importantly, it poses a personal risk to us all. As "good" of people as we may be, it goes without saying that having the contents of our digital lives – for decades – laid bare before the public poses substantial risk to our health and safety.

The potential impact of quantum attacks extends beyond data theft. Quantum computers could:

- **Disrupt Cyber-Controlled Processes:**
  Compromise critical infrastructure systems such as power grids, transportation networks, or communication networks.
- **Manipulate Physical Equipment Remotely:**
  Alter the behavior of machinery, vehicles, or medical devices, leading to catastrophic consequences.

> "Some secrets remain valuable for many years. Even if an adversary can't immediately crack the encryption that protects our secrets, it could still be beneficial to capture encrypted data and hold onto it, in the hopes that a quantum computer will break the encryption down the road. This idea is sometimes expressed as "harvest now, decrypt later" — and it's one of the reasons computers need to start encrypting data with post-quantum techniques as soon as possible."
>
> — National Institute of Standards and Technology (NIST)

2 https://www.microsoft.com/en-us/research/project/post-quantum-tls/
3 https://www.nist.gov/cybersecurity/what-post-quantum-cryptography

The risk of HNDL is not sci-fi fearmongering; it is our impending reality.

Recognizing the risk posed by quantum computers, a few large players are starting to prepare in limited ways. Apple, for instance, now secures iMessage against quantum computer attacks, specifically citing HNDL as a major reason why it does so.[4]

At a minimum, consumers and business partners expect their data to be secure. Implementing quantum-resistant security demonstrates a commitment to robust data protection, enhancing trust.

With the gravity of the issue at hand, the limited response from industry is concerning. Why should sensitive enterprise and government data be vulnerable, while a photo we sent to a friend of a cat is secured in perpetuity?

Xiid SealedTunnel: Zero-Knowledge Networking with Post-Quantum Security

Xiid SealedTunnel secures communication channels and any data in-transit against quantum computer-based attacks through a two-pronged approach:

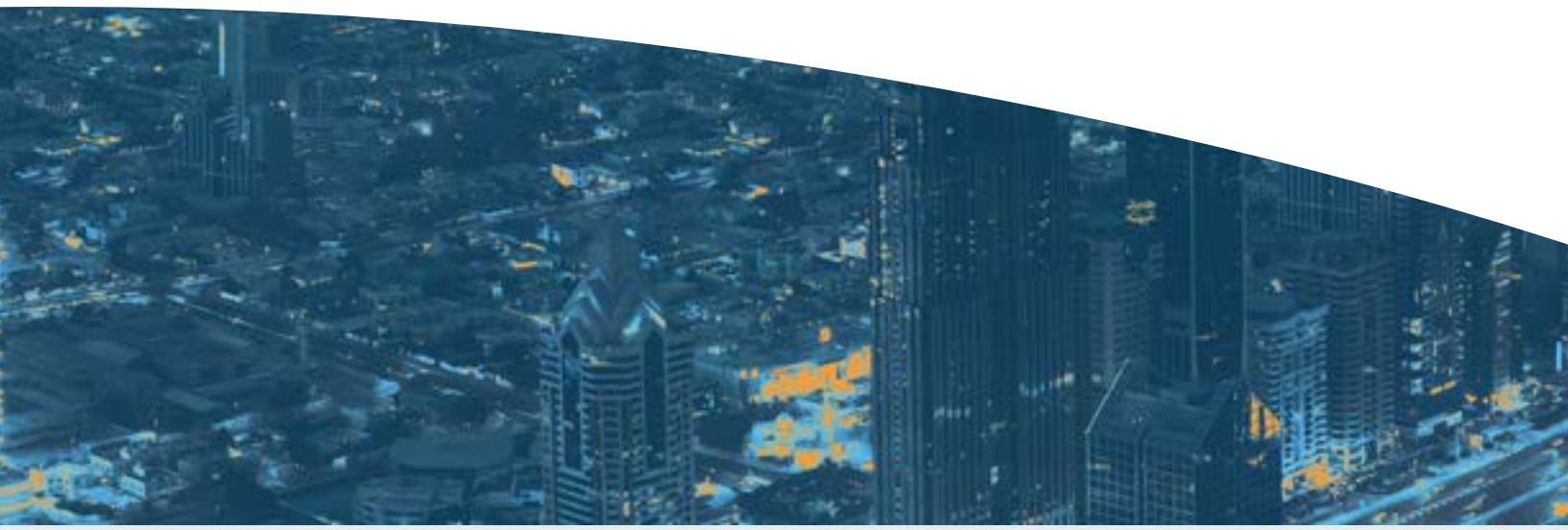
Zero-Knowledge Networking (ZKN)

- **ZKN ensures information exchange without revealing the underlying data.**
- **Inspired by Zero Knowledge Proofs (ZKPs), ZKN provides a secure network overlay for existing communication channels.**
- **Other benefits include confidentiality, privacy preservation, and protection against insider threats.**

Post-Quantum Cryptography

- **Xiid SealedTunnel leverages quantum-resistant algorithms like Kyber and Dilithium.**
- **These algorithms are the gold-standards, as determined by NIST and the broader scientific community, that are mathematically proven to withstand attacks from powerful quantum computers using any of the known quantum crypto-analytic attacks.[5]**
- **An additional security layer using AES-256 GCM mode further strengthens data payload security by performing a rolling authenticated encryption which is also proven unbreakable by any known quantum crypto-analytic attack.**

4 https://security.apple.com/blog/imessage-pq3/
5 https://csrc.nist.gov/projects/post-quantum-cryptography



Kyber and Dilithium: Quantum-Resistant Cryptography

Xiid's solution incorporates Kyber and Dilithium, two lattice-based cryptographic algorithms. These algorithms are designed to resist attacks from quantum computers:

- **Lattice-based cryptography:** These algorithms rely on the inherent hardness of the "inversion problem" over lattices, making them computationally difficult even for quantum computers.
- **Kyber:** A Key Encapsulation Mechanism (KEM) for establishing shared secrets.
- **Dilithium:** A digital signature scheme for verifying the authenticity of data.

The security of these algorithms stems from the complexity of solving certain lattice-specific problems which increases with the size and complexity of the lattices used.

AES-256 GCM: Additional Layer of Security

On the payload layer, Xiid utilizes AES-256 GCM mode, offering both quantum resistance and tamper resistance:

- **AES-256:** With a 256-bit key length, this encryption algorithm is proven to be quantum-resistant. Grover's algorithm, which could theoretically speed up brute-force attacks, still requires an impractically long time to crack AES-256.
- **GCM mode:** Provides authentication alongside encryption, with no known quantum vulnerabilities when the algorithm is used correctly with proper IVs and nonces.

While AES-256 GCM is secure, it still is a symmetric algorithm which requires both parties to use the same key to encrypt and decrypt data, hence the necessity for the continued use of post-quantum key exchange and encapsulation mechanisms as well as quantum-secure digital signatures to ensure long-term security.

Conclusion

While the threat of quantum computers may feel distant, it's the data being sent *right now* that is at risk. Time is of the essence, as the attack on our closely-guarded secrets is happening right now. No industry can afford to wait and risk widespread, reputation-damaging, and potentially catastrophic information disclosure.

Xiid SealedTunnel™ is as a comprehensive solution that can quickly, efficiently, and cost-effectively secure all communication channels in the face of evolving threats. By combining Zero Knowledge Networking with post-quantum cryptography, Xiid bridges the gap between today's vulnerabilities and tomorrow's quantum realities. As HNDL attacks and quantum computing continue to evolve, Xiid SealedTunnel™ reliably safeguards sensitive information – and those cat pictures – today *and* tomorrow.

Recommendations

1. **Adopt Quantum-Resistant Solutions:** Implement post-quantum cryptographic algorithms to safeguard sensitive data.
2. **Continuous Monitoring:** Stay updated on advancements in quantum computing and adjust security measures accordingly.
3. **Educate and Train:** Ensure that all stakeholders understand the importance of quantum security and are trained in the use of new technologies.

By taking these steps, organizations can fortify their defenses against the emerging threats posed by quantum computing and ensure the security of their data well into the future.