Quantum Preparedness: Take Action Now Before the Crypto Sky Falls

Utimaco Applied Crypto Symposium

January 16, 2020

MARK B. COOPER
PRESIDENT & FOUNDER

MARK@PKISOLUTIONS.COM
@THEPKIGUY

PKI SOLUTIONS

The PKI Guy

- President and Founder, PKI Solutions
- Known as “The PKI Guy” since early days at Microsoft
- Leading PKI subject matter expert
- At PKI Solutions, we implement PKI solutions at enterprises
- I lead hundreds of PKI trainings from Scotland to Buffalo, Sweden to Portland
- In-person and online trainings available
- My focus is security, PKI design and implementation, identity management

PKI SOLUTIONS

What Are We Talking About Today?

PKI SOLUTIONS

- The myth
- The impact
- A brief crypto history
- Surviving in a post-quantum world
- Recommendations for enterprises
- Getting a handle on your third parties is critical
- Questions

Myth: The Sky is Falling

- “One day, quantum computers could undermine the widely used encryption technique based on factoring very [prime] large numbers.” - *ScienceNews*

- Myth: Possible disclosure of every identity and encrypted piece of information

- Fact: Quantum computers pose considerable risk to existing public key cryptography, but quantum-proof algorithms will minimize the risk – if we are prepared

The Impact

- Uncertainty
- Quantum supremacy could come at any time
- New cryptographic algorithms will be required
- Slow on the uptake of the new algorithms is not an option
- What are you missing?

The State of Quantum Computing

PKI SOLUTIONS

- Quantum computing won't spell the end to encryption
  - Quantum proof algorithms are already in development
- Enterprises can be in control if they plan ahead and take the right steps
- We are months or years away; change is happening and preparation is key
- Call to action: have a roadmap to address the change

A Brief Crypto History

- RSA – discovered in 1976
  - Grandfather of Asymmetric Algorithms
- Industry Shift from MD5 & SHA1
- NIST currently evaluating 26 quantum-proof algorithms
  - Post-quantum cryptography needs to include standards past 2030
- Similar & Different to Year 2000 Problem (Y2K)

Readying for Quantum Supremacy: Steps

1. Assess environment (current systems, software, appliances):
   - What is using crypto keys?
   - Especially prime number-based crypto: ECC and RSA
2. Determine placement and risk exposure (external gateway vs. internal employee website)
3. Determine which systems have no existing crypto upgrade
   - Contact the manufacturer and discuss timeline and plans
4. Identify potential alternate solutions that provide improved crypto
5. Determine timeline to implement quantum-resistant algorithms
6. Address critical and vulnerable systems (external facing, authentication, critical systems, encrypted financials, etc.)

PKI SOLUTIONS

Engage and Activate Your Third Parties

- Third-party vendors wait-and-see approach
- Enterprise needs vs. cloud provider motivation
- What risks will you face vs. on-premises?
- What kind of encryption are your providers using?
  - Microsoft OneDrive
  - Amazon Sellers, AWS

PKI SOLUTIONS

Key Questions

- Can vulnerable systems that can't be upgraded be augmented with additional controls or must they be replaced?
- Are current systems flexible enough to be easily updated if new algorithms are not sufficiently quantum proof?
- What current practices will need to change?
- Timeline for BYOK and other solutions?
- What is your Quantum Supremacy zero-day timeline
    - How great is that risk?

Surviving in a Post-Quantum World

PKI SOLUTIONS

- Monitor and evaluate diligently
- Be prepared to quickly adopt new algorithms as they emerge
- Work closely with partners, vendors, suppliers to ensure they are following best practices
- Don’t panic

Questions? Let's Connect!

PKI SOLUTIONS

- mark@pkisolutions.com
- @ThePKIGuy
- @PKISolutions
- www.pkisolutions.com
- linkedin.com/in/thepkiguy
- linkedin.com/company/pki-solutions