October 21, 2015

Quantum Resistant Algorithms

Presentation to the ISPAB

Presented by
Mike Boyle
Adrian Stanger

CONFIDENCE IN CYBERSPACE

The CRQC

- Problem: potential future adversarial deployment of “Cryptographically Relevant Quantum Computer”
- Attacks public key algorithms (RSA, DH, DSA, ECDH, ECDSA,…), threatening the confidentiality and authenticity of virtually every electronic communication or transaction (if/when developed).
- Impacts customer planning NOW

Cryptography Yesterday Suite B

	SECRET	TOP SECRET
Public Key Through Oct 2015	RSA 2048 DH 2048 P-256 P-384	P-384
Public Key After Oct 2015	P-256 P-384	P-384
Symmetric	AES 128 AES 256	AES 256
Hash	SHA 256 SHA 384	SHA 384

Cryptography Tomorrow Suite "TBD"

	TOP SECRET
Public Key	TBD Commercial "post quantum" standards
Symmetric	AES 256
Hash	SHA-384

Cryptography Today
Suite "Use What You Have"

	SECRET AND TOP SECRET
Public Key	P-384 RSA/DH 3072+
Symmetric	AES 256
Hash	SHA-384

- Don't force elliptic curve transition (resources)
- Anticipate exceptions
- Use preshared symmetric keys when appropriate

Milestones

- E = Data encrypted
- Q = invention of CRQC
- A = development of quantum resistant algorithms
- I = availability of implemented QRA

Timeline