Securing The Future With Quantum-Safe Cryptography

Scott Totzke, CEO of ISARA Corp.
October 17, 2017
Quantum computing will solve today’s unsolvable problems, opening up

A NEW REALM OF POSSIBILITIES.
THE QUANTUM RACE IS ON
Quantum computing will break today’s public key encryption standards.
### WHAT’S VULNERABLE?

**PRODUCTS**
- VPNs, PKIs, IoT Devices, Vehicles, Apps & CPUs

**PROTOCOLS**
- TLS, IKE, SSH, S/MIME

**CRYPTOSYSTEMS**
- RSA, ECC
A DAY IN LIFE WITHOUT CRYPTOGRAPHY

HOME

VEHICLES

TRANSPORTATION

COMPUTING

ENTERPRISE
PATHWAYS TO QUANTUM SAFETY

Quantum Key Distribution (QKD)
Quantum Random Number Generation (QRNG)
Quantum-Safe Cryptography
SUCCESS IS A
SEAMLESS
(and cost effective)
MIGRATION
...with no impact to end user experience.
SUCCESS REQUIRES
STANDARDS