Human and Technical Factors in the Adoption of Quantum Cryptographic Algorithms

Alyssa Pinkston
Advised by Dr. Joshua Holden

Introduction

The purpose of the research is to understand what factors would cause users to choose quantum key distribution (QKD) over other methods of cryptography.

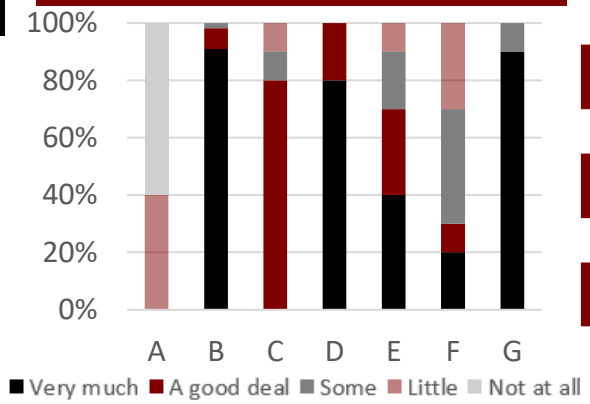
Background

- An AES key can be exchanged through communication using RSA, QKD, or post-quantum cryptography (PQC)
- QKD relies on quantum physics, AES and PQC use complex mathematics
- BB84 Quantum Cryptographic Protocol involves communication over a quantum channel and a public channel
- Technical attacks include beamsplitting and intercept/resend
- Other attacks might be industrial espionage or person-in-the-middle
- QKD products can transmit over maximum distances ranging from 40-150 km with key rates as low as 1.4 kb/s up to over 150 kb/s.

Survey Results

The company makes security a top priority, and thinks protection is the most important factor in security decisions. No survey participant fully trusts current security systems.

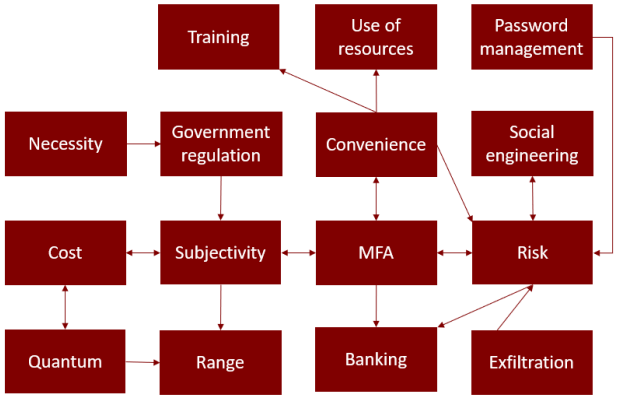
Security Risk and Trust



A: familiarity with quantum cryptography
B: individual values protecting data
C: individual trusts current systems
D: company values security
E: importance of convenience
F: importance of cost
G: importance of protection

Research Results

The focus group discussion centered around threat model, subjectivity of tradeoffs, convenience, and MFA. Range proved to be a critical factor.



Conclusion

Incentives for adoption of QKD would be due to regulation and necessity, but currently adoption is viewed as more inconvenient than the security is worth.

ROSE-HULMAN