Multiprotocol Analysis of Quantum Versus Classic Encryption Methods for Medical Imaging

Young-Tak Kim, PhD, Research Fellow, Radiology, Massachusetts General Hospital
Synho Do, MS, PhD; John Mayfield, MD, PhD, MSc

Background/Problem Being Solved

Given the sensitive nature of information within DICOM images and metadata, encryption is typically the initial step. Up until the recent technological era, AES/RSA have been highly resilient to traditional attacks. However, as quantum computing technologies have grown exponentially in the last few years, there is a growing concern that quantum computation methods such as Grover's Algorithm can reduce the time to brute-force calculation of RSA/AES encrypted data to the square root of the traditional computation time.

Intervention(s)

We propose a series of quantum key distribution (QKD) methods for encryption of DICOM based upon the unique tenets of quantum mechanics including the Heisenberg Uncertainty Principle (BB84, SARG04, E91, Measurement Device Independent and Twin Field Paradox protocols) and Phase Coherence Principle (Differential Phase Shift and Reference Frame Independent protocols). Additionally, we approached the problem from an adversarial point of view with exploration of evolving quantum hacking techniques including injection locking, power analysis, temporal ghost imaging, and wavelength control.

Barriers/Challenges

There are several limitations of the study including the simulated environment where generalizations were made in quantum implementation using a quantum hardware simulator, as well as the simulated photon within an optic fiber which may inherently be more prone to noise and signal loss over extended distances versus in open field implementations. Additionally, adversarial attacks were in a simulated environment and may not incorporate additional barriers such as air gaps, active firewalls, and AI countermeasures.

Outcome

In the experiments with QKD, there was 100% eavesdropping detection as any measurement of the quantum systems results in collapsing of the state into an expected value or observable. While RSA had a lower MITM success percentage, none of these attacks were detected. The potential trade-off is the longer key generation time of the QKD protocols. From the adversarial standpoint, injection locking demonstrated the greatest success rate in intercepting quantum keys without disrupting the QKD process, while power analysis exploited power consumption patterns to identify secret keys.

Conclusion/Statement of Impact/Lessons Learned

This pilot study is meant to start the conversation of future-proofing medical imaging given its inherent vulnerabilities with robust eavesdropping detection which may be of great utility in scenarios such as the recent CrowdStrike event. Implementing both the offensive and defensive strategies helped to identify potential vulnerabilities and opportunities for quantum cryptography across the medical imaging environment. Specific to the operational engineering aspect, the potential utility of these protocols could be readily implemented given the existing architecture of optic cables.

Keywords

Administration & Operations; Applications; Emerging Technologies; Enterprise Imaging; Imaging Research; Quality Improvement & Quality Assurance; Standards & Interoperability; Security; Systems Management