Team Members: Brian Maher, bmaher2@gmu.edu

Project Title: Quantum Cryptography Implementation Vulnerabilities

Introduction and Motivation:

Quantum cryptography provides a secure, tamper-proof means to distribute keys through Quantum Key Distribution (QKD). While the physics behind QKD are sound, the implementation details may not have been closely examined for vulnerabilities. This paper will look to aggregate a listing of known issues with quantum cryptography as well as attempt to identify new issues that could occur due to errors in implementation.

Detailed Description of Problem Being Investigated:

There will be four specific areas of focus on the vulnerabilities in quantum cryptography implementations. First, the specific hardware needed to set up two systems to use quantum cryptography will be analyzed for ways that it could be exploited by an attacker that has access to it. Secondly, the software needed to utilize that hardware will be examined for vulnerabilities that may be used to compromise messages. Third, communication protocol between the two stations as well as between the station and the computer will be analyzed for vulnerabilities. Finally, while the algorithms have likely been vetted, they will be looked at to ensure that a secure standard is used.

Tentative List of Questions That I Am Seeking an Answer To:

- How does quantum cryptography work?
- How does QKD work?
- How is the information exchanged during the QKD protocols authenticated?
- How can a QKD system be protected against a man in the middle attacks?
- What implementation details are required to be the same in systems that implement quantum cryptography?
- What protocols and algorithms are used within quantum cryptography systems?
- What implementation details, specific to quantum cryptography, need to be paid attention to in implementations?
- How can quantum cryptography implementations be compromised by an attacker?
- What are some errors, not specific to quantum cryptography, which could be made in a system that utilizes quantum cryptography?

Hypotheses I am Planning to Investigate:

While the point to point quantum mechanisms will be secure, the surrounding architecture in a quantum cryptography implementation will have many issues leading to it being no more secure than non-quantum cryptography.

Time Schedule:

October 26/27 – Finish research into quantum cryptography. At this stage, specific implementations to be looked at should be identified and a basic understanding of quantum cryptography should be held.

Quantum Cryptography Brian Maher
Implementation Vulnerabilities

November 9/10 – Finish analysis into issues with quantum cryptography. Specific concerns that have been identified by other researchers should be known.

November 23/24 – Initial rough draft.

December 7/8 – Final draft of paper, rough draft of presentation

List of Areas where Specification May Change:

If specific implementation details cannot be found, then the discussion will have to be tailored more towards theoretical implementations.

Tentative Table of Contents:

1. Introduction
2. Quantum Cryptography Mechanics
3. Possible Algorithm Vulnerabilities
4. Possible Software Vulnerabilities
5. Possible Hardware Vulnerabilities
6. Possible Communication Vulnerabilities
7. Conclusion

Possible Implementations to Analyze

- QBox by MagiQ Technologies, Inc. (United States)
- Cerberis QKD by ID Quantique (Switzerland)
- qOptica by QuintessenceLabs (Australia)

Previous Studies

V. Scarani and C. Kurtsiefer [9] describe a number of hardware issues that may arise in QKD. The hardware portion of my paper must necessarily rely on previous studies such as this as I do not have the physics education to assess the hardware limitations of QKD. However, their paper does not further delve into Algorithm or Software vulnerabilities that may be present in QKD implementations.

List of Literature:

[1] D. Mayers, "Unconditional security in quantum cryptography," *Journal of the ACM*, vol. 48, no. 3, pp 351-406, May 2001.

[2] D. Bruss et. al., "Quantum cryptography: a survey," *ACM Computing Surveys*, vol. 39, no. 2, 2007.

[3] C. Elliott, D. Pearson, and G. Troxel, "Quantum cryptography in practice," in *Proceedings of the 2003 conference on applications, technologies, architectures, and protocols for computer communications*, 2003, pp. 227-238.

[4] M. Javed, K. Aziz, "A survey of quantum key distribution protocols," in *Proceedings of the 7th International Conference on Frontiers of Information Technology*, 2009, article 39.

[5] Y. Zhang et. al., "Quantum secret sharing of key in networks," in 2011 *Symposium on Photonics and Optoelectronics*. 16-18 May 2011, pp. 1-3.

[6] Z. L. Yuan, A. J. Shields, "Practical one-way quantum cryptographic system for telecom networks," in *2006 Digest of the LEOS Summer Topical Meetings,* 2006, pp. 26-27.

[7] G. Mone, "Future-proof encryption," *Communications of the ACM*, vol. 56, no. 11, pp. 12-14, Nov. 2013.

[8] K. Kishore et. al., "Quantum key distribution and testing," *International Journal of Advanced Research in Computer Science,* vol 2, no. 6, pp. 156-165, Nov./Dec. 2011.

[9] V. Scarani and C. Kurtsiefer, "The black paper of quantum cryptography: real implementation problems," *Theoretical Computer Science*, vol. 560, no. 1, pp. 27-32, Dec. 2014.

[10] A. K. Ekert, "Quantum Cryptography based on Bell's theorem," *Physical Review Letters*, vol. 67, no. 6, pp. 661-663, Aug. 1991.

[11] Q-Box Workbench Uncompromising QKD Research, [Online], http://www.magiqtech.com/Products_files/QBox%20Datasheet-2011.pdf (Accessed: 14 October 2015).

[12] Cerberis QKD Blade, [Online], http://www.idquantique.com/quantum-safe-crypto/qkd-blade-server/ (Accessed: 14 October 2015).

[13] Advabnced Cyber-Security Solutions, [Online], http://www.quintessencelabs.com/wp-content/uploads/2015/04/20150409_QLabs_company_brochure_final.pdf, (Accessed: 14 October 2015).

[14] A. Lance and J. Leiseboer. (2014, Dec. 1). What is Quantum Key Distribution (QKD)? [Online]. Available: http://www.quintessencelabs.com/wp-content/uploads/2014/11/QL-White-Paper-What-is-Quantum-Key-Distribution.pdf

[15] A. Lance and J. Leiseboer. (2014, Dec. 1). Quantum Key Distribution Systems Compared. [Online]. Available: http://www.quintessencelabs.com/wp-content/uploads/2014/11/QL-White-Paper-QKD-Systems-Compared.pdf