IJCSN - International Journal of Computer Science and Network, Volume 9, Issue 4, August 2020
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Anti-Forensics of Data in Classical and Quantum Systems Over the Classical Communication Channels

[1] Divya Shree S; [2] Anjan K Koundinya; [3] Bharathi R

[1] Department of Computer Science and Engineering, BMS Institute of Technology and Management
Bangalore, Karnataka, 560064, India

[2, 3] Department of Computer Science and Engineering, BMS Institute of Technology and Management
Bangalore, Karnataka, 560064, India

Abstract – In this work, anti-forensics of data in classical and quantum computers over the classical communication channel, storage devices are discussed. The general methodology to apply anti – forensics in storage media without using expensive tools and with low risk of detection on both classical and quantum computers are compared.

Keywords – *Encryption, Contraception, Slack space, Qubit, Superposition*

1. Introduction

Anti-forensics is the application of scientific method applied to the digital media which try to negatively influence the existence of evidence in a crime scene. It makes the examination and analysis difficult/impossible to conduct.[1][2]

There are 4 categories of anti-forensics [1][2]

- Data destruction: deleting particular/entire file systems. Many softwares/techniques are available for this activity.
- Data hiding: The process of downloading and using data is very difficult.
- Data encryption: Publicly available encrypted programs allow the user to create an encrypted virtual disk that can be opened with only one key. Due to modern encryption algorithms and other encryption techniques, it is impossible to read data without a specific key.
- Data contraception: This is an attempt to limit the quality and quantity of forensic evidence to legal or useful data on the disk.

2. In Classical Systems

In this paper, an overview of how a communication channel can be abused for unintended purposes is discussed. Its purpose is to inform forensics about the existence of channels for judicial investigation. The basic idea is to access the hard drive through the diagnostic interface to hide the data. This data is not accessible to the investigator. The actual size is to be manipulated in the firmware setting [3]. This can be done without any expensive tool. So, the forensic investigator must mention alternative applications of communication channels to protect them.

2.1 Methodology

The communications link which is intended for a different purpose is used to access the storage device using an interface for example a maintenance. The hidden partitions of a hard disk drive can be used to do this activity of hiding files. Replace the target user area that is stored in the firmware configuration. When using the firmware data field, the disk capacity decreases. No data can be accessed until the original settings are restored. Only some technical skills and time are required and cost involved is minimal. All these malicious activities are done using the diagnostics interface. [3]

Apart from the communication channels, devices such as camera, USB, system slack space and smart devices such as iOS which now forms a part of the general computing devices can negatively affect the existence of the digital evidence [7][8].

The unusable storage which lies between the last byte of one file in a particular file cluster and the first byte of another file from another cluster is known as slack space. The drawbacks of the slack space is used for the information hiding technique. The 3 major drawbacks are

- When the cover file increases in size, the hidden data is lost
- Due to disk fragmentation, the hidden data is lost.
- Limited amount of data can be hidden because of availability of space.

3. In Quantum Systems

When a case of classical communication is considered in a quantum system, the following conditions are encountered. Some brief introduction of quantum system is discussed.

The system considered is a quantum computer which is different from a classical computer. Instead of bits, the quantum computers have the states called qubits (quantum bits). It is denoted by Dirac notations |0> and |1>.[4][5][6]

The difference between bits and qubits are that qubits can be in states other than |0> and |1> which is termed as entanglement state. Superposition state of a qubit is a linear combination of state

$$|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle \quad (1)$$

where α and β are complex numbers.

BB84 protocol proposed by Bennett and Brassard is the first quantum cryptography. The principles used in BB84 are [4][5]

- No cloning theorem: Quantum states cannot be reproduced. As a result, the communication channel cannot be blocked and quantum states cannot be copied.
- The quantum state cannot be measured. The measurement leads to random bits being generated and the actual data cannot be accessed.
- The quantum state measurements are irreversible.

Because of these principles, the categories of anti - forensics such as data hiding, data encryption, data contraception are encountered in quantum systems over a classical communication channel.

To understand the quantum state measurement and the irreversibility of the measurements, the following use case is discussed in this work.

If the original state of the quantum system is

$$|+\rangle=|0\rangle+|1\rangle/\sqrt{2} \quad (2)$$

When measurements are made on the basis of accumulation {0>, |1>}, the initial state of the system is lost. If the measurement result is 0, a calculation is made based on |±> and the situation is radically different.

When logical 0 is represented by |0>, |+> and logical 1 is represented by |1>, |->. When one person sends the random sequence of bits to the other person over the communication channel, the other individual measures each bit by randomly selecting the {|0>,|1>} basis or on |±> basis at each position.

As a result of this communication, construct the segments n {|0>,|1>} created and creates |±> based n bits. When two people compare notes, they only discover which ones are used just in case. As a result, most of the valuable data is destroyed.

As a result of this communication, n of the bits are created in {|0>,|1>} basis and n bits are created in the |±> basis. When both individuals compare the notes, revealing only to each other which basis was used at each position. If both have used different basis they discard the qubit. So, most of the valid data is destroyed.

Another use case is discussed here is about the quantum information hiding protocol which is about hiding the data in multimedia images, audio and video using the protocols of quantum image processing and RSA algorithms. The data to be hidden is encrypted using a CNOT(Controlled NOT Gate). The data can be acquired easily without proper key for forensic purpose [9].

4. Conclusion

This document develops a common methodology for applying anti – forensics to storage media using a communication channel without an expensive set of tools and low risk of detection in classic computer systems. On the other hand, a light is shed on the risk of anti – forensics on the quantum system in a totally different computing paradigm.

References

[1] Nina Godbole, Sunit Belapure,"Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives", Wiley India Pvt Ltd, ISBN: 978-81-265-21791, Publish Date 2013

[2] Wikipedia link "https://en.wikipedia.org/wiki/Anti-computer forensics"

[3] H. Baier and J. Knauer, "AFAUC -- Anti-forensics of Storage Devices by Alternative Use of Communication Channels," 2014 Eighth International Conference on IT

Security Incident Management & IT Forensics, Munster, 2014, pp. 14-26

[4] Michael A. Nielsen, Isaac L. Chaung, “Quantum Computation and Quantum Information”, Cambridge University Press

[5] David McMahon, “Quantum Computing Explained”, WILEY- INTERSCIENCEA John Wiley & Sons, Inc., Publication

[6] D. P. DiVincenzo, D. W. Leung and B. M. Terhal, "Quantum data hiding," in IEEE Transactions on Information Theory, vol. 48, no. 3, pp. 580-598, March 2002.

[7] A. Srinivasan, S. T. Nazaraj and A. Stavrou, "HIDEINSIDE — A novel randomized & encrypted antiforensic information hiding," 2013 International Conference on Computing, Networking and Communications (ICNC), San Diego, CA, 2013, pp. 626-631, doi: 10.1109/ICCNC.2013.6504159

[8] C. DOrazio, A. Ariffin and K. R. Choo, "iOS Anti-forensics: How Can We Securely Conceal, Delete and Insert Data?," 2014 47th Hawaii International Conference on System Sciences, Waikoloa, HI, 2014, pp. 4838-4847, doi: 10.1109/HICSS.2014.594.

[9] A. A. Abd El-Latif, B. Abd-El-Atty, M. S. Hossain, M. A. Rahman, A. Alamri and B. B. Gupta, "Efficient Quantum Information Hiding for Remote Medical Image Sharing," in IEEE Access, vol. 6, pp. 21075-21083, 2018, doi: 10.1109/ACCESS.2018.2820603.

Authors -

Divya Shree S, member IEEE is currently pursuing Masters degree in Computer Science and Engineering in BMS Institute of Technology and Management. She has 4 years of work experience as a software test engineer. Currently she has a publicatiuon in SPIE Conference. Research interests include but not limited to Complex modeling, Quantum Computing

Dr. Anjan Koundinya K, senior IEEE member is B.E, MTech and PhD in Computer Science and Engineering. He has been awarded Best Performer PG 2010, First Rank Holder (M. Tech CSE 2010) and recipient of Best Doctoral Thesis Award by BITES, Karnataka for the academic year 2016-17. He has served in industry and academia in various capacities for more than a decade. He is currently working as Associate Professor in Dept. of Computer Science and Engineering, BMS Institute of Technology and Management, Bengaluru.