QATT&CK: Threat-Intelligence For Understanding the Hybridization of Utility-Scale Quantum Computers Based on ATT&CK

Justin Woodring, Aisha Ali-Gombe
Louisiana State University

ABSTRACT

The integration of quantum computing into governmental and business processes has raised concerns about potential threats to these systems. To address this, we introduce a novel extension of the MITRE ATT&CK framework, QATT&CK, which provides a extended taxonomy for classifying adversarial behavior in quantum cybersecurity. Our adapted framework bridges the definitions of traditional cybersecurity with an focus on quantum computing infrastructure, enabling a more comprehensive understanding of adversarial behavior in this domain.

KEYWORDS

QATT&CK, MITRE, ATT&CK, quantum computing, cybersecurity, taxonomy

1 INTRODUCTION

First conceptualized in the late 1980s by Deutsch, quantum computing promises to revolutionize traditional computing processes for advanced fields such as materials sciences, pharmaceuticals development, machine learning, and cryptography [1, 5, 9]. Having captured the attention and focus of researchers, corporations, and nation-states alike its only natural to assert that these quantum computers will become targets of adversarial behavior as well.

A significant amount of literature has already attempted to understand, how quantum computers may be used to break our traditional computing infrastructures, Shor's efficient prime factorization algorithm which served as a catalyst to prove the potential of quantum computing was based on this very notion [5, 9]. However, as organizations begin to hybridize their classical infrastructure with quantum processes we must also consider the protection of these quantum computational assets themselves, and development of new kinds of threats targeting quantum infrastructure.

In light of this, it becomes essential to effectively classify adversarial behaviors in order to empower organizations to identify and respond to threats relating to the quantum paradigm. The MITRE ATT&CK framework is well-established in the traditional cybersecurity landscape and is essential for security professionals and researchers looking to provide guidance to corporations and governments. [6, 10] Therefore we propose to extend MITRE's ATT&CK, in order to capture the significant changes affected by the quantum-classical hybridization. We introduce this novel extension as QATT&CK, or Quantum Adversial Techniques, Tactics, and Common Knowledge.

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

2 BACKGROUND AND RELATED WORK

2.1 The MITRE ATT&CK Framework

The MITRE ATT&CK framework is a cornerstone of enterprise cybersecurity awareness, providing a comprehensive foundation for understanding the Tactics and Techniques used by adversaries in real-world attacks. This globally-accessible knowledge base is built on observations from actual cyber-attacks, offering a unique perspective on the evolving threat landscape [7].

By organizing these Tactics and Techniques into a structured taxonomy, the ATT&CK framework enables cybersecurity researchers and professionals to classify offensive and defensive strategies with ease. This framework serves as a valuable resource for threat intelligence, empowering security experts to assess potential threats and stay one step ahead of attackers [6].

In essence, the MITRE ATT&CK framework is an essential tool for anyone working in cybersecurity, providing a common language and framework for understanding and addressing the ever-changing nature of cyber threats [6, 10].

2.2 An Overview of Quantum Architectures

Quantum computing relies on the principles of quantum mechanics to perform computations using qubits instead of classical bits. Qubits can exist in a superposition of states, which if used correctly with particular quantum algorithms allows for an exponential speedup in solving certain types of problems. Several architectures have been proposed for building large-scale quantum computers, each with its unique advantages and challenges. However each of them follows a relatively consistent pattern we refer the reader to Figure 2). Specific implementations of quantum computing architectures include: superconducting, ion trap, photonic, neutral atom, and quantum annealing based architectures [3].

2.3 Sample Attack Landscape

The introduction of quantum technology into hybridized infrastructure has enabled a set of unique new forms of attacks, for example the measurement attack. In this kind of attack, an attacker executes a quantum circuit that immediately measures the results of the previous circuit. Generally speaking this relies on an insecure reset operation being utilized on a quantum system [4]. However, if this

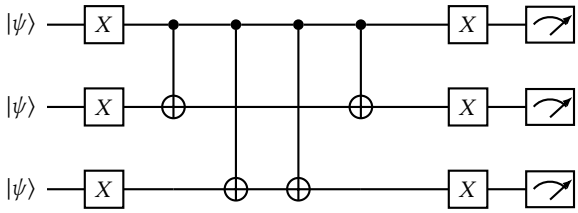

Figure 1: A quantum circuit that looks as though it is performing some computation but actually does nothing and then measures the states with which the circuit began running, circuits like these can be used in measurement attacks to evade detection.

is the case the an attacker can perform the attack by injecting malicious code into the job queue or manipulating the classical frontend interface to execute a specific sequence of circuits [4].

Typically this attack is perpetrated in the following steps:

- Previous circuit execution: A legitimate user submits a job to the quantum computer, which performs a computation and returns a measurement result.
- Attacker's circuit injection: The attacker injects a malicious circuit into the job queue or manipulates the classical frontend interface to execute a specific sequence of circuits.
- Immediate measurement: The attacker's circuit immediately measures the results of the previous circuit, potentially compromising sensitive information such as cryptographic keys.

These attacks may even be disguised [11] as circuits that don't actually do anything. For example refer to Figure 1, a quantum circuit that looks as though it is performing some computation but actually does nothing. After performing no actual computation, measurement would reproduce results that duplicate the results of the previously executed circuit before decoherence occurs.

Other common kinds of attacks may include those such as trojans [2], shuttle-exploiting attacks [8], malware [12], and sidechannel attacks [13].

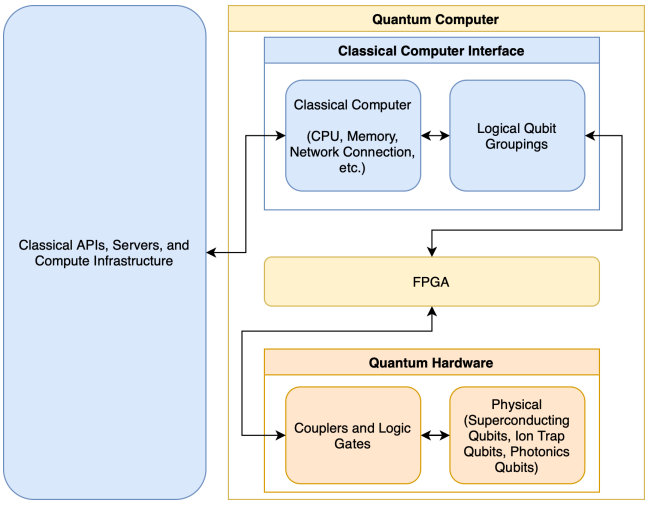

Figure 2: A generalized model of quantum computing architectures that captures that classical and quantum components.

Table 1: Quantum Techniques for Adversarial Tactics

Tactic	Quantum Technique
Reconnaissance	T1599 Gather Victim Host Information (Quantum Topology and Error Fingerprinting) T2003 Attack Quantum Side Channels (Quantum Side Channel Monitoring)
Resource Development	T1504 Compromise Infrastructure (Compromise and Leverage Quantum Machines)
Initial Access	T1659 Content Injection (Measurement Manipulation)
Execution	T1651 Cloud Administration Command (Dashboard Based Quantum Job Queuing) T1059 Command and Scripting Interpreter (Script Based Job Submission and Execution)
Persistence	T1554 Compromise Host Software Binary (Transpiler Augmentation, Queuing and Job Manager Augmentation) T2002 Post Circuit Measurement (Replicate Job Results)
Privilege Escalation	No additions
Defense Evasion	T2001 Alter Quantum Calibration Processes (Alter Quantum Calibration Processes) T1042 Process Injection (Altered Quantum Circuit Submission)
Credential Access	T2002 Post Circuit Measurement (Replicate Job Results) T1557 Adversary-in-the-Middle (Quantum Job Sniffing)
Discovery	No additions
Lateral Movement	No additions
Collection	T2002 Post Circuit Measurement (Replicate Job Results) T1554 Compromise Host Software Binary (Queuing and Job Manager Augmentation) T1557 Adversary-in-the-Middle (Quantum Job Sniffing)
Command & Control	T1659 Content Injection (Measurement Manipulation) T1071 Application Layer Protocol (Commands through Quantum Circuity Job Queue)
Exfiltration	T1567 Exfiltration Over Web Service (Exfiltration through Quantum Circuit Job Queue)
Impact	T1554 Compromise Host Software Binary (Queuing and Job Manager Augmentation) T2003 Attack Quantum Side Channels (Quantum Side Channel Impact) T1565 Data Manipulation (Measurement Manipulation) T1486 Data Encrypted for Impact (Measurement Encryption) Intentional Qubit Degradation (Adversarial Job Submission)

3 METHODOLOGY/DESIGN

This section delves into the extensions and contributions that QATT&CK brings to the ATT&CK framework. QATT&CK is organized into several subsections, each focusing on a specific tactic in the MITRE ATT&CK framework: Reconnaissance, Resource Development, Initial Access, Execution, Persistence, Defense Evasion, Credential Access, Command & Control, Exfiltration, and Impact.

A concise overview of the extended techniques can be found in Table 1, which demonstrates a relationship with existing ATT&CK Tactics. Notably, sub-techniques have been expanded from existing techniques where relevant, while a few independent techniques have also been introduced. Our Technique contributions are clearly denoted by numbering T2001 and above.

The rationale behind this methodology is based on the understanding that quantum computers will bring new challenges to cybersecurity. For instance, quantum computers can process certain forms of information more efficiently, making it easier for an attacker to gather large amounts of data or perform complex calculations. Additionally, quantum computers have unique side channels and qubit decoherence properties that can be exploited by attackers.

Overall, QATT&CK covers the quantum-enhanced ATT&CK tactics such as:

- Quantum Reconnaissance: Gathering information about a victim's quantum machine, including its topology, error rate, and supported basis gates.
- Quantum Resource Development: Compromising third-party quantum machines to leverage their computational abilities for an attacker's goals.
- Quantum Initial Access: Injecting malicious code or commands into a quantum system through measurement manipulation or quantum circuit job queues.

- Quantum Execution: Running malicious jobs on a quantum computer using dashboard-based quantum job queuing or script-based job submission and execution.
- Quantum Persistence: Maintaining access to a quantum system by altering transpiler code, job queuing software, or calibration processes.
- Quantum Defense Evasion: Avoiding detection by security controls through altered quantum calibration processes or injected quantum circuits.
- Quantum Credential Access: Obtaining sensitive information, such as passwords or encryption keys, through replicated job results, captured data being sent between the quantum computer and a remote job submission, or sniffed quantum jobs.
- Quantum Command & Control: Remotely controlling or commanding a system or network using measurement manipulation or quantum circuit job queues.
- Quantum Exfiltration: Transferring sensitive information from a system or network through quantum circuit job queues.
- Quantum Impact: Causing significant damage or disruption to a system or network by altering quantum calibration processes, attacking quantum side channels, manipulating data, encrypting measurements for ransom, or degrading qubit quality.

This methodology is designed to provide a comprehensive understanding of the potential quantum threats and tactics related to cybersecurity. It serves as a foundation for organizations and individuals to begin preparing for the future security challenges posed by this emerging technology.

4 FUTURE WORK

As quantum computing infrastructure continues to evolve, it is crucial that we continue to adapt and refine our frameworks for classifying adversarial behavior. Potential future work may consist of:

- Incorporating more relevant research: We plan to expand the scope of our framework to include additional tactics and techniques relevant to quantum computing.
- Refining Techniques: We aim to refine our Techniques and Sub-techniques so as to effectively capture changes in adversarial behavior as the quantum cybersecurity landscape changes with time.
- Documenting mitigations: We will work on cataloging effective countermeasures to mitigate threats related to quantum computing, including transpiler and compiler augmentation, quantum side channel attacks, and other Techniques.

By continuing to advance our understanding of adversarial behavior in the quantum paradigm, we can better equip organizations and governments with the tools they need to protect against future threats.

5 CONCLUSION

In this paper, we have introduced QATT&CK, a novel extension of the MITRE ATT&CK framework, for classifying adversarial behavior targeting quantum systems. Our adapted framework bridges the rigorous definitions of traditional cybersecurity with an adapted focus on quantum computing infrastructure, enabling a more comprehensive understanding of adversarial behavior in this domain.

The significance of our work lies in its ability to provide valuable insight to organizations and governments seeking to identify and respond to future threats related to quantum computing. By extending the existing definitions of Tactics and introducing new Techniques pertinent to quantum computers, we have demonstrated the effectiveness of our extended framework in understanding and classifying current and ongoing cybersecurity research in the field of quantum computing.

REFERENCES

[1] Andreas Bayerstadler, Guillaume Becquin, Julia Binder, Thierry Botter, Hans Ehm, Thomas Ehmer, Marvin Erdmann, Norbert Gaus, Philipp Harbach, Maximilian Hess, Johannes Klepsch, Martin Leib, Sebastian Luber, Andre Luckow, Maximilian Mansky, Wolfgang Mauerer, Florian Neukart, Christoph Niedermeier, Lilly Palackal, Ruben Pfeiffer, Carsten Polenz, Johanna Sepulveda, Tammo Sievers, Brian Standen, Michael Streif, Thomas Strohm, Clemens Utschig-Utschig, Daniel Volz, Horst Weiss, Fabian Winter, Quantum Technology, and Application Consortium QUTAC. 2021. Industry quantum computing applications. *EPJ Quantum Technology* 8, 1 (2021), 25. https://doi.org/10.1140/epjqt/s40507-021-00114-x

[2] Subrata Das and Swaroop Ghosh. 2024. Trojan Attacks on Variational Quantum Circuits and Countermeasures. In *2024 25th International Symposium on Quality Electronic Design (ISQED)*. 1–8. https://doi.org/10.1109/ISQED60706.2024.10528776

[3] Saumya Jain. 2015. Quantum computer architectures: A survey. In *2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom)*. 2165–2169.

[4] Allen Mi, Shuwen Deng, and Jakub Szefer. 2022. Securing Reset Operations in NISQ Quantum Computers. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22)*. Association for Computing Machinery, New York, NY, USA, 2279–2293. https://doi.org/10.1145/3548606.3559380

[5] John Proos and Christof Zalka. 2004. Shor's discrete logarithm quantum algorithm for elliptic curves. (2004). arXiv:quant-ph/quant-ph/0301141 https://arxiv.org/abs/quant-ph/0301141

[6] P Rajesh, Mansoor Alam, Mansour Tahernezhadi, A Monika, and Gm Chanakya. 2022. Analysis Of Cyber Threat Detection And Emulation Using MITRE Attack Framework. In *2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA)*. 4–12. https://doi.org/10.1109/IDSTA55301.2022.9923170

[7] P Rajesh, Mansoor Alam, Mansour Tahernezhadi, A Monika, and Gm Chanakya. 2022. Analysis of cyber threat detection and emulation using mitre attack framework. In *2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA)*. IEEE, 4–12.

[8] Abdullah Ash Saki, Rasit Onur Topaloglu, and Swaroop Ghosh. 2022. Shuttle-Exploiting Attacks and Their Defenses in Trapped-Ion Quantum Computers. *IEEE Access* 10 (2022), 2686–2699. https://doi.org/10.1109/ACCESS.2021.3139085

[9] Peter W. Shor. 1997. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* 26, 5 (Oct. 1997), 1484–1509. https://doi.org/10.1137/s0097539795293172

[10] Blake E Strom, Andy Applebaum, Doug P Miller, Kathryn C Nickels, Adam G Pennington, and Cody B Thomas. 2018. Mitre att&ck: Design and philosophy. In *Technical report*. The MITRE Corporation.

[11] Aakarshitha Suresh, Abdullah Ash Saki, Mahababul Alam, Rasit Onur Topaloglu, and Swaroop Ghosh. 2022. Short Paper: A Quantum Circuit Obfuscation Methodology for Security and Privacy. In *Proceedings of the 10th International Workshop on Hardware and Architectural Support for Security and Privacy (HASP '21)*. Association for Computing Machinery, New York, NY, USA, Article 6, 5 pages. https://doi.org/10.1145/3505253.3505260

[12] Siyi Wang, Alex Jin, Suman Deb, Tarun Dutta, Manas Mukherjee, and Anupam Chattopadhyay. 2024. POSTER: MalaQ - A Malware Against Quantum Computer. In *Proceedings of the 19th ACM Asia Conference on Computer and Communications Security (ASIA CCS '24)*. Association for Computing Machinery, New York, NY, USA, 1946–1948. https://doi.org/10.1145/3634737.3659432

[13] Chuanqi Xu, Ferhat Erata, and Jakub Szefer. 2023. Exploration of Power Side-Channel Vulnerabilities in Quantum Computer Controllers. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23)*. Association for Computing Machinery, New York, NY, USA, 579–593. https://doi.org/10.1145/3576915.3623118