Quantum Computing Threat Modelling on a Generic CPS Setup

Lee, C. C., Tan, T. G., Sharma, V., & Zhou, J. (in press). *Quantum Computing Threat Modelling on a Generic CPS Setup*. Paper presented at Third International Workshop on Artificial Intelligence and Industrial Internet-of-Things Security, Kamakura, Japan.

Document Version:
Publisher's PDF, also known as Version of record

Queen's University Belfast - Research Portal:
Link to publication record in Queen's University Belfast Research Portal

Publisher rights
Copyright 2021 the Author(s).
This work is made available online in accordance with the publisher's policies. Please refer to any applicable terms of use of the publisher

General rights
Copyright for the publications made accessible via the Queen's University Belfast Research Portal is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The Research Portal is Queen's institutional repository that provides access to Queen's research output. Every effort has been made to ensure that content in the Research Portal does not infringe any person's rights, or applicable UK laws. If you discover content in the Research Portal that you believe breaches copyright or violates any law, please contact openaccess@qub.ac.uk.

Open Access
This research has been made openly available by Queen's academics and its Open Research team. We would love to hear how access to this research benefits you. – Share your feedback with us: http://go.qub.ac.uk/oa-feedback

Download date:19. Apr. 2024

Quantum Computing Threat Modelling on a Generic CPS Setup

Cher Chye Lee[1] Teik Guan Tan[1], Vishal Sharma[2], and Jianying Zhou[1]

[1] Singapore University of Technology and Design, Singapore
[2] Queen's University Belfast, NI, United Kingdom

Abstract. The threat of quantum computers is real and will require significant resources and time for classical systems and applications to prepare for the remedies against the threat. At the algorithm-level, the two most popular public-key cryptosystems, RSA and ECC, are vulnerable to quantum cryptanalysis using Shor's algorithm, while symmetric key and hash-based cryptosystems are weakened by Grover's algorithm. Less is understood at the implementation layer, where businesses, operations, and other considerations such as time, resources, know-how, and costs can affect the speed, safety, and availability of the applications under threat.
We carry out a landscape study of 20 better-known threat modelling methods and identify PASTA, when complemented with Attack Trees and STRIDE, as the most appropriate method to be used for evaluating quantum computing threats on existing systems. We then perform a PASTA threat modelling exercise on a generic Cyber-Physical System (CPS) to demonstrate its efficacy and report our findings. We also include mitigation strategies identified during the threat modelling exercise for CPS owners to adopt.

Keywords: Quantum Computing · Threat Modelling · Post-Quantum Cryptography · Cyber-Physical Systems

1 Introduction

Breakthroughs in quantum computing (QC) where the computational power of quantum computers exceed all possible classical computer systems are happening more regularly. In 2019, a team at Google demonstrated quantum supremacy by checking the validity of random samples [5] on their superconducting-based Sycamore 53-qubit quantum chip. More recently in 2020, a team in China also demonstrated quantum supremacy with Gaussian Boson sampling[44], this time using a photonics-based quantum setup. While these breakthroughs bring about potential advances in science and technology [31], it also threatens the security of classical computer systems. On a quantum computer, Shor's [35] algorithm can solve integer-factoring and discrete-logarithm problems in polynomial time which means that public key cryptosystems that are built on Rivest-Shamir-Adleman (RSA), Diffie-Hellman (DH), and Elliptic-Curve Cryptography (ECC)

algorithms are no longer secure, and can be crypt-analyzed easily. Another example is Grover's [14] algorithm, which on a quantum computer provides a quadratic speed-up in performing brute-force attacks against symmetric-key and hash-based cryptography. Applications that rely on cryptography to achieve confidentiality, integrity, authenticity and non-repudiation for their data, users and communication will need to use alternative mechanisms or have the security and trust eroded due to quantum computers. The National Institute of Standards and Technology (NIST) is currently running on a Post-Quantum Cryptography (PQC) contest [26] to standardize suitable quantum-resistant asymmetric key algorithms for key exchange and digital signatures and is expected to finalize the standard by 2024 [24].

The good news is that current quantum computers are not sufficiently powerful to run Shor's or Grover's algorithm on a large-enough scale. Shor's algorithm has been demonstrated up to a 7-qubit quantum computer [41] and none of the current-day noisy intermediate-state quantum computers (NISQ) [28] are fault-tolerant enough to beat classical computers at asymmetric key cryptanalysis. On the other hand, NIST mentions in 2016 [8] that by 2030 with a budget of $1 billion, a quantum computer could likely be built to break RSA-2048 keys. So how can organizations be sufficiently prepared to face the threat of quantum computers? The study by Arslan et. al. [4] listed 4 areas that are all cryptography-specific. We intend to dive deeper and use threat modelling to find the answer.

The rationale to use threat modelling is logical. Organizations face circumstances and situations that can impact and cause harm to the organizations' own, other organizations' or even national assets, personnel, processes, mission, function, image or reputation. These circumstances or situations are potential violations of security are known as threats and are caused by threat sources [6]. Any environment where the system operates may have both known and unknown vulnerabilities or weaknesses and can be exploited by one or more threats causing a breach of the system's security processes or policy. As technology continually evolves (in the case of QC), new threats and even threat types emerge. NIST describes threat modelling as a risk assessment method that is used to model aspects of both offensive and defensive sides of a specific logical entity, which can be a system or an environment, an application or a host or even a piece of data or information [37]. Here, we have distinguished the difference between a threat, vulnerability and risk.

– *Threat.* The word "threat" has an extensive range of different meanings associated with it and it can be understood as people or person, event, weakness or vulnerability and in the context of cybersecurity, also as malware, criminal activity, and espionage. A threat can be described as an event or a development of events that are possible and harmful. Compared to danger which is more tangible and well-defined, a threat has a more uncertain evolution phase and has to be dealt with using risk management procedures. During the risk management process, threats are usually decomposed further to threat events and threat sources to give a more detailed picture

of threats, their impact and possible mitigation. In essence, a threat is an undesired event or something malicious that can happen to or through a system/product/service.
- *Vulnerability.* A vulnerability refers to any trust assumption that can be violated to exploit a system. It is a weakness in a system, process, individual, control, implementation, architecture or even organizational structure and external dependencies. These weaknesses can be exploited, and vulnerabilities revealed to provide attackers with the window of opportunity.
- *Risk.* A risk is uncertainty or insecurity affecting objectives. Risk causes a deviation from expected and can be positive, negative or both, although the word "risk" is often associated with being implicitly negative. A risk usually contains an evaluation of the likelihood and impact and it has a score based on these estimations [37]. In the case of Cyber-Physical system (CPS) and other critical infrastructure, there is an added safety risk to the human operators, system and environment that must be considered.

In this paper's context, the advent of quantum computers poses a *threat* to classical computing systems because adversaries can run Shor's algorithm [35] on quantum computers to exploit *vulnerabilities* in RSA/DH/ECC asymmetric key cryptography and, to a lesser extent, run Grover's algorithm [14] to carry out faster brute-force attacks on encrypted data, passwords, and hashes, thus rendering such cryptographic primitives inadequate to provide the necessary security primitives that the application requires. What is less known or unquantified is the potential extent of the threat and therefore the risks faced by present-day applications and data.

Highly operational systems such as CPS require to go through regular threat modelling exercises to update their design and/or processes to remain secure. But not all threat modelling methods (TMM) are suitable for evaluating and mitigating QC threats. Our paper attempts to complement the post-quantum cryptography (PQC) standardization efforts by NIST [26, 24] by identifying an appropriate TMM that system owners can use in their preparation for the post-quantum computing era. Our contributions are:

- Performing a study of different threat modelling approaches and evaluating 20 TMMs to select PASTA, when complemented with Attack Trees and STRIDE, as the most appropriate TMM for evaluating QC threats for existing systems.
- Carrying out a threat modelling exercise using PASTA on a generic CPS set up to demonstrate its efficacy at evaluating QC threats, and providing the outputs of the exercise including mitigation strategies.

In Section 2, we perform a landscape study of different threat modelling approaches and methods to select an appropriate TMM for evaluating the QC threats. In Section 3, we carry out a threat modelling exercise using our selected method on a CPS setup to demonstrate its efficacy before concluding in Section 4.

2 Threat Modelling Landscape Study

Different threat modelling methodologies, frameworks, and tools have been developed. Some are more comprehensive than others; some have a higher abstraction level while some focus on one or a combination of a few domains with greater granularity. Different methods can be distinguished by the logical entity that is being modelled (data, software, system, service, product), the phase of the entity's lifecycle and the goal of the threat modelling. TMMs and tools can be consolidated with other methods and even risk management processes to create custom tools for special needs.

In selecting an appropriate TMM, it should be comprehensive enough to effectively communicate the relevant threats and risks to the management but should also have ample details for those responsible for mitigating the threat. Threat modelling is a continuous process against newer threats and matching it with the existing mitigation efforts. The key benefit from routine threat modelling is the precision of modelling results from the increased frequency in which newer data from the system is obtained, reviewed, and reported. We are mindful that as the evolving nature of QC still presents numerous facets of factors and considerations, it is unlikely to address all the QC threats by designing a perfect TMM. Instead, we start by identifying suitable threat modelling approaches that can be used, before narrowing them down to the most appropriate TMM for evaluating QC threats.

2.1 Threat Modelling Approaches

We describe the different (non-exclusive) approaches [36] and their suitability to analyzing the QC threat.

Asset-centric Approach. An asset-oriented approach begins with the identification of critical assets and impacts or consequences towards them. Asset-centric modelling focuses on questions, such as what one's most valuable assets are and what can go wrong with them. A list of valuable assets is then cycled through, and each asset is considered one at a time. Threat scenarios that can have an impact on the asset are described and prioritized. Assets that have a supporting role or can be used as a secondary asset to harm primary assets should also be included [36]. In modelling for QC threats, we expect the effort to be large but the results to be comprehensive since the threat modelling exercise will cycle through each asset to evaluate the QC-specific vulnerability. **Relevance: High**.

Attacker-centric or Threat-centric Approach. In the attacker-centric approach, potential adversaries' intent, capabilities, resources, characteristics relationships and/or behaviour are consolidated as a type of threat model. Understanding what adversaries seek to achieve for their actions against a system, may give an organization more understanding and insight into the Tactics, Techniques, and Procedures (TTP) of these adversaries. Adversary behaviours can

be organized using a cyber kill-chain model into a threat scenario or attack scenario. Threat sources and/or events are usually identified first, and threat scenarios and the developments of threats are described in more detail. Adversary characteristics and behaviours as well as intents and motivations are the key elements when identifying impacts[6]. Attacker-centric modelling focuses on questions, such as what the attacker wants and why as well as how attackers gain their objectives. In modelling for QC threats, this approach is efficient in narrowing down the scope as the QC threat posed by the cryptographic weakness is already known and the threat modelling effort can be targeted at identifying and mitigating negative outcomes. **Relevance: High**.

Software-centric. Software-centric threat modelling is performed during the software design and development process to reduce vulnerabilities in the software [37]. Software-centric modelling focuses on questions, such as what the system is and how it works, as well as what can go wrong and how it can be used incorrectly or harmfully. Hence it is often requirements and vulnerability oriented. In software or system-centric modelling techniques, data flow diagrams are usually used to first model the system, data, and boundaries and then determine which threats are relevant to each component and trust boundary-crossing. In modelling for QC threats, this approach is useful mainly for developers since the vulnerabilities are well understood which allows the software to be designed and evaluated accurately. On the other hand, the unknown impact of QC threats may lead to a large number of overlapping threats being identified. **Relevance: Low**.

Data-centric Approach. Data-centric threat modelling focuses on protecting types of data/ information within a system instead of hosts, operating systems or applications. The system and data of interest are identified and characterized and prioritised. The focus is on the characteristics of authorized locations for storing, transmitting, executing, inputting and outputting data within the system: data flows between authorized locations, security objectives and people and processes authorized to access the data [37]. In modelling for QC threats, this approach is efficient since a large proportion of the cryptographic implementation is meant for data protection. However, we are concerned that this focused approach may not be ideal for non-data-related considerations such as business-impact analysis. **Relevance: Medium**.

2.2 Risk Management

Risk management [40] is usually not a stand-alone threat modelling approach, but one that integrates risk considerations and processes into one or more of the approaches mentioned in Section 2.1. While it increases the overall effort in performing the threat modelling exercise, the outcome is a more comprehensive and complete picture, especially in threats where the resulting impact is

not well defined or known. It also allows organizations to take on a more preventive posture when dealing with such threats. In modelling for QC threats, risk management extends the known QC threats into identified risk areas for application owners to calibrate and manage. It can help organizations assess, quantify and prioritize the various risk areas including business costs, probable losses, organizational preparedness, safety, etc, and embark on both technical and non-technical preventive and/or mitigation actions.

2.3 Threat Modelling Methods (TMM)

TMMs are used to create an abstraction of the system, profiles of potential attackers, including their goals and methods and producing a catalogue of potential threats that may arise. Some TMMs are typically used on their own while others are used in combination with others. We performed a landscape study that included a total of 20 different TMMs (see Table 1). The study includes all 12 TMMs studied by Shevchenko [33] and all 6 most popular TMMs listed by EC-Council [12].

In our study, we are looking for an asset-centric approach TMM that includes risk management techniques and can be complemented with a threat/data-centric approach to provide QC threat focus. This criterion is likely to yield the most appropriate TMM candidate for evaluating QC threats while balancing between completeness and efficiency.

2.4 Result of Study

PASTA [40], incorporating Attack Trees [32] and STRIDE [18], stands out as the TMM that is suitable for evaluating QC threats. The purpose of PASTA is to provide a process for simulating attacks to systems (even as a subset of just applications), analysing threats and mitigate the risks and impacts that these threats present to organizations. PASTA comprises a seven-stages process for modelling attacks and analysing threats to a particular system and environment. The objectives are curtailing risks and their associated impact on the organisation or business. Organisations or businesses can address the adequate level of countermeasures or risk mitigation measures to be deployed to mitigate the risk from threats and attacks by following this process. A description of the PASTA threat modelling method, along with Attack Trees and STRIDE, is found in Appendix A.

We chose PASTA over OCTAVE [7] due to the former's ability to incorporate attacker-centric and data-centric to its asset-centric approach. This allows the threat modelling exercise (see Section 3) to be more efficient in identifying and addressing the QC threats as compared to a generic threat modelling method. We chose PASTA over IDDIL/ATC [25] due to the former's availability of documentation and use-cases, and its ability to address risk at a strategic level.

Table 1. List of TMM studied on suitability for QC threat evaluation.

TMM	Approach	Risk	Pros	Cons	Suitability
ATT&CK [39]	Attacker		Indepth understanding of the adversary, useful for hunting new threats	Lacks focus on individual threats. Lacks operational impact analysis.	No. Insufficient focus on QC threats.
Attack trees [32]	Threat		Easy to use and can quickly map out threats.	Does not consider business objectives and lacks operational impact analysis.	Partial
CAPEC [27]	Attacker		Large searchable collection of known attack patterns	More suitable for penetration testing and less on understanding new threats	No. Much of QC threats and controls are still evolving.
DREAD [20]	Attacker	✓	Relatively simple for a risk model.	Incomplete risk modelling.	Not considered. Deprecated.
hTMM [21]	Attacker, Software	✓	Builds on SQUARE & Persona non Grata	Relatively new. Lacks documentation and use-cases	Not considered. Immature.
IDDIL / ATC [25]	Asset, Data	✓	Comprehensive modelling methodology. Incorporates other TMMs	Lacking in available documentation as compared to other TMMs.	Likely.
Invincea [15]	Attacker		Process is made easier through gamification	Uses existing security products as controls	No. Much of QC threats and controls are still evolving.
LINDDUN [10]	Data	✓	Strong focus on privacy threats.	Lacking in available documentation as compared to other TMMs.	Partial. Unclear if non-privacy related QC threats may be uncovered.
NIST SP 800-154 [37]	Asset, Data		Easy to adopt	Highly dependent on collection of available references and known security controls	No. Much of QC threats and controls are still evolving.
OCTAVE [7]	Asset	✓	Flexible methodology that incorporates security and operational risk considerations.	Training and experience of team is important. Large effort needed	Likely
OWASP [42]	Attacker		Easy to adopt	Focused on threats on web-based platforms	No. Lacks non-web QC threats.
PASTA [40]	Asset	✓	Comprehensive threat modelling at technical, operational, and business levels. Incorporates other TMMs.	Large effort needed	Yes.
Persona non Grata [9]	Attacker		Easy to adopt	Lacks focus on individual threats. Lacks operational impact analysis.	No. Insufficient focus on QC threats.
Security Cards [11]	Attacker		Process is made easier through gamification	Inconsistent results as process relies on brainstorming	No. QC threats may not be well understood.
SQUARE [22]	Software	✓	Proper security and risk considerations are built-in early.	Mainly relevant during requirements and design phase.	No. May not be suitable for existing systems.
STRIDE [18]	Software, Data		Easy to learn and well-documented	Lacks analysis on different operational environments	Partial
Tara (Intel) [29]	Attacker		Easy to adopt by referencing Threat Agent Library	Highly dependent on completeness of library.	No. Much of QC threats and controls are still evolving.
TARA (Mitre) [43]	Asset, Threat	✓	Easy to adopt by scoring against known TTPs and CVS	Simplified risk modelling.	Partial
Trike [30]	Asset	✓	Includes model for evaluating and prioritizing acceptable risk	Lacks documentation and use-cases	Not considered. Deprecated
VAST [3]	Attacker		Has an automated tool. Able to scale to large systems.	Lacks open documentation	Not considered. Requires commercial license.

3 QC Threat Modelling Exercise

We perform a threat modelling exercise using PASTA on a generic CPS set up as a walk-through on how QC threats can be identified, evaluated and mitigated.

3.1 Generic CPS Model

In [19], Lee described the CPS problem as the intersection between the cyber and physical problems and all three areas need to be examined and addressed separately. The environment we define in our model therefore comprises three parts, namely, physical environment, CPS and cyber IT, as shown in Fig 1. The physical environment includes the external physical operations that control the inputs and manages the supply to the CPS. It includes several maintenance features that manage the external assets and the associated physical processes. The CPS layer is intermediate, and it involves the supervisory control system, the internal communication system which manages the sensors and controls the actuators. The operations of this layer are managed through command and control operations of the Programmable Logic Controller (PLCs) that use sensory data acquisition to take action based on the input as well as output from the sensors and actuators. Finally, the cyber IT environment involves parts supporting remote invocations and accessibility through the external communication network. This layer helps with the management of features of CPS allowing control over the cloud.

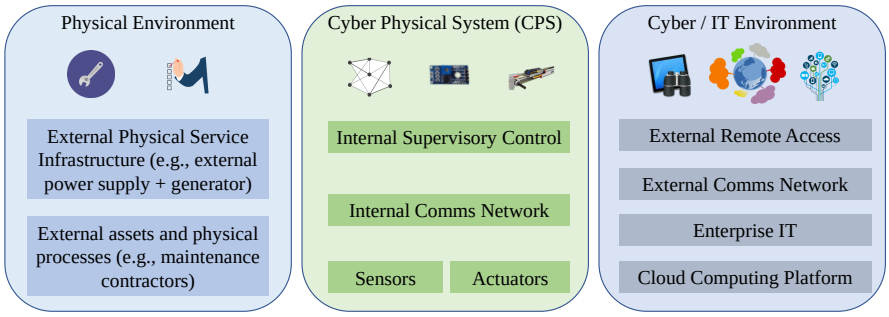

Fig. 1. An overview of a generic CPS model.

The security requirements for a CPS system extend beyond the traditional technical security requirements that govern a cyber IT system. The additional interface with the physical environment means that the security of the CPS system can impact the physical environment and vice versa. In NIST's "Guide to Industrial Control Systems (ICS) Security" [38], the health and safety of human

lives as well as damage to the environment are identified security considerations that a CPS system, but not a cyber IT system, may face. Conversely, the CPS system is required to maintain its robustness and resilience [2] against possible events, such as weather hazards, acts of war, and power outage, that the physical environment may impact the safety and security of the CPS system.

In the rest of this section, we will only flesh out QC-related[3] threats and risks.

3.2 PASTA Stage 1 to 3

The first 3 PASTA stages require us to define the objectives, define the technical scope, and perform the decomposition of the system. The guiding questions we use at these stages are:

- Stage 1 - Define Objectives
  - What are the key business objectives?
  - What are the critical functions and assets that might be affected by a QC threat?
  - What are the system safety standards at risk?
  - How does the compromised system cause catastrophic or irreparable damages?
  - What are the risk tolerance levels concerning Confidentiality, Integrity, Availability and Authentication?
- Stage 2 - Define Technical Scope
  - What is the system architecture and the boundaries?
  - What are the security controls and draw bridges?
  - What is the Data Flow or Process Flow, and interdependencies?
  - What are the external interfaces? (Cyber to CPS interfaces)
  - What are the protection measures in this external infra (ie. power sources, security system, enterprise IT system)?
- Stage 3 - System / Application Decomposition
  - What are the different components/environment in the system assessed? (cyber, physical, cyber-physical)
  - What are the possible QC threats/vulnerabilities arising from these different components/ environments?
  - Where are their entry points in a different environment?
  - Where are the "trusted environments/zones"?
  - What are the supply chain weakness in the system? (ie. suppliers of a thumb drive, backup storage media, cloud enterprise system that needs transfer)

[3] For non-QC-related CPS threat modelling, the reader is invited to reference [17, 13, 1, 16]

Output. We reference a generic CPS model, as shown in Figure 1. To evaluate QC threats, there are no changes to the boundaries of the technical environment and interdependencies between its infrastructure and application. Overall, the boundaries are depicted between the Physical environment, Cyber-Physical System (CPS) and the Cyber-IT environment. We next add on the objective that the critical systems and assets in the CPS can continue to operate safely and resiliently in the post-quantum era.

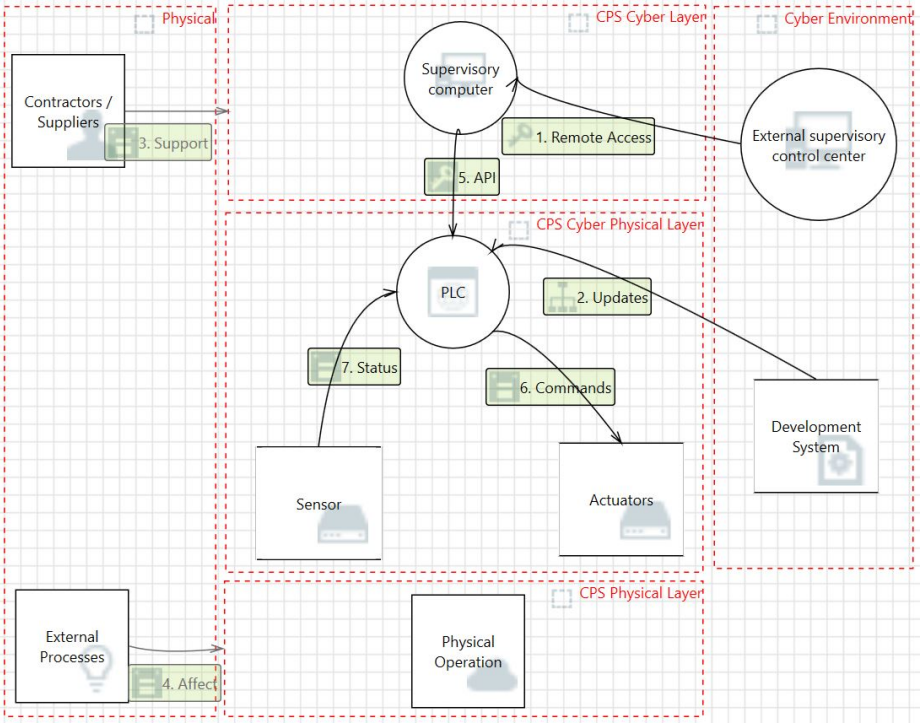

Fig. 2. Generic CPS setup with data flows identified.

We then divide the CPS boundary into the cyber layer, cyber-physical layer and physical layer, and identify seven major data flows (diagrammatically shown in Figure 2) that could be affected by QC threats. These are:

DF#1: This refers to the data flow from an external supervisory control centre to the onsite supervisory control system via remote access. This allows a central body to remotely manage and monitor multiple CPS setups.

DF#2: This refers to the data flow from an external computing system (eg. Enterprise IT or Cloud computing) via the external communication networks into the CPS setup. Updates and patches can be transmitted via this flow. Employees with access to the Enterprise IT or Cloud

computing service might fall prey to social engineering and will in turn infect the CPS with transferred files, programs or malware.

DF#3: This refers to data flow from external assets and physical processes to the CPS setup. This can be in the form of external contractors conducting support and maintenance works on the CPS. For example, CPS patches handled by contractors via thumb drive, hard disk or vendor laptop will inevitably expose the CPS setup for exploits.

DF#4: This refers to data flow from external physical infrastructure providers into the CPS setup. For example, the electrical or water supply contractor might tweak the readings or measurements of the supporting environment system.

DF#5: This refers to the data flow from on-site supervisory control (e.g. Human Machine Interface) to the PLCs. Commands are likely to be sent via API to the PLCs for executing controls.

DF#6: This refers to data flow from PLC to actuators within the CPS setup. PLC commands are sent directly to the actuators to execute the designated actions like opening and closing of valves or the starting or stopping of pumps.

DF#7: This refers to the data flow from CPS sensors to PLC. Sensor readings are being routed back to the PLC as feedback signals. These include status information such as water level in the tank, temperature readings, or alerts.

3.3 PASTA Stage 4 to 6

The next 3 PASTA stages require us to perform the threat analysis, vulnerability and weakness analysis, and attack modelling. The guiding questions we use at these stages are:

- Stage 4 - Threat Analysis
  - What are the threats that the STRIDE model tells us?
  - How does the attack/hack take place? What are the probabilities of each of the attack vector?
  - What does the identified threats correlate with the severity and fixability of the threats from the available threat intelligence?
  - What is the analysed impact of these identified threats?
- Stage 5 - Vulnerability and Weakness Analysis
  - What are the available vulnerability and penetration testing reports?
  - Any recent audits or vulnerability scanning or penetration testing conducted?
  - Are there trends of certain vulnerabilities being exploited?
  - What are the false positives and false negatives trends?
  - What is the overall vulnerabilities score?
  - What is the security posture from vulnerabilities?
- Stage 6 - Attack Modelling

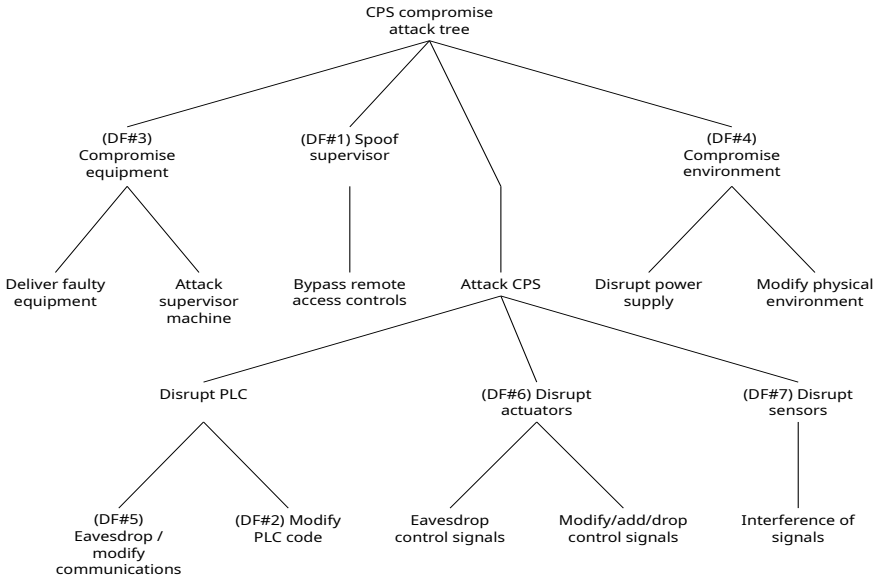

Fig. 3. Attack Tree for generic CPS setup when evaluating QC threats.

- From the Attack Tree, for each application that uses public-key cryptography, how can Shor's algorithm be used to compromise the system? Can the algorithm be replaced with a PQC candidate algorithm [26]?
- From the Attack Tree, for each application that uses symmetric key cryptography and hashing, how can Grover's algorithm be used to compromise the system? Can we increase the key size?
- How are the vulnerabilities and attacks vector associated?
- Are there attack vectors that have been made less effective with the vulnerabilities remediated?
- Any vulnerabilities that could not be fixed?

Output. We use a combination of Attack Trees [32] (see figure 3) and STRIDE [18] to analyze the data flows to list out the threats in Table 2.

3.4 Stage 7 - Risk & Impact Analysis

This step requires the analysis of the business impact in both qualification and quantifiable terms. There is also a need to propose some countermeasures and residual risk mitigation measures. Lastly the need to identify and recommend some risk mitigation strategies for the system owners. The guiding questions we use at this stage are:

Table 2. STRIDE threat evaluation of data flows

Data Flow	STRIDE Property Affected	Threat Description
DF#1 - Data flow from external computing system and communication networks	STRI__	The assessed threat can come from external hackers performing cryptanalysis on the encryption and authentication for the remote access link to the supervisory control centre using Shor's algorithm. This will allow the hacker to view or modify the communications.
DF#2 - Data flow from external supervisory control centre	STRI_E	The assessed threat can come via external communication networks into the CPS system. Employees with external access may fall prey to man-in-the-middle or social engineering attacks and in turn transfer malware or improper code that the PLC may use.
DF#3 - Data flow from external environment controls	STRI_E	the assessed threat will likely come from the compromised contractors and vendors who turned against the CPS system owners. These contractors may be able to introduce exploits or malware that disrupt the internal CPS setup while supplying, maintaining and patching the CPS.
DF#4 - Data flow from external physical infrastructure providers	ST____	Supply chain vendors can sabotage (deliberately or unintentionally) the electrical, water, temperature controls through the equipment they supply. The assessed threat is the vendor introducing errors in the parameters such as temperature, water, or even electrical level which affects the PLC's processing logic.
DF#5 - Data flow from on-site supervisory control to PLC	ST_I__	The assessed threat is fake connections introduced by the malicious insider. Potentially, these staff, who turned rogue can view or modify the communications between the supervisory control system and the PLCs.
DF#6 - Data flow from PLCs to actuators	ST_I__	The assessed threat is the malicious insider/staff who observe or modify the commands being sent to the actuator. This will potentially cause damage to the entire CPS such as overflow of water, or overheating or undercooling of equipment.
DF#7 - Data flow from sensors to PLCs	ST_I__	the assessed threat is from a malicious insider who can view the sensor readings, deliberately tamper the sensor hardware or provide erroneous feedback to the programmable controller and supervisory control system.

- What are the key business objectives and critical services that are affected?
- How else can the risk of safety be minimized? How resilient is the system to an unaddressed QC threat?
- What is the degraded mode of operations/ services?
- What mitigating / remediation measures are possible to counter the remaining threats?

Output. As the last step of PASTA, the broad mitigation strategies we identified for mitigating the threats brought about by QC are as follows:

1. *Strict Network Segregation.* Where algorithm replacement is not possible, this will ensure that the core CPS setup is separated from any external connectivity. This includes a clear delineation from Enterprise IT network and Cloud computing services. It will require that remote access to the supervisory control system to be terminated if the security measures cannot be strengthened to guard against QC threats. CPS should build an alert system to flag any illegitimate external connectivity or devices modification.
2. *Tight Supply Chain Controls.* Contractors and vendors will remain the weakest link in the entire ecosystem of the CPS. To prevent the unauthorised and unauthenticated actions by these contractors and vendors, there is a need for close monitoring and checks on the actions such as patching and system maintenance of the CPS setup.
3. *Internal Supervisory Controls and Monitoring.* To circumvent the malicious insider threat, procedural security clearance and monitoring need to be put in place. There must be a "check and balance" system to only allow authenticated actions by the staff and against any unsolicited actions.

4 Conclusion

In this work, we studied the different approaches for threat modelling to find the most appropriate TMM for evaluating QC threats. Although the cryptographic vulnerabilities exposed by QC on classical asymmetric and symmetric key cryptography is known, much of the potential impact from the threat of QC is still unknown and evolving. Hence, an asset-centric threat modelling approach with strong risk management, when complemented with a threat/data-centric approach to provide focus, is the criteria we used. We narrowed the field of 20 TMMs to find PASTA as the most appropriate TMM. We then carried out a threat modelling exercise using PASTA on a generic CPS setup to test its efficacy and showed the output of the threat modelling exercise. The effect of including risk management in the threat modelling exercise allows us to consider the possibility that some QC threats may not be completely addressable (due to constraints in time, resources, know-how, etc) and hence adopt additional broad-based mitigation strategies.

Acknowledgement. This project is supported by the Ministry of Education, Singapore, under its MOE AcRF Tier 2 grant (MOE2018-T2-1-111).

References

1. Ali, B., Awad, A.I.: Cyber and physical security vulnerability assessment for iot-based smart homes. sensors **18**(3), 817 (2018)
2. Arghandeh, R., Von Meier, A., Mehrmanesh, L., Mili, L.: On the definition of cyber-physical resilience in power systems. Renewable and Sustainable Energy Reviews **58**, 1060–1069 (2016)
3. Arguwal, A.: Threat Modeling Methodologies: What is VAST?, online: https://threatmodeler.com/threat-modeling-methodologies-vast/ [accessed: March 2021]
4. Arslan, B., Ulker, M., Akleylek, S., Sagiroglu, S.: A study on the use of quantum computers, risk assessment and security problems. In: 2018 6th International Symposium on Digital Forensic and Security (ISDFS). pp. 1–6. IEEE (2018)
5. Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J.C., Barends, R., Biswas, R., Boixo, S., Brandao, F.G., Buell, D.A., et al.: Quantum supremacy using a programmable superconducting processor. Nature **574**(7779), 505–510 (2019)
6. Blank, R.M.: Guide for conducting risk assessments (2011)
7. Caralli, R.A., Stevens, J.F., Young, L.R., Wilson, W.R.: Introducing octave allegro: Improving the information security risk assessment process. Tech. rep., Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst (2007)
8. Chen, L., Jordan, S., Liu, Y.K., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D.: Nistir 8105 draft—report on post-quantum cryptography. Information Technology Laboratory Computer Security Resource Center (2016)
9. Cleland-Huang, J.: How well do you know your personae non gratae? IEEE software **31**(4), 28–31 (2014)
10. Deng, M., Wuyts, K., Scandariato, R., Preneel, B., Joosen, W.: A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. Requirements Engineering **16**(1), 3–32 (2011)
11. Denning, T., Friedman, B., Kohno, T.: The security cards: A security threat brainstorming toolkit. Univ. of Washington, http://securitycards.cs.washington.edu/ (2013)
12. EC-Council: 6 of the most popular threat modelling methodologies (2020), online: https://blog.eccouncil.org/6-of-the-most-popular-threat-modeling-methodologies/ [accessed: March 2021]
13. Fernandez, E.B.: Threat modeling in cyber-physical systems. In: 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech). pp. 448–453. IEEE (2016)
14. Grover, L.K.: Quantum mechanics helps in searching for a needle in a haystack. Physical review letters **79**(2), 325 (1997)
15. invincea: Know Your Adversary: An Adversary Model for Mastering Cyber-Defense Strategies (2015), online: https://www.ten-inc.com/presentations/invincea1.pdf [accessed: March 2021]
16. Islam, M.M., Lautenbach, A., Sandberg, C., Olovsson, T.: A risk assessment framework for automotive embedded systems. In: Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security. pp. 3–14 (2016)
17. Khan, R., McLaughlin, K., Laverty, D., Sezer, S.: Stride-based threat modeling for cyber-physical systems. In: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). pp. 1–6. IEEE (2017)

18. Kohnfelder, L., Garg, P.: The threats to our products (1999), online: https://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx [accessed: March 2021]
19. Lee, E.A.: Cps foundations. In: Design Automation Conference. pp. 737–742. IEEE (2010)
20. Mackman, A., Dunner, M., Vasireddy, S., Escamilla, R., Murukan, A.: Improving web application security: threats and countermeasures. Redmond, WA: Microsoft (2003)
21. Mead, N.R., Shull, F., Vemuru, K., Villadsen, O.: A hybrid threat modeling method. Carnegie MellonUniversity-Software Engineering Institute-Technical Report-CMU/SEI-2018-TN-002 (2018)
22. Mead, N.R., Stehney, T.: Security quality requirements engineering (square) methodology. ACM SIGSOFT Software Engineering Notes **30**(4), 1–7 (2005)
23. Microsoft: Microsoft threat modeling tool 2016 (2016), online: https://www.microsoft.com/en-sg/download/details.aspx?id=49168 [accessed: March 2021]
24. Moody, D.: NIST PQC Standardization Update - Round 2 and Beyond. Online:https://csrc.nist.gov/CSRC/media/Presentations/pqc-update-round-2-and-beyond/images-media/pqcrypto-sept2020-moody.pdf [accessed: March 2021] (2020)
25. Muckin, M., Fitch, S.C.: A threat-driven approach to cyber security: Methodologies, practices and tools to enable a functionally integrated cyber security organization (2017), online: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Threat-Driven-Approach.pdf, [accessed March 2021]
26. NIST: Post-Quantum Cryptography: Round 3 Submissions. Online: https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions [accessed: March 2021] (2019)
27. numerous: Common Attack Pattern Enumeration and Classification (CAPEC), online: https://capec.mitre.org/ [accessed March 2021]
28. Preskill, J.: Quantum computing in the nisq era and beyond. Quantum **2**, 79 (2018)
29. Rosenquist, M.: Prioritizing information security risks with threat agent risk assessment. Intel Corporation White Paper (2009)
30. Saitta, P., Larcom, B., Eddington, M.: Trike v. 1 methodology document [draft] (2005), online https://www.octotrike.org/papers/Trike_v1_Methodology_Document-draft.pdf [accessed: March 2021]
31. Savage, N.: Google's Quantum Computer Achieves Chemistry Milestone (2020), online: https://www.scientificamerican.com/article/googles-quantum-computer-achieves-chemistry-milestone/ [accessed: March 2021]
32. Schneier, B.: Attack trees. Dr. Dobb's journal **24**(12), 21–29 (1999)
33. Shevchenko, N.: Threat Modeling: 12 Available Methods (2018), online: https://insights.sei.cmu.edu/sei_blog/2018/12/threat-modeling-12-available-methods.html [accessed: March 2021]
34. Shevchenko, N., Chick, T.A., O'Riordan, P., Scanlon, T.P., Woody, C.: Threat modeling: a summary of available methods. Tech. rep., Carnegie Mellon University Software Engineering Institute Pittsburgh United ... (2018)
35. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM review **41**(2), 303–332 (1999)

36. Shostack, A.: Threat modeling: Designing for security. John Wiley & Sons (2014)
37. Souppaya, M., Scarfone, K.: Guide to data-centric system threat modeling. Tech. rep., National Institute of Standards and Technology (2016)
38. Stouffer, K., Falco, J., Scarfone, K.: Guide to industrial control systems (ics) security. NIST special publication **800**(82), 16–16 (2011)
39. Strom, B.E., Applebaum, A., Miller, D.P., Nickels, K.C., Pennington, A.G., Thomas, C.B.: Mitre att&ck: Design and philosophy. Technical report (2018)
40. UcedaVélez, T.: Threat modeling w/pasta: Risk centric threat modeling case studies. Tech. rep., Technical Report. Open Web Application Security Project (OWASP) (2017)
41. Vandersypen, L.M., Steffen, M., Breyta, G., Yannoni, C.S., Sherwood, M.H., Chuang, I.L.: Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance. Nature **414**(6866), 883–887 (2001)
42. Watson, C., Zaw, T.: OWASP Automated Threat Handbook Web Applications. Technical report, OWASP (2018)
43. Wynn, J., Whitmore, J., Upton, G., Spriggs, L., McKinnon, D., McInnes, R., Graubart, R., Clausen, L.: Threat assessment & remediation analysis (TARA): Methodology description version 1.0. Tech. rep., MITRE CORP BEDFORD MA (2011)
44. Zhong, H.S., Wang, H., Deng, Y.H., Chen, M.C., Peng, L.C., Luo, Y.H., Qin, J., Wu, D., Ding, X., Hu, Y., et al.: Quantum computational advantage using photons. Science (2020)

Appendix A PASTA

PASTA, or Process for Attack Simulation and Threat Analysis, is developed by Tony UcedaVélez [40] in 2012 to merge business objectives and impact with technical requirements. It provides a hybrid risk and attacker (relying on Attack Trees, STRIDE and/or other methods) perspective to threat modelling and produces an output based on assets. PASTA focuses on understanding the effect on business and how to plan and implement effective countermeasures where the involvement of decision-makers and stakeholders are part of the process.

A.1 PASTA Threat Modelling Method

PASTA is first implemented at the system level, using high-level architecture. This initial round should allow for the effective definition of all inputs and outputs for each component of the system. Then, PASTA should be implemented recursively for each component. All findings from the high-level system architecture should be passed to the next level component as input. It is a seven-stage process where the objectives and scope are first defined, the system is described in its components, before the threat, vulnerability and risk analysis are done. The stages and activities within the stages are listed in Table 3.

A.2 Attack Trees Threat Modelling Method

Attack / threat trees was developed by Bruce Schneider [32] in 1999. It comprises diagrams depicting possible attacks on a system that spans out in a tree-like

Table 3. 7 stages of the PASTA Threat Modelling Method [40, 34]

PASTA stages	Threat Modelling Activities
#1-Define Objectives	Identify Business Objectives Identify Security & Compliance Requirements Business Impact Analysis
#2-Define Technical Scope	Capture the boundaries of the Technical Environment Capture Infrastructure | Application | Software Dependencies
#3-System / Application Decomposition	Identify Use Cases | Define App, Entry Points and Trust levels Identify Actors | Assets | Services | Roles | Data Sources Data Flow Diagramming (DFDs) | Trust Boundaries
#4-Threat Analysis	Probabilistic Attack Scenarios Analysis Regression Analysis on Security Events Threat Intelligence Correlation & Analytics
#5-Vulnerability & Weakness Analysis	Queries of Existing Vulnerabilities Reports & Issues Tracking Threats to Existing Vulnerability Mapping Using Threat Trees Design Flow Analysis Using Use & Abuse Cases Scorings | Enumerations
#6-Attack Modelling	Attack Surface Analysis Attack Tree Development | Attack Library Management Attack to Vulnerability & Exploit Analysis using Attack Trees (see Appendix A.2) and STRIDE (see Appendix A.3)
#7-Risk & Impact Analysis	Qualify & Quantify Business Impact Countermeasure Identification & Residual Risk Mitigation Measures Identify Risk Mitigation Strategies

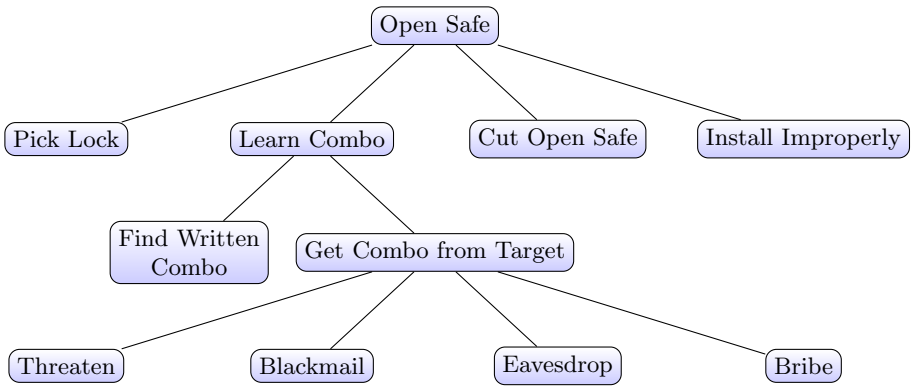

Fig. 4. Attack Tree example of a physical safe [32]

format, where the goal of an attack is akin to the root of the tree and the ways to achieve that goal are depicted as leaves of the tree, as seen in Figure A-1. Each separate tree represents a goal, and many aggregated trees form a "forest of attack trees. An attack tree can be formed for an exact use case or used together with existing and relevant attack trees to find threats. Each node of the attack tree is analysed on the issue that impacts the system, which is usually modelled with DFDs. Attack Trees is commonly used in combination with other TMMs.

In the Attack Tree example of a physical safe shown in Figure A.2, the goal of the attacker, i.e. an open safe, is first defined in the root node. The child nodes are then enumerated with the different actions or sub-goals that can lead to the goal, and their child nodes then list more detailed actions that may lead to the sub-goals. This process is repeated iteratively, and Attack Trees can be revisited after further studies or brainstorming sessions which can uncover other issues. Attack Trees require relatively less effort to model as it is a straightforward threat identification methodology. However, it does not consider factors like operating environment and operational/ business impact.

A.3 STRIDE Threat Modelling Method

STRIDE, short for "Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege", is a mnemonic that lists the six threats (described in Table 4) that can happen when a security property is violated. It is by far the most mature and well-understood TMM created by Loren Kohnfelder and Praerit Garg in 1999.

Table 4. STRIDE explained [36]

Threats	Property Violated	Threat Description
Spoofing	Authentication	Pretending to the something or someone other than yourself
Tampering	Integrity	Making changes to something that should not be modified
Repudiation	Non-repudiation	Claiming you did not do something, or were not responsible
Information Disclosure	Confidentiality	Providing information to someone not authorized to see it
Denial of Service	Availability	Preventing system to provide service by exhausting resources
Elevation of Privilege	Authorization	Allowing someone to do something they are not authorized to do

It starts by representing the system under evaluation using data flow diagrams (DFD) and identifying the entities, interfaces, boundaries and event flow. Using the DFD, every possible threat can then be enumerated and evaluated based on its vulnerability to the six properties of STRIDE. Microsoft has made available a STRIDE threat modelling tool available for download [23].