Threat Modeling in Construction: An Example of a 3D Concrete Printing System

M.U.R. Mohamed Shibly [a] and B. Garcia de Soto [a]

[a] S.M.A.R.T. Construction Research Group, Division of Engineering, New York University Abu Dhabi (NYUAD), Experimental Research Building, Saadiyat Island, P.O. Box 129188, Abu Dhabi, United Arab Emirates
E-mail: maahirur@nyu.edu, garcia.de.soto@nyu.edu

Abstract –

Cybersecurity threats related to new technologies get little attention until an incident occurs, and vulnerabilities are highlighted. In the case of construction projects, any cyber breach, either malicious or incidental, has the potential to cause significant damage. This varies from unauthorized access of sensitive project information to hijacking construction equipment to cause structural damage to the site or harm to personnel. Given the potential implications of threats in cyber-physical systems, and the potential for physical damage to products and personnel, serious consideration from a research perspective is needed. The risk of such attacks occurring is exacerbated in regions such as the UAE, where new technologies, such as 3D printing, are trending.

With that in mind, the objective of this study is twofold. First, to raise awareness about the cybersecurity implications of the new technologies adopted by the AEC industry. Second, to understand the core cybersecurity aspect of threat modeling concerning cyber-physical systems applied to construction projects. Several threat modeling methods such as STRIDE, OCTAVE, PASTA, and VAST have been developed. However, they are not easy to adopt by construction professionals who generally have limited knowledge of the cybersecurity domain. To address that, this study aims to develop a preliminary threat modeling approach that is relevant to the construction industry and can be quickly adopted to investigate the current technology being implemented. To demonstrate the practical feasibility of the proposed threat model, we consider an industrial-grade robotic arm system to 3D print construction elements offsite. This threat model will provide insights into a range of different threats that these systems are vulnerable to, allowing us to secure these systems against such threats, and raising awareness about the cybersecurity implications of implementing such technologies in the AEC industry.

Keywords –

3D Concrete Printing; Construction4.0; Cyber-Physical Systems; Cybersecurity; Cyberattack; CVSS; Risk Propagation; Smart Construction Sites; STRIDE; Threat model; Vulnerability Assessment

1 Introduction

The notion of having a digital model and a machine able to build it with a high degree of accuracy, with little human intervention, and in a timely fashion is very attractive and appealing. In the construction sector, that notion has been materialized with the development of 3D printing technology along with the use of contour crafting in which successive layers of cementitious material are placed to generate building elements. Although there are still many challenges to overcome (e.g., scalability, mobility, materials), there are already construction projects that have benefited from the use of 3D printing [1]. Some recent examples include the Apis Cor's two-story building in Dubai, UAE [2], Winsun China's villa [3], concrete bridges in Spain [4] and China [5], portions of the DFAB HOUSE [6] and the Concrete Choreography project [7] in Switzerland, single-family houses in Denmark [8] and France [9], and military barracks in the US [10].

A lot of efforts have been made in the research community regarding the technical aspects of 3D printing in the construction sector; however, the aspect of cybersecurity has been disregarded. The use of 3D printing in construction opens the door to new risks and vulnerabilities. Researchers are starting to consider the cybersecurity challenges and vulnerabilities caused by the digital transformation taking place in the construction industry [11, 12] and quantifying the cyber vulnerability of construction participants [13]. The ability to maliciously access to remote devices has already been documented. For example, [14] found that the radio signals typically used for crane controllers are not encrypted and can be easily intercepted and spoofed using off-the-shelf equipment and basic knowledge of electronics and radio engineering.

Similarly, regarding cybersecurity implications of 3D printing in other industries, [15] investigated how sabotage attacks could compromise the quality of 3D printed parts. Their study showed an attack against a desktop 3D printer used to manufacture propellers for an unmanned aerial vehicle (UAV). The sabotaged part experienced structural decay and caused the UAV to crash during flight.

As with other cyber-physical and connected systems, the connectivity requirements of 3D printing systems (e.g., controllers and manipulators, network connectivity, and peripherals, such as pumps or mixers), raises the potential for cyber-attacks. Considering the sensitive nature of construction projects, the introduction of the 3D concrete printing system as a cyber-physical system (CPS) that can be accessed by third parties with malicious intents poses several problems that need to be addressed.

The rest of the paper is organized as follows. In Section 2, we provide an overview of threat modeling, including existing methods and an evaluation of appropriate methods applicable to the construction industry. Section 3 discusses our efforts in the development of a threat modeling method (TMM), along with a high-level description of the overall procedure. In Section 4, we show the application of the TMM using a generic 3D Concrete Printing (3DcP) System. Also, we explain the specifics of each stage in the proposed TMM. Section 5 contains a discussion of the application and an identification of where the TMM succeeds and where it does not. Finally, we summarize key findings and suggest areas for future work in Section 6.

2 Threat Modeling

Threat modeling can be defined as the process of identifying potential threats, vulnerabilities, attackers, and targeted assets, with the goal to define countermeasures and plan risk mitigation strategies. The objective is to get a clear picture of the attack map, that is, how, where, why, and by whom an attack might occur. It consists of analyzing the security of an application or system by systematically cataloging and inspecting vulnerabilities present in a variety of contexts in the system under consideration [16]. The threat modeling process, as viewed by [17], can loosely be seen to consist of three high-level stages: (1) system characterization, (2) asset and access point identification, and (3) threat enumeration. Based on these principles, threat modeling requires a fundamental understanding of the underlying architecture, its design and implementation in order to prepare a thorough review and security analysis that can then be used to provide countermeasures that would prevent, or mitigate, the effects of any threats to the system. We proceed to identify two primary threat targets, Information Technology (IT) and Operational Technology (OT). The former relates to threats concerning the network infrastructure governing the system under consideration, while the latter relates to matters of physical security concerning the hardware operating in the system and potential damages to surrounding areas and people.

As with [18], in which a new threat modeling method was developed to fit a unique case, there is a need in the construction industry to investigate and consider the risks of cyberattacks due to the integration of new technology. With this in mind, we develop a threat modeling method that suits the small-scale but heavily interconnected nature of a 3D printing system used in construction.

2.1 Threat Modeling Methods (TMMs)

We place a heavy emphasis on understanding the nuances of existing TMMs, and what makes these methods suitable for specific systems. Our review of [19], [20], and [21] provided an understanding of a broad range of methodologies, from commonly used systems such as STRIDE and PASTA to uncommon ones such as CORAS and TRIKE. A summary of all the TMMs considered is shown in Table 1. This information will allow us to gauge the strengths and weaknesses of a range of TMMs along with which of their characteristics might come into use based on a variety of situations. There are a variety of characteristics to consider, from the range of threats, the existence of a built-in empirical component, to the availability of documentation.

2.2 Shortlisting Candidates

Considering the range of TMMs evaluated (Table 1), the following criteria were used to narrow down the selection of the TMMs to be used.

1. Threat Range (Low, Medium, High): Refers to the variety of threats captured.
2. Empiricism (Yes, No): Whether the TMM has an empirical component to gauge threats.
3. Consistency (Yes, No): Whether repeated use of the TMM yields the same results.
4. Risk-Mitigation (Yes, No): Whether the TMM contains some in-built component for mitigating the threats captured.
5. Suitability (Yes, No): Whether the TMM has not been explicitly developed for some specific system.
6. Documentation (Low, Medium, High): The amount of documentation available.

These characteristics are chosen based on our perspective on what would a generic situation be in which our TMM is used, with regards to the participants involved, the resources available, and the system under consideration. We chose the characteristics to capture a

broad range of threats, output an empirical result to gauge the magnitude of the risk of each threat, produce the same results consistently, contain in-built prioritization of risk mitigation and management that can be applied to a generic context while having proper documentation to aid during the threat modeling process.

Table 1. Summary of TMMs and characteristics used for selection in this study

Method	Threat Range	Empiricism	Consistency	Risk - Mitigation	Suitability	Documentation
OCTAVE	Medium	Yes	Yes	Yes	No	Medium
Trike	High	Yes	No	Yes	Yes	Low
PASTA	Medium	Yes	Yes	Yes	No	High
STRIDE	High	No	No	Yes	Yes	High
CORAS	Medium	Yes	Yes	Yes	No	Low
VAST	Medium	No	Yes	Yes	No	High
LINDDUN	High	No	No	Yes	Yes	Medium
hTMM	High	No	Yes	Yes (4)	Yes	N/A (3)
QuantitativeTMM	High	Yes	Yes	Yes (4)	Yes	N/A (3)
CAPEC (1)	Medium	No	N/A	No	No	N/A
ATT&CK (1)	Medium	No	N/A	Yes	No	N/A
IIDIL / ATC	High	No	Yes	Yes	Yes	Low
Security Cards + PnG (2)	Medium	No	Yes (SC) – No (PnG)	No	No	High (SC) – Low (PnG)

(1) CAPEC and ATT&CK are considered threat libraries and do not necessarily provide information as to modeling threats in a system

(2) Security Cards + PnG are essentially a gamification of the threat modeling process and should be used for training and brainstorming purposes only

(3) hTMM and QuantitativeTMM use STRIDE, and therefore we use the STRIDE documentation as a baseline for these TMMs; however, the methods themselves are not as mature as STRIDE

(4) Risk Mitigation based on STRIDE

Based on the selection characteristics previously described, Table 1 yields a few clear winners, with STRIDE and its derivatives meeting most of our criteria at their highest standards. Therefore, we have chosen the QuantitativeTMM as the basis for the modeling method for threat modeling in the rest of the paper.

3 Framework of proposed TMM – QuantitativeTMM

The framework of the QuantitativeTMM (QTMM) described in this section is a combination of the QTMM proposed in [22] along with parts of [23]. The high-level steps are shown in Figure 1 and described as follows.

Step 1: Define use case / problem statement
We begin by delineating our system; this includes an explanation of the system goals, the system components, information flows within our system, as well as users of our system [24].

Step 2: Define Data Flow Diagram (DFD)
Data Flow Diagrams are a method of breaking down the system into single components in the form of *Entities*, *Data Flows*, *Data Stores*, and *Processes*. *Trust Boundaries* are another component used to delineate the border between trusted and untrusted components in the DFD. The DFD acts as a graphical representation of these components in order to present the user with a high-level overview of the interactions between separate components in the system [23]. For a given use case or problem statement, the user creates a DFD with the required granularity. A finer granularity will produce a more refined overview that, at later stages, will yield a higher number of threats related to specific component interactions.

Step 3: Map STRIDE Elements into DFD
Once the DFD is created, we use the STRIDE classification of threats to 'map' individual components of the DFD to the respective threat classes. Table 2, adapted from [24], delineates the threat classes associated with each component. Once this is done, the user may begin to internalize the form of threats that may appear.

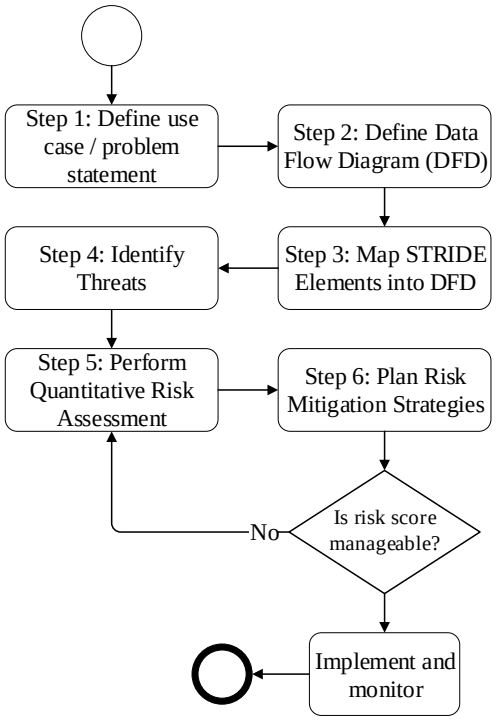


Figure 1. Main steps of the QTMM

Table 2. DFD Component Vulnerabilities as per STRIDE Threat Classes

Component	S	T	R	I	D	E
Data Flow		✓		✓	✓	
Data Store		✓		✓	✓	
Entity	✓		✓			
Process	✓	✓	✓	✓	✓	✓

A brief description of the different threat classes as per the STRIDE threat classification is summarized in Table 3. The purpose of this step is to identify the threat classes that are most prevalent to each component and prioritize the threat identification procedure for those classes.

Step 4: Identify Threats
Iterate over each component in the DFD and begin considering potential threats starting from generic attacks to more process-specific ones. If necessary, once threats are enumerated and cataloged, create short misuse case scenarios [25] for each attack. Due to space limitations, we forgo creating misuse case scenarios in this study.

Step 5: Perform Quantitative Risk Assessment
For each component in the DFD, and the relevant STRIDE threat classes, we generate attack trees using the information collected from the previous step. These component-based attack trees are then scored using a combination of the Common Vulnerability Scoring System (CVSS) and a risk propagation technique in order to gauge the final risk value of the threats [22].

Table 3. Threats classes per STRIDE

Threat	Description
Spoofing	An attacker attempts to mislead users or systems by falsifying either a process or an identity.
Tampering	An attacker modifies the system to cause harm.
Repudiation	An attacker rejects a transaction in the system.
Information Disclosure	An attacker obtains access to sensitive data concerning the system.
Denial of Service	An attacker makes the system unavailable to users.
Elevation of Privilege	An attacker manages to obtain administrator privileges.

Step 6: Plan Risk Mitigation Strategies
Considering the attack trees and their relevant scores, as well as the earlier generated misuse-case scenarios, the user can continue to ideate on potential actions to mitigate these threats. After mitigation strategies have been developed, a user may re-evaluate the previously defined attack trees to update the risk score for a threat class. Steps 5 and 6 are repeated until the user is satisfied with the level of threat mitigation. Once an acceptable risk score is obtained, the mitigations are implemented, and the system is monitored and updated as needed.

4 Example: TMM for 3DcP application

To illustrate the implementation of the proposed framework, we use a generic Robotic 3D Concrete Printing System as an example.

4.1 Define use case / problem statement

The system under consideration was chosen based on the review of existing literature and information obtained from industry experts to ensure a realistic case. The specification in question is based on ABB's IRB 6620 6-axis robot arm, with additional interfaces provided by the IRC5 industrial robot controller [26].

A schematic representation of the different elements for the 3DcP system used in this example is shown in Figure 2. The different elements identified in Figure 2 are described below.

1. **System Command:** The System Command refers to whichever device is used to relay instructions to the robot controller. This can be an Arduino microcontroller.

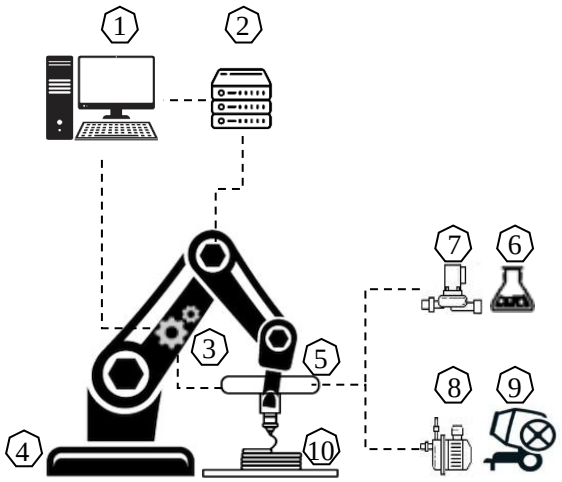


Figure 2. Schematic of the 3DcP system

2. **Robot Controller:** The Robot Controller is responsible for converting and relaying high-level commands passed through the system command onto the robotic arm itself. The IRC5 is an industrial standard for robot controllers.
3. **Printing Controller:** Based on the dimensions of what is being printed, the printing controller has several axes of movements that it can operate in to facilitate printing over a large surface area.
4. **Robotic Arm:** The Robotic arm is responsible for receiving instructions from the system command and passing on instructions to the precise part of the printing controller.
5. **Printhead:** The printhead is responsible for extruding the concrete mixture.
6. **Accelerating Agent:** A deposit containing the accelerating agent used in speeding up the concrete formation chemical reaction.
7. **Pump for Accelerating Agent:** Responsible for pumping the accelerating agent into the mixture, controls factors such as speed and throughput.
8. **Pump for Premix:** Responsible for pumping the premix into the printhead, controls factors such as speed and throughput.
9. **Premix Mixer:** A deposit containing the concrete premix used in the concrete printing process.
10. **3D Printed Object:** The designated 3D printed object as specified by the user.

4.2 Define the Data Flow Diagram (DFD)

Using the Legend defined in Microsoft's STRIDE Application article [24], we have defined the Data Flow Diagram, as shown in Figure 3, for our use case of the generic 3DcP application in Figure 2. Each of the data flows represent the flow of instructions in some digital format necessary in the 3DcP process.

A. 3D Specification Loaded into the System Command
B. Printed Item Specifications
C. Pump Control Information
D. Robotic Arm Printing Instructions
E. Robotic Arm Movement Instructions
F. Printhead Positioning Instructions
G. Printhead Extrusion Information

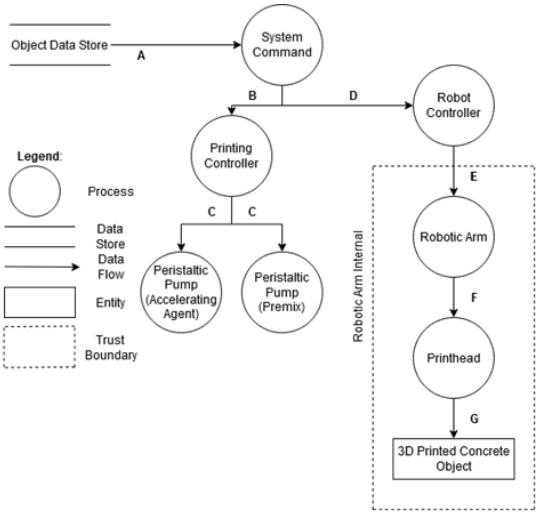


Figure 3. Data Flow Diagram

The trust boundary is a subjective measure of different levels of security that are present within the same system. The trust boundary in this example has been defined at the robotic arm and printhead, assuming that those elements would be less susceptible to direct access.

4.3 Map STRIDE to Elements into DFD

There are multiple 'process' components in the DFD. These components are, by nature, susceptible to all threat classes introduced by the STRIDE threat classification. Considering the data flows between these components, we realize that the information moved across the system is related to one another and, at times, are subsets of the preceding data flow. Threats that target one such data flow can potentially be replicated on another as per the goals of the attacker. However, the risk evaluation is dependent on the component in question. If we were to consider the "Robot Controller" component, it is unlikely that *Spoofing* or *Elevation of Privilege* threats are prevalent; *Tampering* threats, however, pose a serious concern.

4.4 Identify Threats

Consider the "Robot Controller" component. As a 'process,' it is susceptible to any of the STRIDE classes of attacks, but as mentioned previously, certain threats classes pose a greater risk than others. If we were to

deliberate on the potential threats that fall under the threat class of 'Tampering,' we would see threats like those delineated in Figure 4. As previously mentioned, these generic threats could take place in another DFD component, considering the nature of the data flow. To understand these threats in greater detail, the user may choose to generate misuse-case scenarios that dive into the context-aware specifics of these threats while providing a basis upon which risk-mitigation strategies are developed. The ideation performed at this step is fundamental to the remainder of the threat modeling process as it deepens the users' understanding of the system while providing a foundation upon which the Quantitative Risk Assessment may be carried out.

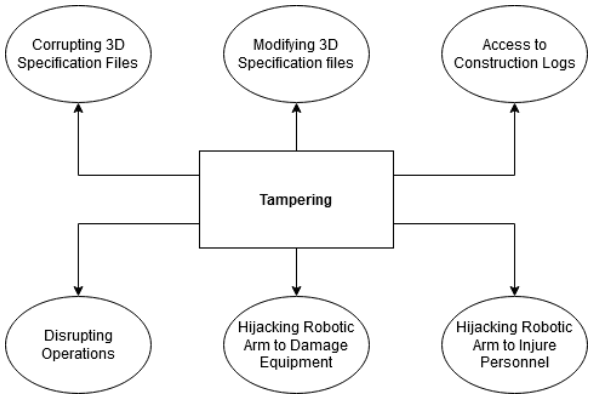


Figure 4. Potential Tampering Threats

4.5 Perform Quantitative Risk Assessment

An understanding of the variety of threats associated with the 'Tampering' threat class for the Robotic Controller aids us in developing the attack trees for this scenario. Using [22] as a guideline, we create Component Attack Trees (CAT) for a STRIDE threat class. This system uses four nodes, the *root node* (red), *intermediary node* (black), *leaf node* (gold), *class node* (white), and *mitigation node* (blue). The *class node* is designed to help systematically divide up threats. Each of the leaf and mitigation nodes are assigned a value reflecting the probability of success. This value is propagated upwards to the root node to determine the odds of success. To read the CAT, a user would begin at a leaf node and follow the path until the root node, at which point the attack has 'succeeded' [22].

Figure 5a is the high-level attack tree we generate for the Tampering threat class, and Figure 5b the risk propagation using CVSS. Unless otherwise specified, all leaf nodes are related by an 'OR'. Once we have created the attack tree, we use the CVSS to attribute a risk score to the leaf (gold) nodes. We then propagated these risks upwards as per the operations listed in [22] and summarized here.

- "OR" operation between two nodes (x,y): P(x)+P(y)-P(x)P(y)
- "AND" operation between two nodes (x,y): P(x)P(y)
- "MITIGATION" of node (x), with mitigation P(m): P(x) = P(x)*(1-P(m))

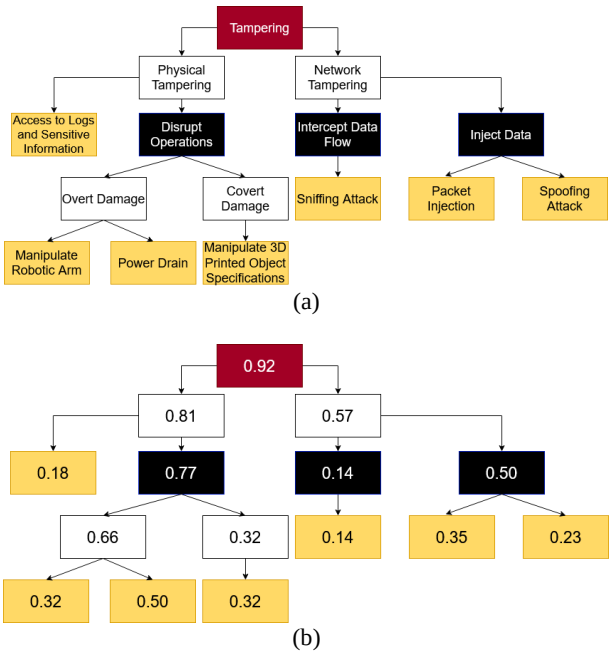


Figure 5. (a) Attack tree and (b) risk propagation and assessment for the Tampering Threat Class

Using the CVSS score [27] for the leaf nodes of this attack tree and the operations above to calculate the remaining risk scores for the various nodes, the overall risk score for the tampering threat class can be determined. This is showcased in Figure 5b. To illustrate the calculation of the score, consider the "Overt Damage" class, the 'manipulate robotic arm' threat has a lower risk value than 'power drain' because it is harder to accomplish while disconnecting the system from a power source is much easier to accomplish. However, they both present a threat, and together their risk score is calculated as follows:

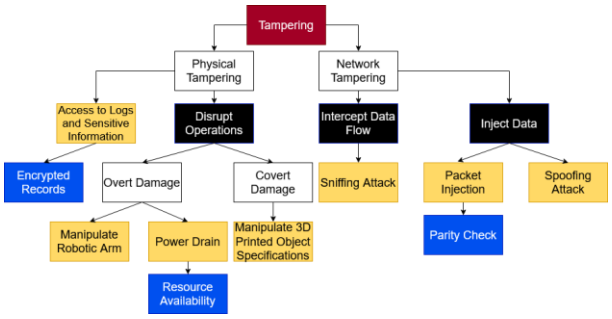
$$0.50 + 0.32 - (0.5 * 0.32) = 0.66$$

Following the same approach, the overall risk score for the Tampering Threat Class is calculated to be 0.93 (9.3/10 in the CVSS scale), which is classified as a critical threat.

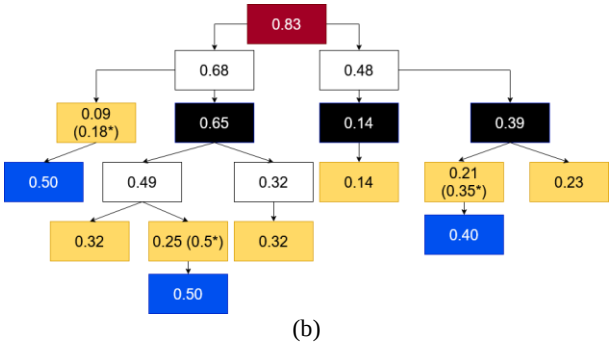
4.6 Plan Risk Mitigation Strategies

As a process, risk mitigation begins with the generation of the attack trees. Once a user has identified the different attack vectors, their understanding of the system will allow them to intuit strategies to counteract

threats at the lowest levels. The more detailed the DFDs and, consequently, the attack trees, the more nuanced simplified components will be available for a user to ideate mitigation strategies. Usage of attack libraries such as CAPEC and ATT&CK may help this brainstorming process. Figure 5 displays a scenario where there are no mitigation strategies. The user may update the attack tree with mitigation nodes (Figure 6) that would reduce the risk score of the corresponding leaf node (the "*" in Figure 6b indicates the pre-mitigation risk score). For illustration purposes, a subjective mitigation score was assigned to the mitigation (blue) nodes. Once the mitigations are considered, the overall risk score of the threat class can be recalculated. In this example, the mitigation nodes considered reduce the overall risk from 0.93 to 0.83, or a reduction of the risk of the tampering threat class from a critical risk threat, to a high-risk threat. This feedback loop can continue until the user is satisfied with the risk level, as well as the quality of the risk mitigation strategies in place.



(a)



(b)

Figure 6. (a) Attack tree and (b) risk propagation and assessment for the Tampering Threat Class with countermeasures (mitigation nodes)

5 Discussion

The nature of this paper hinges on providing an example of applying a TMM in the field of 3D printing in construction. Section 4 shows an example that can be used as a guide for users when tackling similar systems.

Although the length of this paper imposes limitations on the extent of details shown in the example, enough information is provided to allow the reader to get a general idea of the different steps required in the threat modeling analysis. The DFD and attack trees are simplistic in nature to convey the idea of the threat modeling process as opposed to providing a thorough threat model of this system specification.

The threat class we chose for this application was the STRIDE threat class of 'Tampering' applied onto the DFD's 'Robot Controller' process component. Considering the nature of the data flows in our system, many of the attack trees generated are likely to contain the same threats in relation to those components that are either inside the trust boundary or outside of it. However, the threats delineated in these attack trees would be scored differently, and ultimately the same threat could have different risk levels based on the component in question. We consider the Robot Controller component, a rather central piece in the 3DcP process, and one that is highly susceptible to Tampering threats.

For our example, we modeled both physical and network threats as two separate classes. While there is a degree of overlap between the two, we realized it would be more beneficial from a practical standpoint to illustrate a wider scope of threats. The threats related to network tampering are a generic class of threats that involve exploiting known vulnerabilities in any network system. On the other hand, the physical tampering threats are process-aware and are attacks that are carried out respective to the system in question.

The methodology presented is effective in detailing and visualizing the extent of the threats posed to a system with minimal effort, that is, once the attack trees have been generated and the CVSS scores for the lead nodes calculated, the risk propagation is straightforward. The most significant obstacle to a TMM is in its ability to capture a substantial proportion of potential threats. To succeed in this endeavor, a great deal of emphasis must be placed into developing the DFD; this aspect of the TMM is core to all subsequent steps.

6 Conclusion and Future Work

As 3D printing technologies emerge and their use in construction projects become more common, it is of utmost importance to develop methods and frameworks to identify vulnerabilities and address them before full implementation or integration with other systems is done.

This endeavor is heavily based on understanding the nuances of a threat modeling method in relation to cyber-physical systems and developing a threat modeling method with a specific application in mind, in this case, the use of 3D printers in construction. A large part of this involves an understanding of both the existing threat modeling methods as well as contemporary 3D printing

technology in construction that would allow the creation of an applicable threat modeling method.

Our ongoing work includes improving the current threat modeling method to better suit a more extensive scope of 3D printing specifications and configurations that involve supplementary machinery that would complicate the threat landscape. Such improvements will be complemented with research into specific attacks allowing us to gauge their viability. Attacks that involve physical externalities can be conducted over a simulated environment, whereas more traditional IT-related attacks can be attempted directly with the appropriate equipment on hand.

Once a thorough modeling methodology to scope threats is in place, our focus will shift into techniques for securing the systems investigated. This process is two-pronged, considering both proactive and reactive measures. Proactive measures will aim to patch security flaws in the system that can be easily avoided. Reactive measures will seek to provide guidance to 'worst-case' scenarios.

The culmination of this research will be a holistic guide to identifying and securing 3D printing specifications in construction against any manner of threats for both OT and IT scenarios.

Acknowledgment: *The authors would like to thank the support from the Center for Cyber Security at New York University Abu Dhabi (CCS-AD).*

References

[1] P. Raitis and B. García de Soto, "Preliminary Productivity Analysis of Conventional, Precast and 3D Printing Production Techniques for Concrete Columns with Simple Geometry," In: Bos F., Lucas S., Wolfs R., Salet T. (eds) *Second RILEM International Conference on Concrete and Digital Fabrication*. DC 2020. RILEM Bookseries, vol 28. Springer, Cham. https://doi.org/10.1007/978-3-030-49916-7_100.

[2] N. Webster, "Dubai unveils world's largest 3D printed two-storey building," 2019. Online: https://www.thenational.ae/uae/government/dubai-unveils-world-s-largest-3d-printed-two-storey-building-1.927590 (accessed April 18, 2020).

[3] Y. Ma and Y. Che, "A brief introduction to 3D printing technology," *GRC 2015 Dubai*, p. 4, 2015.

[4] IAAC, "3D printed bridge," *IAAC*, 2016. Online: https://iaac.net/project/3d-printed-bridge/ (accessed April 18, 2020).

[5] Z. Yu, "3D-printed 'ancient bridge' put to use in Tianjin - Chinadaily.com.cn," 2019. Online: https://www.chinadaily.com.cn/a/201910/17/WS5da7d747a310cf3e35571065.html (accessed April 18, 2020).

[6] Empa, "Empa - NEST - Digital Fabrication," 2017. Online: https://www.empa.ch/web/nest/digital-fabrication (accessed April 18, 2020).

[7] A. Anton, P. Bedarf, A. Yoo, B. Dillenburger, L. Reiter, T. Wangler, J.R., Flatt, "Concrete choreography: prefabrication of 3D printed columns," In: Burry, J., Sabin, J.E., Sheil, B., Skavara, M. (eds.) *FABRICATE 2020*, 2020, pp. 286-293, 2020.

[8] The BOD, "The BOD - The first 3D printed building in Europe," 2019. Online: https://cobod.com/the-bod/ (accessed April 18, 2020).

[9] T. Vialva, "A French family is the first to move into a 3D printed house - 3D Printing Industry," 2018. Online: https://3dprintingindustry.com/news/a-french-family-is-the-first-to-move-into-a-3d-printed-house-135881/ (accessed April 18, 2020).

[10] K. Kelly, "MCSC teams with Marines to build world's first continuous 3D-printed concrete barracks," *The Official United States Marine Corps Public Website*, 2018. Online: https://www.marines.mil/News/News-Display/Article/1611532/mcsc-teams-with-marines-to-build-worlds-first-continuous-3d-printed-concrete-ba/ (accessed April 18, 2020).

[11] B.R.K. Mantha and B. García de Soto, "Cyber security challenges and vulnerability assessment in the construction industry," pp. 29–37, 2019, doi: 10.3311/ccc2019-005.

[12] E.A. Pärn and B. García de Soto, "Cyber threats and actors confronting the Construction 4.0," in *Construction 4.0*, Routledge, pp. 441–459, 2020, doi: 10.1201/9780429398100-22.

[13] B.R.K. Mantha, Y. Jung, and B. García de Soto, "Implementation of the Common Vulnerability Scoring System to Assess the Cyber Vulnerability in Construction Projects," *In Proceedings of the Eight Creative Construction Conference*, pp. 117-124, 2020, doi: 10.3311/CCC2020-030.

[14] J. Andersson, M. Balduzzi, S. Hilt, P. Lin, F. Maggi, A. Urano, and R. Vosseler, "A Security Analysis of Radio Remote Controllers for Industrial Applications," 2019, Technical Report, Trend Micro, Inc.

[15] S. Belikovetsky, M. Yampolskiy, J. Toh, J. Gatlin, and Y. Elovici, "Dr0wned – Cyber-physical attack with additive manufacturing," in *11th USENIX Workshop on Offensive Technologies, WOOT 2017, co-located with USENIX Security 2017*, Sep. 2017.

[16] A. V. Uzunov and E. B. Fernandez, "An extensible pattern-based library and taxonomy of security threats for distributed systems," *Comput. Stand. Interfaces*, vol. 36, no. 4, pp. 734–747, Jun. 2014, doi: 10.1016/j.csi.2013.12.008.

[17] S. Myagmar, A. J. Lee, and W. Yurcik, "Threat Modeling as a Basis for Security Requirements," *StorageSS '05 Proc. 2005 ACM Work. Storage Secur. Surviv.*, pp. 94–102, 2005.

[18] K. Singh and A. K. Verma, "Threat modeling for multi-UAV Adhoc networks," in *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, Dec. 2017, vol. 2017-Decem, pp. 1544–1549, doi: 10.1109/TENCON.2017.8228102.

[19] N. Shevchenko, T. A. Chick, P. O. Riordan, T. P. Scanlon, and C. Woody, "Threat Modeling : a Summary of Available Methods," 2018.

[20] S. Hussain, A. Kamal, S. Ahmad, G. Rasool, and S. Iqbal, "Threat Modelling Methodologies: a Survey," *Sci.Int.(Lahore)*, vol. 26, no. 4, pp. 1607–1609, 2014.

[21] J. Selin, "Evaluation of Threat Modeling Methodologies A Case Study," *Sch. Technol. Inf. Commun. Technol.*, MSc Thesis. May, 2019.

[22] B. Potteiger, G. Martins, and X. Koutsoukos, "Software and attack centric integrated threat modeling for quantitative risk assessment," HotSoS '16. pp. 99–108, 2016, doi: 10.1145/2898375.2898390.

[23] J. Luna, N. Suri, and I. Krontiris, "Privacy-by-design based on quantitative threat modeling," *7th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, Cork, 2012, pp. 1-8, doi: 10.1109/CRISIS.2012.6378941.

[24] S. Hernan, S. Lambert, T. Ostwald, and A. Shostack, "Uncover Security Design Flaws Using The STRIDE Approach," Microsoft Docs. Online: https://docs.microsoft.com/en-us/archive/msdn-magazine/2006/november/uncover-security-design-flaws-using-the-stride-approach (accessed June 01, 2020).

[25] G. Sindre and A. L. Opdahl, "Eliciting security requirements by misuse cases," *Proc. Conf. Technol. Object-Oriented Lang. Syst. TOOLS*, no. TOOLS-PACIFIC2000, pp. 120–131, 2000, doi: 10.1109/tools.2000.891363.

[26] ABB, "IRB 6620 - Industrial Robots from ABB Robotics." Online: https://new.abb.com/products/robotics/industrial-robots/irb-6620 (accessed Jun. 01, 2020).

[27] FIRST, "Common Vulnerability Scoring System Version 3.0 Calculator," Forum of Incident Response and Security Teams. Online: https://www.first.org/cvss/calculator/3.0 (accessed June 06, 2020).