Lessons Learned from the "Hack My Robot" Competition and Considerations for Construction Applications

Muammer Semih Sonkor[1], and Borja García de Soto[1]

[1]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
semih.sonkor@nyu.edu, garcia.de.soto@nyu.edu

Abstract –

The construction industry is going through a digital transformation where automation and robotics are slowly making their way into construction projects. This change brings numerous benefits, such as cost and time efficiency and higher accuracy and quality. At the same time, it raises cybersecurity concerns. Since most construction environments are far from being human-free in the near future, the importance of providing robust cybersecurity when utilizing cyber-physical systems such as robots is augmented. The use of robotics in construction processes has long been under academia's and industry's spotlight, but the cybersecurity aspects have not received the attention they deserve. Several surveys have shown low awareness among construction stakeholders about cybersecurity, which increases the need for further studies on this topic.

This study provides an overview of the first academic-driven cybersecurity competition in the construction context, Hack My Robot (HMR), as part of CSAW'22, the most comprehensive student-run cybersecurity event in the world. HMR was held for the first time at New York University Abu Dhabi (NYUAD). The competition had two main rounds: the qualification round and the final round, where students presented their ideas to compromise the provided robotic system's functionality and the collected information. The system used in the competition imitated a construction progress monitoring robot that utilizes Robotic Operating System (ROS). This paper presents how this competition aims to contribute to construction cybersecurity efforts, what main outcomes were obtained, and how it will be improved in the upcoming editions.

Keywords –

Construction 4.0; Cybersecurity; Competition; Robotics

1 Introduction

Construction has long been an industry that relies on conventional equipment and traditional methods to perform most tasks. In a report by McKinsey in 2016, construction was listed as the least digitized industry after agriculture and hunting [1]. However, this has been rapidly changing with the integration of new technology in recent years. In a 2021 report, construction was indicated as the second industry with the highest potential for productivity growth from 2019 to 2024 as a result of digital construction, industrialization, and operational efficiency [2]. Cyber-physical systems (CPSs), such as robots, have a significant role in the expected productivity growth since they are an integral part of industrialization and digitization in almost every sector.

Digital transformation of the construction industry is often called Construction 4.0. This transformation, which includes the use of robotics and automation, increases productivity, improves the quality and accuracy of the handled tasks, improves safety on construction sites, and decreases the inclusion of humans, who are, by nature, prone to make mistakes. Examples of robots used in construction include progress monitoring robots [3], autonomous machinery to handle repetitive tasks such as earthworks material loading [4] and overhead drilling [5], and drones to inspect structures for damage or defects during the operations and maintenance (O&M) phase [6]. Construction robotics holds significant potential for improving cost and safety while reducing time; it also introduces cybersecurity risks that must be considered to ensure the secure operation of these systems.

Attacks against construction companies and projects can lead to serious safety issues and financial losses due to disrupted operations and damaged reputation. Some cyberattacks in the construction industry had significant impacts, supporting this statement. For example, confidential design documents of the Australian Intelligence Service's headquarters building were stolen by hackers in 2013 during the construction phase [7]. A study published by Trend Micro Research in 2019

included testing radio frequency (RF) remote controllers for cranes supplied by 17 vendors. The results showed that all tested controllers were vulnerable to cyberattacks [8]. Considering the close human-machine interaction in construction environments, potential attacks against the control systems of robots, which could result in the manipulation of functions, can cause serious safety issues. Since automated and robotic systems are starting to become a part of construction tasks in recent years, there have not been any known cyberattacks against construction projects that caused physical damage. However, examples from other sectors have proved the criticality of robust cybersecurity for safety. For example, a cyberattack against a steel mill in Germany caused the malfunction of a furnace and led to significant physical damage [9]. Also, sensitive data collected and transmitted by robots could be vulnerable to data breaches if proper security measures are not in place. Zhu et al. [10] emphasized that modern robotic systems are susceptible to various cyberattacks since most companies are targeting to get their products ready for the market quickly, which leads to overlooking cybersecurity mechanisms. Therefore, construction companies need to implement robust security measures to protect against these risks and ensure the safe and secure operation of robots on site.

Hack My Robot (HMR), held in 2022 to address the mentioned concerns, can be considered the first academic-driven cybersecurity competition in the construction context. It was a part of Cyber Security Awareness Week (CSAW), the world's most extensive student-led cybersecurity event. It took place at New York University Abu Dhabi (NYUAD), which hosted the Middle East and North Africa (MENA) region competitions of CSAW'22 on November 9-12, 2022. The students were challenged to generate ideas to compromise the data and operations of a progress monitoring robot, considering the characteristics of construction sites.

This study presents an overview of HMR and its preliminary results. The HMR competition and this paper do not aim to make a technical advancement in construction automation and robotics. Instead, the goals are to achieve a raised awareness about the cybersecurity aspects of digitalized construction environments with a particular focus on robotics, bringing the attention of the cybersecurity community to the construction sector, and utilizing the cybersecurity knowledge of students to discover potential problems raised with the use of robotics in construction projects. As mentioned by Salami Pargoo and Ilbeigi [11], construction cybersecurity studies have mostly focused on building information modeling (BIM), while issues related to construction robots have been considered for future work. To address this gap in the literature, this paper derives conclusions based on the initial results of the HMR event and tries to answer the question, "Is it possible to identify cybersecurity vulnerabilities of construction robots through a competition?".

The rest of this paper is structured as follows. Section 2 explains the significance of cybersecurity in construction by showing the previous efforts and some examples of cyberattacks against construction companies. Section 3 gives an overview of HMR, presenting an overview of the robotic system, different rounds of the competition, and lessons learned. Finally, Section 4 discusses the conclusions of this study and presents the planned future work.

2 The Importance of Cybersecurity in Construction

Cybersecurity concerns in construction have been augmented as the industry increasingly relies on technology to produce and store information, handle tasks on-site, and connect stakeholders. Previous incidents showed that hackers could cause financial losses, disruption of operations, and reputational damage. The construction industry is no different from the other sectors regarding the potential consequences of cyberattacks. Therefore, construction companies must prioritize cybersecurity and take the necessary actions before any adverse event occurs.

The first aspect to consider is the cybersecurity of information generated and stored throughout the lifecycle of construction projects since the digitalization of information has been running ahead of the digitalization and automation of physical tasks in the industry. BIM technologies such as design authoring software and online collaboration tools allow planning, designing, and managing projects in digital environments. As a result of this change in projects, from paper to digital, the amount of valuable and sensitive data increases, which creates potential vulnerabilities that hackers can exploit. Some studies addressed these issues and proposed solutions. For example, Zheng et al. [12] proposed a context-aware access control for BIM data environments to replace the mainstream role-based access control. Boyes [13] emphasized the need for change in the construction companies' security practices and the security policies by governments.

Since the digital transformation of physical tasks and the use of operational technologies (OT) in construction projects has been relatively slow compared to the digitalization of information, there have not been many studies focusing on OT cybersecurity in construction so far. One of the studies on this topic has been conducted by Sonkor and García de Soto [14]. They performed a bibliometric analysis to scrutinize the OT, construction, and cybersecurity literature. Their study revealed a

research gap regarding the cybersecurity of automation and robotics in the construction industry, which is one of the motivations of the HMR competition presented in this paper.

Previous cyberattacks against the construction industry raised cybersecurity concerns and alerted construction decision-makers and policymakers. For example, a British construction company, Interserve, has recently been fined £4.4 million by the Information Commissioner's Office due to its failure to prevent a cyberattack in May 2020 and caused leakage of more than 110 thousand employees' personal data [15]. An employee of Interserve forwarded a phishing email to a colleague who opened the email and downloaded the malicious file, which resulted in the leakage. Even though most cyberattacks against construction companies targeted information systems, similar patterns of attacks can be seen impacting OT as it becomes more pervasive in construction. Therefore, the industry should learn from past incidents of attacks and take action to provide a secure environment for robots as they make their way into construction projects.

Finally, it is essential to understand the level of cybersecurity awareness in the industry since small human mistakes are mostly the reason for falling victim to severe attacks. An academic survey [16] conducted among construction professionals and academics from May to September 2020 revealed the extent to which the construction industry is ready for the upcoming cyber threats. The survey—with the participation of 281 people—showed that nearly half of the respondents had never heard of the cybersecurity standards and frameworks provided to them. Thirty-five percent of the participants did not know whether or not their company had a cybersecurity plan. On the other hand, most of the respondents (84%) indicated that they were concerned about cybersecurity in the construction industry.

3 Hack My Robot

HMR is the first academic-driven cybersecurity competition in the construction context. It was organized by the S.M.A.R.T. Construction Research Group at NYUAD. The competition was a part of the 19th edition of Cyber Security Awareness Week (CSAW). CSAW 2022 took place in five regions (i.e., Europe, India, MENA, Mexico, US-Canada) with more than 3,000 competitors. HMR happened only in the MENA region (i.e., CSAW'22 MENA) and was open to all undergraduate and graduate students registered in MENA universities. HMR will be held annually in the upcoming years with different challenges and construction robots as a part of CSAW.

The competition had two rounds: the qualification round and the final round. Students were asked to submit ideas to compromise the collected data and the functionality of the robot during the qualification round and implement their ideas in front of the judges in the final round. The most successful teams in the final round, determined by the group of judges, were awarded cash prizes. The provided robotic system and its functionality simulated an autonomous progress monitoring task on a construction site. The data collection task in the challenge consisted of the robot autonomously moving across different predefined positions, capturing images on each of them, and returning to the initial position to start transmitting the collected data to another computer in the network, which would act as the server. The following subsections provide an overview of the competition and detail the different rounds.

3.1 Overview of the Robotic System

The robotic system used in the competition performs autonomous data acquisition to simulate a fully functional construction progress monitoring robot. Figure 1 shows different components of the robotic system divided into five levels based on their functionalities and the communications between them. This diagram was created based on the autonomous site monitoring system diagram presented in [17]. Further details of each level and the communication between the components can be found in [17]. Therefore, this section only provides a brief overview of the different levels.

Level 0 includes the physical components of the robotic system, including the robotic platform that houses all peripherals and the cameras and sensors that acquire data from the surrounding environment. Level 1 shows the network that connects all the elements of Level 0, the computer embedded in the robot (i.e., robot computer) that controls all the functionalities, the router that enables wireless communications, and the external computer that acts as the data server. Level 2 involves the Robot Operating System (ROS) [18] network, which is a widely used system in the robotics sector [19]. ROS 1, which has much fewer security features than ROS 2 [19], was chosen to show the cybersecurity vulnerabilities more clearly. In the ROS network, the robot computer functions as the ROS master, and the external computer connects to the ROS network to communicate with it. The ROS nodes can receive and publish information in the direction of ROS topics and give and receive commands in ROS services. Level 3 shows the autonomous control function of the robot. The robotic platform can autonomously communicate via ROS with all the actuators and sensors.

Finally, Level 4 demonstrates the human-machine interaction. Several graphical user interfaces provided by ROS enable visualizing the information collected by the sensors and cameras of the robot.

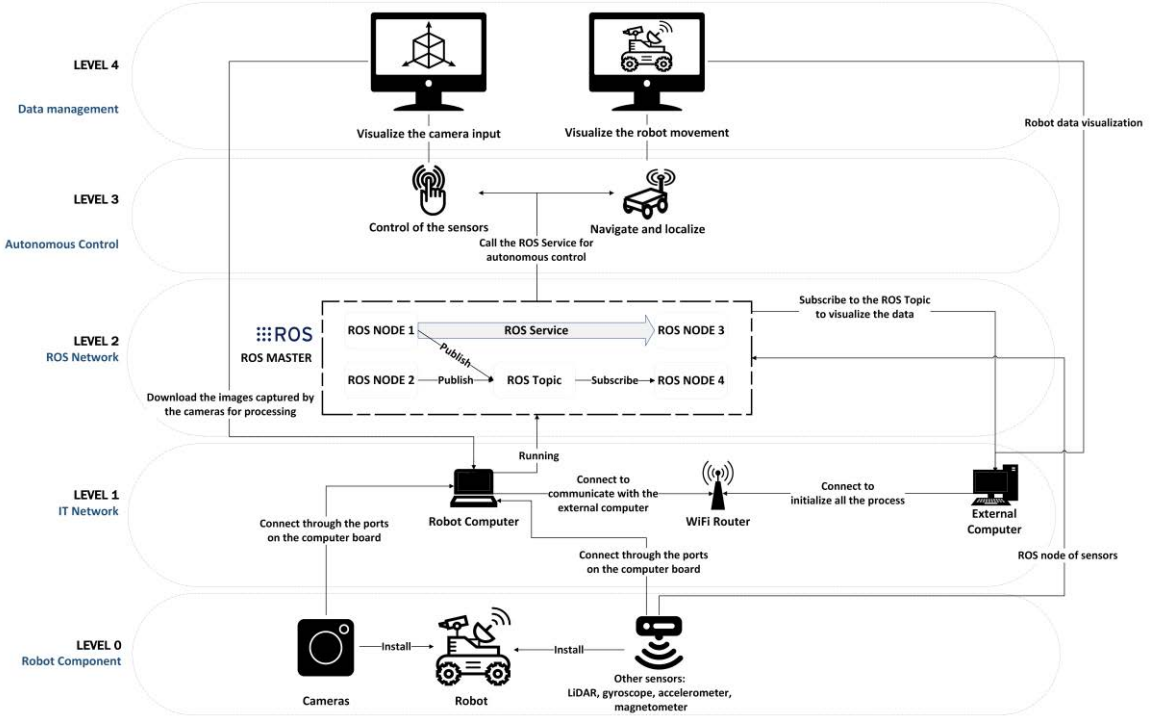

Figure 1. Diagram of the robotic system used in HMR (adapted from [17])

3.2 Qualification Round (Round 1)

The first round (i.e., qualification round) challenged the participating teams to generate ideas to compromise the provided robotic system (see Section 3.1) and find ways to improve its security level to mitigate the vulnerabilities they mentioned. They were also asked about their motivation to compromise such a system considering the construction context. They were given a Google Form to answer five open-ended questions for the qualification round and several other questions (e.g., team name, email addresses, university name) for registration purposes. The registration and the first round were open for one and a half months (from August 15 to September 30, 2022). The open-ended questions for the qualification round were as follows:

1. Considering the robotic system in the provided challenge document, what would you do to compromise the data collected?
2. Considering the robotic system in the provided challenge document, what would you do to compromise the operation?
3. In your opinion, what are the most vulnerable components? Why?
4. What modifications would you suggest to make the system less vulnerable? In other words, what would you change to reduce the vulnerabilities you identified in Question 3?
5. What would be your motivation to compromise the described robotic system? Consider the characteristics of the environment where the robot operates and the potential impacts of such compromise on the business processes/continuity.

Six teams, including 19 students, registered and answered the questions in the qualification round. The answers from the participating teams were evaluated considering their technical knowledge, the feasibility of their ideas, the relevance of the answers in the given context, and the breadth of the responses. Based on the evaluation, five teams, including 18 students, were selected for the final round. Four finalist teams were from NYUAD, and one was from King Abdullah University of Science and Technology (KAUST), Saudi Arabia.

3.3 Final Round (Round 2)

3.3.1 Overview of the Final Round

Shortly after announcing the qualification round results, the finalist teams were provided with the robots (i.e., TurtleBot 3 Burger RPi4 4GB) and the peripherals (i.e., fisheye lens camera and camera frame) that they were going to use in the final round. The assembled robot can be seen in Figure 2. They were also provided with instructions (see the GitHub repository [20] for more details) to set up their robots and an IMG (.img) file with which they could flash the SD cards of their robots. The provided IMG file included a ROS system (ROS Noetic), including the ROS nodes, similar to the one used in the

final round. They had one month (from October 12 to November 11, 2022) to set up the robot and the ROS system to get familiar with them, research more on the given challenges, detail their ideas, and test their feasibility.

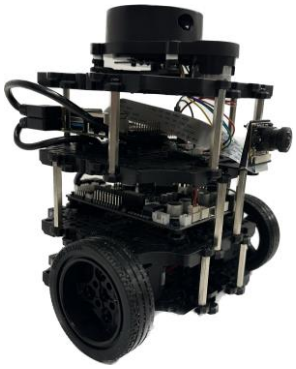

Figure 2. The robot provided to the finalist teams to be used in the final round

The final round took place on November 11, 2022, at NYUAD (see Figure 3 for the final round setup, including the arenas for the robots), with the attendance of four teams (16 students) since one of the finalist teams withdrew from the competition. The robots were collected from the teams one day before the competition and reset by the organizing team to have the final round system and settings. Moreover, an individual Wi-Fi network for each team was set up to prevent any interruptions among the teams while performing their attacks. The finalists had to bring their personal computers to the final round to perform their attacks. The final round took four hours, including 30 minutes for preparation/set up, two and a half hours for competition and judging, and one hour for poster presentations and judges' deliberations. Each team had to make a 10-minute poster presentation to summarize what they intended to do and what they could achieve.

Figure 3. The final round setup, including the different groups and arenas (square boxes) for the robots

The final round consisted of six judges, including one from the organizing team. The other five judges had different backgrounds to cover the robotics, cybersecurity, and construction aspects of the competition. One of the judges was a post-doctoral researcher specializing in robotics, another judge was a cybersecurity research engineer, two were from construction companies based in the UAE, and the fifth judge was a consultant working on forensic technology. The judges determined the winners based on the evaluation criteria explained in the following subsection.

3.3.2 Evaluation Criteria

The evaluation criteria (see [20] for the details) aimed to test the extent to which finalist teams are able to compromise the given system while being creative and thinking outside the box. The criteria were designed in consultation with the researchers from the Center for Cybersecurity (CCS) at NYUAD based on their expertise in the field and experiences in organizing cybersecurity competitions. There were seven criteria totaling 100 points and a bonus of up to 15 points. Therefore, the team scoring the highest out of 115 points (100 + 15) was chosen as the first-place team. The first five criteria were based on the targets that the teams were supposed to achieve during the competition and did not depend on the judges' personal opinions. However, each team was responsible for proving the achieved targets to the judges to receive the corresponding points. Moreover, each of these five criteria had sub-criteria to achieve a more detailed scoring. The teams could have physical access to the robot, Wi-Fi router, and external computer; however, half of the regular score was given if the team achieved a goal by utilizing a physical attack.

The last three criteria, including the bonus points (totaling 40 points), depended on the judges' opinions based on the teams' performances and poster presentations. Therefore, the poster presentations and the teams' ability to explain what they targeted and what they could achieve had an essential role in the final scores. All criteria—without including the sub-criteria—are as follows:

1. Did the team need the Wi-Fi password to proceed with the competition? (10 Points)
2. Is the team able to acquire/access the data collected by the robot and stored in the temporary or final storage? (15 Points)
3. Is the team able to alter/modify the data collected by the robot? (20 Points)
4. Is the team able to alter the predefined path or the functionality (i.e., preventing it from taking images) the robot should follow? (15 points)
5. Is the team able to compromise the availability of the robot? (15 Points)
6. Technical difficulty/sophistication of the utilized

techniques (15 points)
7. Creativity (wow factor) (10 points)
8. Other/bonus points (15 points)

3.3.3 Main Outcomes of the Final Round

During the final round, each team tried to implement their ideas from the qualification round and achieve the targets provided in the list of evaluation criteria by utilizing different techniques. While all the teams achieved some of the targets, others remained unachieved. For example, the first criterion required the teams to proceed with the competition without asking for the Wi-Fi password to achieve the maximum score. If the team asked for a list of possible passwords, they received a partial score. Finally, they did not receive any points if they asked for the correct password. All teams received a partial score for this criterion since all asked for the list of possible passwords. Most of them asked for it after a long duration of trying, utilizing dictionary attacks and brute force attacks. It shows that the level of difficulty for achieving the maximum score for this criterion was too high, considering the resources and time the teams had.

The second and third criteria that required teams to access and alter the collected data (i.e., photos taken by the robot's camera) could not be achieved by any teams. The main reason for this is the long duration spent on the first criterion that delayed the successful completion of the remaining targets. This showed the organizers that reducing the first criterion's difficulty could give the teams more time to spend on the other targets, or the teams would benefit from asking for the list of possible Wi-Fi passwords earlier at the competition. The fourth criterion (i.e., altering the predefined path or functionality) was achieved by two teams; however, both teams could achieve it by having physical access to the robot. For this reason, both teams received half of the standard score for this criterion. The only target fully achieved by all the teams was compromising the availability of the robot (i.e., the fifth criterion). Most teams used deauthentication attacks to disconnect the robot from the network and make it unavailable.

3.4 Results

Five out of six teams that attended the qualification round provided answers to the open-ended questions. These answers were analyzed using the qualitative data analysis software, MAXQDA, to find the most frequently mentioned words and word combinations. The words, such as determiners (e.g., the, this, each), pronouns (e.g., she, they), and auxiliary verbs (e.g., am, is, are) that do not have a contribution in the analysis were removed before analyzing the word frequencies. The result showed that the most commonly used word was "robot" (n=66). Other frequently used words include "attack(s)" (n=60), "access" (n=39), "attacker(s)" (n=28), "data" (n=25), "ROS" (n=20), "master" (n=18), "network" (n=18), and "information" (n=17). None of these words are unexpected, considering the competition's context and the robotic system provided. Some frequently used words, such as "network", "ROS", "authentication" (n=13), "communication" (n=11), "router" (n=11), "sensors" (n=10), and "firmware" (n=10), show the most commonly targeted elements and functionalities of the robotic system by the participants. Besides the individual words, frequently used word combinations were identified as well. The most frequently mentioned ones were "robotic agent" (n=6), "construction site" (n=5), "direct access" (n=5), "information about" (n=5), and "access point" (n=4). Having "construction site" as a commonly used word combination shows that the participants considered the described construction environment while drafting their responses.

The finalist teams included the attacks and techniques they planned to use in their final poster presentations. These attacks and techniques planned to be conducted in the final round were categorized using the CIA Triad, which stands for Confidentiality, Integrity, and Availability [21], based on the security aspect that the attack mainly aims to compromise. Most cyberattacks affect more than one principle of the CIA triad. For this reason, this categorization intends to show the main focus of the attacks rather than covering all the impacted principles. This categorization can be seen as follows:

- **Confidentiality:** Packet sniffing, targeted packet sniffing, brute-force cracking, backdoor attack.
- **Integrity:** Packet modification attack, steganography.
- **Availability:** SYN-ACK flood denial of service (DoS) attack, deauthentication attack, ARP poisoning attack.

The attacks categorized above are mostly generic, not particularly targeting ROS-based systems and robots. Some examples of sophisticated attacks targeting ROS, which were partially presented by a finalist team, were suggested by Dieber et al. [22]. These attacks include the following:

- **Stealth Publisher Attack:** The mode of communication in ROS is based on a publish-subscribe pattern [10]. This attack targets injecting incorrect data into a running ROS application and tricking another ROS node into using the falsified data from this node. The subscriber is isolated from the regular publishers and forced into receiving data from the exploited publisher.
- **Action Person-in-the-Middle Attack:** One of the communication patterns in ROS is actions [10]. ROS actions are used for long-running and preemptable tasks, such as taking a laser scan. This attack utilizes the traditional Person-in-the-Middle attack to compromise ROS actions. The attacker aims to intercept the communication between the action client and the action server to publish malicious messages.

- **Service Isolation Attack:** ROS uses a client-server / request-reply way of communication as well, using services [10]. In this attack, the attacker aims to isolate a ROS service from the rest of the network and call it later for malicious purposes.
- **Malicious Parameter Update Attack:** Parameter API in ROS networks manages global configuration parameters [10]. One of the methods for a ROS node to get a parameter's value is to subscribe to a particular parameter, which requires the node to store the value in a local variable [22]. This attack exploits this method by maliciously updating the parameter value locally and not making any changes in the globally accessible parameter server.

3.5 Contributions to Construction Cybersecurity

The HMR competition is intended to (1) raise awareness about the increasing cybersecurity problems in the construction industry, (2) attract the cybersecurity community's attention to construction, and (3) utilize the cybersecurity skills and knowledge of students to solve construction-related problems while contributing to their learning process.

Considering the feedback from the judges of the competition from the construction industry, they agreed that this event helped point out some of the cybersecurity issues that are not always well-considered (or known) in construction projects. Although it is beyond the scope of this paper to assess the effectiveness of the event in improving cybersecurity awareness in the construction industry in general, it is reasonable to assume that this and future publications related to the competition and future editions of the HMR events will contribute to achieving that goal. Organizing the event as part of the world's most comprehensive student-led cybersecurity event helped achieve the second goal. Even though HILTI organized a construction cybersecurity event in 2022 [23], HMR was the first academic-driven event with the same focus, making it an important milestone in making the construction industry a part of cybersecurity efforts. The event included cybersecurity experts as judges and was prepared in collaboration with the CCS at NYUAD, contributing to the second goal. Finally, the third goal was achieved by challenging the students to tackle real-life cybersecurity issues related to robotics. The robots in the competition used ROS, which is a commonly used middleware suite. It helped students gain knowledge about ROS and discover potential security problems. The feedback from the students also showed that the competition helped them develop their skills and learn more about cybersecurity and robotics.

The research question of this study was "Is it possible to identify cybersecurity vulnerabilities of construction robots through a competition?", as presented at the beginning of the paper. Based on the presented preliminary results from the competition and the feedback from the judges, collaborating cybersecurity experts, and attending students, it is possible to identify such vulnerabilities through a cybersecurity competition, such as HMR, which gathers large groups of people to solve an industry-specific problem. However, there are many areas for improvement and future work to achieve this target, which will happen in the following editions of the event.

4 Conclusions and Future Work

A crucial part of the digital transformation in the construction industry includes using robots to handle repetitive, labor-intensive, time-consuming, or dangerous tasks on construction sites. Even though construction robots are still not ubiquitous in projects, there have been considerable efforts from the industry and academia. Besides the benefits of robotics, such as increased productivity, improved safety, and higher accuracy, cybersecurity concerns are raised by the construction community. To address these concerns, the first student-led and academic-driven cybersecurity competition in the construction context, HMR, was organized by the S.M.A.R.T. Construction Research Group at NYUAD as a part of CSAW'22 MENA. The competition had two rounds, where students were initially challenged to generate ideas to compromise the data and functionality of an autonomous construction progress monitoring robot. The finalist teams chosen based on their answers in the first round were required to implement their ideas on a small-scale robot (i.e., TurtleBot 3 Burger) equipped with a camera that simulates a real progress monitoring robot. This paper presents an overview of the competition, its motivation, and its contributions.

Construction is still not a part of cybersecurity studies, and cybersecurity is still not the focus of construction studies. Therefore, one of the significant contributions of HMR was bringing the attention of the cybersecurity community to the construction sector while raising cybersecurity awareness within the construction community. Since HMR was the first robot hacking competition of CSAW, it also gave students a chance to learn more about robotics and the cybersecurity aspects of robotic platforms and ROS. They were required to think about cybersecurity in the construction context, which offered them an additional perspective.

As a part of future work, this paper will be extended to a journal article to include detailed analyses of the data collected during the competition. The collected data consists of the responses from the participants in the qualification round, the poster presentations (i.e., the content of the poster and the transcription of the presentation), and the responses of the finalist teams to

the follow-up questionnaire. Another significant future work is to improve the competition, considering the lessons learned and areas for improvement—including the suggestions from the finalists—and organize it annually with new challenges and robotic systems. The competition will focus on a different robot every year to draw attention to the cybersecurity aspects of automating different construction tasks.

Acknowledgment

The HMR competition was organized by the S.M.A.R.T. Construction Research Group with the support and collaboration from the Center for Cybersecurity (CCS) at NYUAD and the Center for AI and Robotics (CAIR) at NYUAD, which provided technical and financial support for the event. Special thanks are given to Prof. Ramesh Karri, Prof. Ozgur Sinanoglu, Prof. Mihalis Maniatakos, Prof. Farshad Khorrami, and Dr. Prashanth Krishnamurthy. The organizers of the HMR competition included the authors of this paper and two other researchers from the S.M.A.R.T. Construction Research Group: Xinghui Xu and Dr. Samuel A. Prieto. The authors would also like to thank them for their efforts in organizing the event. Finally, the authors thank all the competitors for their interest and all the judges of HMR—Nader Kayali from Accuracy, Sabyasachi Jana from ALEC, Dr. Daniel Feliu Talegon from Khalifa University, Christoforos Vasilatos from NYUAD's CCS, and Ebrahim Hamed from Aldar—for their valuable contributions to the event.

References

[1] Agarwal R., Chandrasekaran S., and Sridhar M. Imagining construction's digital future. *McKinsey&Company*, (Exhibit 1), 2016.

[2] McKinsey&Company. Highlights from McKinsey's 2021 sector research. 2021.

[3] Prieto S. A., García de Soto B., and Adan A. A Methodology to Monitor Construction Progress Using Autonomous Robots. In *Proceedings of the 37th International Symposium on Automation and Robotics in Construction (ISARC 2020)*, pages 1515-1522, Kitakyushu, Japan, 2020.

[4] Zhang L. *et al.* An autonomous excavator system for material loading tasks. *Science Robotics*, 6(55):3164, 2021.

[5] Xu X., Holgate T., Coban P., and García de Soto B. Implementation of a Robotic System for Overhead Drilling Operations: A Case Study of the Jaibot in the UAE. In *Proceedings of the 38th International Symposium on Automation and Robotics in Construction (ISARC 2021 Online)*, pages 661-668, Dubai, UAE, 2021.

[6] Ciampa E., De Vito L., and Rosaria Pecce M. Practical issues on the use of drones for construction inspections. *Journal of Physics: Conference Series*, 1249(1):12016, 2019.

[7] Watson S. Cyber-security: What will it take for construction to act? *Construction News*. On-line: https://www.constructionnews.co.uk/tech/cyber-security-what-will-it-take-for-construction-to-act-22-01-2018/, Accessed: 07/01/2023.

[8] Andersson J. *et al.* A Security Analysis of Radio Remote Controllers for Industrial Applications. 2019. On-line: https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-radio-remote-controllers.pdf, Accessed: 07/01/2023.

[9] BBC News. Hack attack causes "massive damage" at steel works. *BBC News*. On-line: https://www.bbc.com/news/technology-30575104, Accessed: 17/03/2023.

[10] Zhu Q., Rass S., Dieber B., and Mayoral-Vilches V. Cybersecurity in Robotics: Challenges, Quantitative Modeling, and Practice. *Foundations and Trends in Robotics*, 9(1):1–129, 2021.

[11] Salami Pargoo N. and Ilbeigi M. A Scoping Review for Cybersecurity in the Construction Industry. *Journal of Management in Engineering*, 39(2):3122003, 2023.

[12] Zheng R., Jiang J., Hao X., Ren W., Xiong F., and Zhu T. CaACBIM: A context-aware access control model for BIM. *Information*, 10(2):47, 2019.

[13] Boyes H. Security, Privacy, and the Built Environment. *IT Professional*, 17:25–31, 2015.

[14] Sonkor M. S. and García de Soto B. Operational Technology on Construction Sites: A Review from the Cybersecurity Perspective. *Journal of Construction Engineering and Management*, 147(12):4021172, 2021.

[15] Prior G. Interserve hit with £4.4m fine after cyber attack. *Construction Enquirer*. On-line: https://www.constructionenquirer.com/2022/10/24/interserve-hit-with-4-4m-fine-after-cyber-attack/, Accessed: 05/01/2023.

[16] García de Soto B., Turk Ž., Maciel A., Mantha B. R. K., Georgescu A., and Sonkor M. S. Understanding the Significance of Cybersecurity in the Construction Industry: Survey Findings. *Journal of Construction Engineering and Management*, 148(9):4022095, 2022.

[17] Sonkor M. S., Xu X., Prieto S. A., and García de Soto B. Vulnerability Assessment of Construction Equipment: An Example for an Autonomous Site Monitoring System. In *Proceedings of the 39th International Symposium on Automation and Robotics in Construction (ISARC 2022)*, pages 283-290, Bogotá, Colombia, 2022.

[18] Quigley M. *et al.* ROS: an open-source Robot Operating System. In *ICRA workshop on open source software*, 3(3.2), 2009.

[19] Mayoral-Vilches V., White R., Caiazza G., and Arguedas M. SROS2: Usable Cyber Security Tools for ROS 2. In *2022 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, pages 11253–11259, Kyoto, Japan, 2022.

[20] S.M.A.R.T. Construction Research Group. Hack My Robot. *GitHub*. On-line: https://github.com/SMART-NYUAD/hack_my_robot/tree/hmr_2022, Accessed: 07/01/2023.

[21] ISO/IEC. ISO/IEC 27001:2013 - Information technology - Security techniques -Information security management systems - Requirements. 2013. On-line: https://www.iso.org/standard/54534.html, Accessed: 17/03/2023.

[22] Dieber B. *et al.* Penetration Testing ROS in *Robot Operating System (ROS) - The Complete Reference (Volume 4)*, 183–225, A. Koubaa, Ed. Springer International Publishing, Cham, 2020.

[23] HILTI. Hilti IT Competition 2022. *HILTI*. On-line: https://itcompetition.hilti.group/2022/index.html, Accessed: 20/03/2023.