Cyber Funfair: Creating Immersive & Educational Experiences for Teaching Cyber Physical Systems Security

Alan Mills
alan.mills@uwe.ac.uk
University of the West of England
Bristol, UK

Jonathan White
jonathan6.white@uwe.ac.uk
University of the West of England
Bristol, UK

Phil Legg
phil.legg@uwe.ac.uk
University of the West of England
Bristol, UK

ABSTRACT

Delivering meaningful & inspiring cyber security education for younger audiences can often be a challenge due to limited expertise & resources. Key to any outreach activity is that it both develops a learner's curiosity, as well as providing educational objectives. To address this need, we developed a novel learning & awareness activity that addresses the Cyber Physical Systems (CPS) Security knowledge area as mapped by the Cyber Security Body of Knowledge (CyBOK). At the core of our activity is the integration of the Raspberry Pi device with LEGO SPIKE kits. LEGO SPIKE is part of the LEGO Education system that combines colourful LEGO building blocks with motors & sensors, creating an adaptable & engaging learning environment. This hands-on approach allows participants to witness the tangible consequences of cyber & network actions in a physical & engaging format. To evaluate the effectiveness of the activity, we used the activity as part of an outreach activity day attended by approximately 300 students aged between 12-14 from schools across the West of England. Participants of the activity were surveyed & the results showed an increase in understanding of CPS specific & wider cyber security for over 90% of respondents. Activity engagement was also well received with no negative feedback. We report on our survey findings & discuss best practices to support other practitioners in developing hands-on interactive experiences for engaging & educational cyber security activities.

CCS CONCEPTS

• Applied computing → Interactive learning environments; **• Computer systems organisation → Sensors and actuators**; **• Security and privacy → Systems security**.

KEYWORDS

Cyber security education, Cyber physical systems

ACM Reference Format:
Alan Mills, Jonathan White, and Phil Legg. . Cyber Funfair: Creating Immersive & Educational Experiences for Teaching Cyber Physical Systems Security. In *Proceedings of* . ACM, New York, NY, USA, 6 pages.

1 INTRODUCTION

A recent report by the UK government's Department for Science Innovation & Technology (DSIT) [1] has highlighted that approximately 50% of businesses currently face a skills gap for basic cyber security, as defined in the Cyber Essentials scheme [6]. Cyber security education is key to increasing the future talent pool to address this shortage. While upskilling & bootcamps are targeted at existing workforces to bridge the skills gap, it is equally important that future generations receive adequate education & training in cyber security to prevent a stagnation or contraction of the talent pool. A significant challenge in this regard is ensuring that middle & high school students are not only aware of cyber security but are also actively engaged in it. By targeting students at a middle & high school level, we can sustain the pipeline of students who will pursue higher education within cyber security.

Unlock Cyber is a regional consortium across the West of England that is supported by the National Cyber Security Centre (NCSC) [7]. It brings together cyber representatives from employers, professional bodies, delivery partners, education providers & academia. The consortium aims to raise awareness of cyber security, excite & engage young people about cyber, & to showcase the opportunities that exist for young people on local & national levels [3]. Since 2018, Unlock Cyber have hosted an annual cyber taster day at the University of the West of England in Bristol, UK. It is attended by approximately 300 students aged between 12-14 from schools across the West of England region. The most recent event in June 2023 was supported by 12 industry partners & reached over 20 regional schools. During the day, students rotate around a set of 40-minute workshops. The workshops cover a variety of cyber security topics such as Capture The Flag (CTF) challenges, social engineering, & networking concepts.

Our objective was to provide an engaging, hands-on activity that actively involved school-aged students in the learning process & to continue our outreach work with regional schools. A key element of our activity was the use of LEGO SPIKE [5], part of the LEGO Education system that combines colourful LEGO building blocks with motors & sensors, creating an adaptable & engaging learning environment. For the activity, we combined LEGO SPIKE with Raspberry Pi's, creating Cyber Physical Systems (CPS) that serve as both demonstration & educational tools. These systems illustrate the real-world impact of cyber attacks on physical infrastructure. This cyber security education initiative aimed to inspire students to explore this field further, ultimately hoping to address the digital skills gap. It also raises awareness of broader resources, including the Cyber Security Body of Knowledge (CyBoK) [4]. Importantly, all resources used during this activity; image files, code, documentation, & teaching material, are publicly accessible. This enables teachers to adapt & reuse the activity within their schools, extending the reach of this educational aide beyond the event itself.

In this paper, we detail the process of developing a CPS for cyber security education, balancing the need for an engaging environment that also encourages deeper learning & awareness of wider

,
.

cyber security knowledge bases. We report on initial results & observations of running the activity, discuss lessons learnt & propose possible improvements & future work.

2 RELATED WORK

Pencheva et al.[8] used discussion groups with teachers to explore the integration of cyber security concepts in classrooms, as well as strategies for enhancing student engagement while teaching cyber security. Their findings highlighted the importance of raising awareness among students & parents about the various prospects that cyber security careers offer. Additionally, the study emphasised the need to provide teachers with proper support in implementing practice-based learning approaches in their classrooms. Ensuring that teachers feel confident in leading these classes is crucial, with a key component in assuring their confidence being that practical demonstrations run smoothly from the outset to prevent student disengagement. Rahman et al. [9] highlight the challenges associated with cyber security education, including a lack of both expertise & resources. They also acknowledge that this issue is further impacted by the continually evolving nature of this area, with the "latest" technology often changing, making it harder for teachers to keep pace. Crick et al. [2] also underscore the challenges associated with teaching Cyber Security at the university level in the UK. Their findings reveal that several challenges stem from the need for current & practical learning methods that can inspire & captivate students. They stress the importance of effectively conveying the significance of cyber security within both academic & broader organisational contexts. Additionally they highlight the challenges that educators face in staying up to date with the ever changing cyber security field, mirroring the themes found in other research works.

In our previous works [10], we emphasise the importance of making CPS security engaging & interactive utilising a slot-car race track to create a self contained & novel CPS which presented students with a CTF style challenge. While the work highlights the engagement & potential use case for other educators that such a novel system presents, the system itself was not a typical CPS, with the cyber elements having no physical impact. The findings of our earlier study also only presented observational feedback. In this work, we now look to improve on this with a new CPS system which shows a physical impact on the running CPS of cyber attacks & utilised a survey to produce results around engagement & improved understanding within targeted areas.

3 SYSTEM DESIGN

In this section we outline the system components, discuss the high level design choices & describe in detail the functionality of both the CPS & UI created for the activity.

3.1 System Overview

The main components were two Raspberry Pi's; funfair rides, created from the LEGO SPIKE kit (hereafter referred to as "LEGO rides"); & laptops, as shown in Figure 1. Each LEGO ride was powered by a single LEGO motor. A LED matrix was utilised as part of one attack scenario to help maintain a degree of novelty, interest & differentiation.

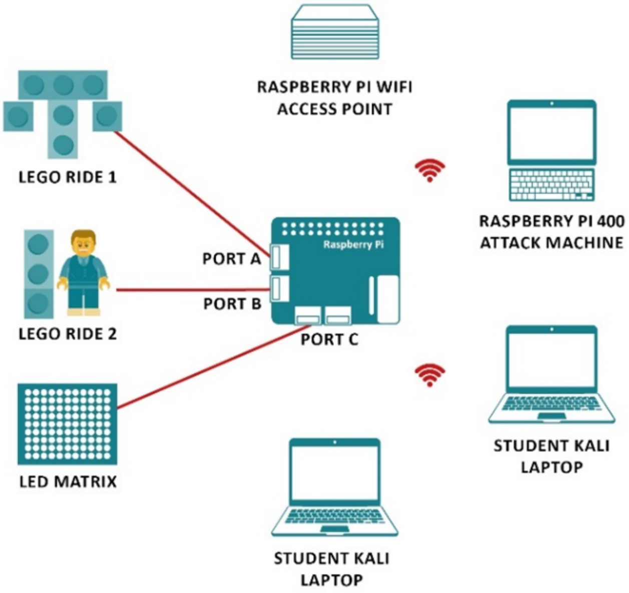


Figure 1: System setup

One Raspberry Pi would have a Build HAT attached & would be used to control the LEGO motors & LED matrix. This was our Cyber Physical System (CPS). The CPS was designed to run each motor as part of a separate "kit". As such two student laptops could be utilised allowing one system to run the attacks on different LEGO rides in parallel. For example one group of students could be engaged in one attack scenario against "kit" A (the LEGO ride connected to port A), whilst a second group could be running a different attack scenario against "kit" B (the LEGO ride connected to port B).

Each student laptop runs a custom-built UI, along with Wireshark so that students can analyse the attacks. By using hints provided in the UI & the traffic analysis tools, students can learn about the possible attacks & observe their effect on the specific LEGO ride to improve their understanding. A separate attack machine (Pi 400) was used to launch & control the attacks against the CPS. This machine was used to SSH onto the student laptops & run the attack scripts from there. By using a separate attack machine (connected via SSH) we were able to remove any breaks or flow in the immersion of the attack scenarios for the students.

A Wireless Local-Area Network (WLAN) access point was created using a Raspberry Pi 3b, serving as the central hub that all other machines connect to. We use a Raspberry Pi for this so that the access point configuration can be pre-configured & imaged to an SD card for quick deployment.

The system was designed to allow remote access & control of the attacks by supporting personnel, while minimising any breaks in immersion from the student perspective. By utilising a separate WLAN we remove any potential interference that other devices might cause, "polluting" the traffic captures & causing confusion for the students. Logical separation of the ports into different "kits" allowed us to maximise the use case for a single LEGO SPIKE kit & provides simultaneous activity for different groups of students.

The bespoke CPS server & UI provide "out of the box" solutions for educators who may not be experts within the field of cyber security or CPS. The UI specifically provides all the required background information & resources that would be required to run the activity, while the pre-built CPS means that the more technical aspects of the activity can be setup as a simple "plug & play" by following the provided documentation.

3.2 CPS - Pi Server

The Pi server was fitted with a Raspberry Pi Build HAT which allows for control of up to four LEGO motors & sensors. The motors are connected to ports A & B while the LED matrix is connected to port C. Figure 2 shows a CPS setup example with connected LEGO motor(s) + LED matrix.

A Python script launches on startup that controls the CPS functionality. The script launches multiple UDP servers & a single TCP server. The UDP servers are used to manage the attacks. Each listening port on the server is associated with a specific motor & attack. The TCP server (port 4242) was used as a "C2" for control commands & countermeasures.

The UDP servers listened on the following ports:

- Motor A
  - 4444 - Denial of Service (DoS) attack
  - 5555 - Man in the Middle (MitM) attack
  - 6666 - Code injection attack
- Motor B
  - 7777 - Denial of Service (DoS) attack
  - 8888 - Man in the Middle (MitM) attack
  - 9999 - Code injection attack

With this method, scenario management is simplified. A single system is able to run different attacks in parallel, minimising interference between the two motors (or "kits"), allowing traffic analysis to be filtered on port ranges if required.

3.3 CPS - Attack Client

The attack client, designed as a simple menu-based Command Line Interface (CLI) script was executed on the student laptops. The scripts are remotely controlled from a separate attacking machine via SSH. By loading the attack client onto the student laptops, students could observe the traffic generated from their machines, while remote control & execution ensured a seamless experience without interruptions. Since a single system is able to operate two kits, using two student laptops, this necessitated two distinct SSH sessions concurrently, as illustrated in Figure 3.

The attack client initially requires the facilitator to select a kit (A or B), following which it presents a simple options menu. The menu enables the selection of the different attack, DoS, MitM or code injection. When an attack commences, the script sends "idle" traffic to establish a baseline of normal network activity. Subsequently the attack is manually activated & deactivated where students can observe the change in traffic patterns & physical behaviour of the system. On completion of an attack, the prompt reverts to the main menu.

Two additional options were also present:

- Stop - Used to manually stop the associated motor & clear the LED matrix
- Flush - Used to flush the CPS Pi server iptables rules

As the countermeasures deployed would use iptables on the CPS Pi server the flush command was required to ensure that attacks could be re-run. If not flushed then attacks would "fail" to run from the start as the attacking IP would be blocked in advance.

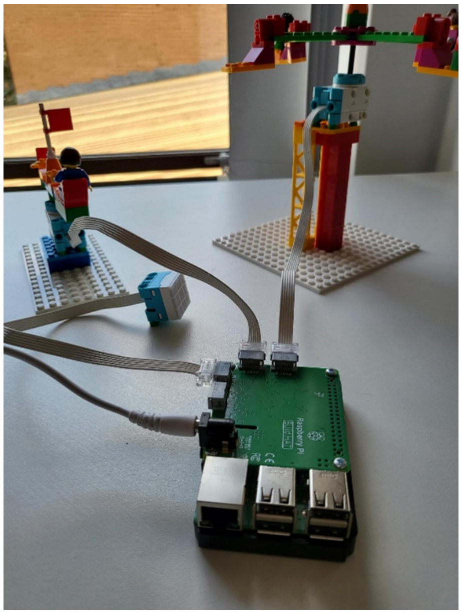
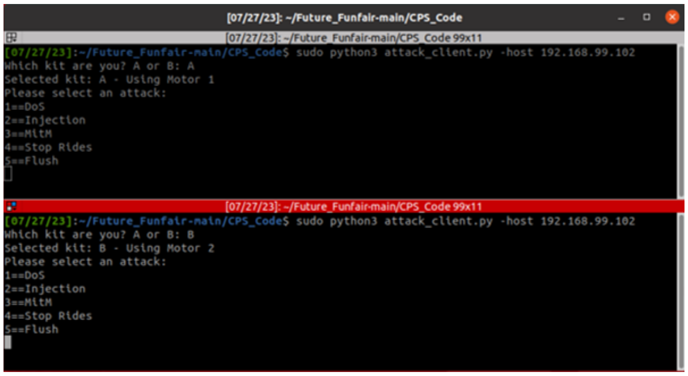


Figure 2: System setup - Example



[07/27/23]: ~/Future_Funfair-main/CPS_Code
[07/27/23]: ~/Future_Funfair-main/CPS_Code 99x11
[07/27/23]: ~/Future_Funfair-main/CPS_Code 99x11

```
[07/27/23]:~/Future_Funfair-main/CPS_Code$ sudo python3 attack_client.py -host 192.168.99.102
Which kit are you? A or B: A
Selected kit: A - Using Motor 1
Please select an attack:
1==DoS
2==Injection
3==MitM
4==Stop Rides
5==Flush
```

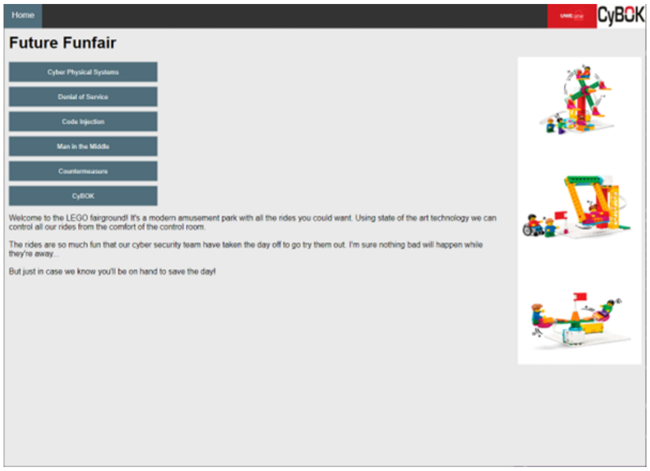
```
[07/27/23]:~/Future_Funfair-main/CPS_Code$ sudo python3 attack_client.py -host 192.168.99.102
Which kit are you? A or B: B
Selected kit: B - Using Motor 2
Please select an attack:
1==DoS
2==Injection
3==MitM
4==Stop Rides
5==Flush
```

Figure 3: Attack Client - CLI

3.4 UI

The UI developed for the activity offers information about the attacks, countermeasures, & background details on both CPS & the CyBOK. The UI is served from a Python http.server. As the activity operates within the WLAN without external internet access, all necessary materials & resources are hosted locally.

Figure 4 displays the initial splash page which provides a brief introduction to the scenario & then facilitates navigation to more in-depth pages.



Future Funfair

Welcome to the LEGO fairground! It's a modern amusement park with all the rides you could want. Using state of the art technology we can control all our rides from the comfort of the control room.

The rides are so much fun that our cyber security team have taken the day off to go try them out. I'm sure nothing bad will happen while they're away...

But just in case we know you'll be on hand to save the day!

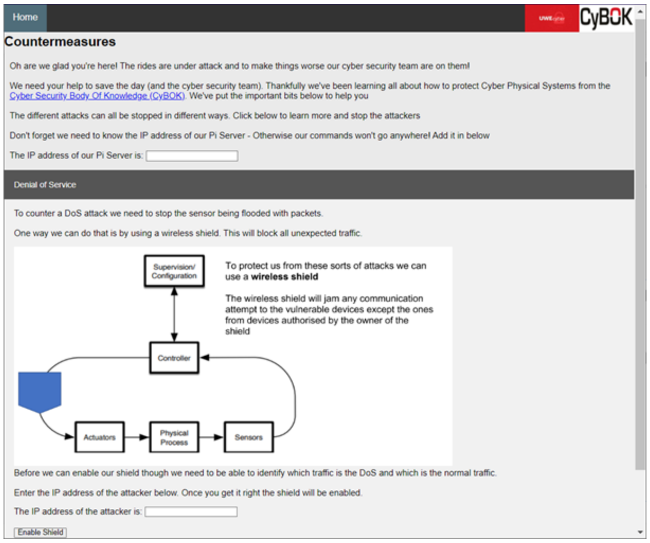
Figure 4: System setup

The countermeasures used to mitigate the attacks are launched through the UI. This approach ensured that students engaged with the UI during the activity, making it a valuable resource for information, not only about the specific attacks, but also for a broader understanding of CPS & CyBOK.

3.4.1 CPS & CyBOK. The CPS & CyBOK sections of the user interface were designed to provide foundational information for students with little to no prior knowledge of these subjects. The CPS page explained the concept of Cyber Physical Systems, contextualising it within the funfair scenario used in the activity. The CyBOK page acknowledged the CyBOK as the principal reference for all material within the UI, including links to local resources derived from the CyBOK documentation. These resources were intended to enrich the activity & deepen the student's understanding of both CPS & network security.

3.4.2 Attacks. In the Attacks section, each page detailed the indicators of a specific attack & provided context specific information about where within a CPS this attack normally occurred. The terminology, sourced directly from the CyBOK (e.g. actuators), was used & explained in relation to our system setup, such as equating actuators with motors.

3.4.3 Countermeasures. The Countermeasures section was where the students could actively engage in mitigating the ongoing attacks. Each attack had a corresponding countermeasure, employing terminology & strategies directly from the CyBOK. Figure 5 illustrates the countermeasures page, highlighting the DoS countermeasure & an introduction section that underscores the CyBOK as the key reference for all included material.



Countermeasures

Oh are we glad you're here! The rides are under attack and to make things worse our cyber security team are on them!

We need your help to save the day (and the cyber security team). Thankfully we've been learning all about how to protect Cyber Physical Systems from the Cyber Security Body Of Knowledge (CyBOK). We've put the important bits below to help you

The different attacks can all be stopped in different ways. Click below to learn more and stop the attackers

Don't forget we need to know the IP address of our Pi Server - Otherwise our commands won't go anywhere! Add it in below

The IP address of our Pi Server is: □

Denial of Service

To counter a DoS attack we need to stop the sensor being flooded with packets.

One way we can do that is by using a wireless shield. This will block all unexpected traffic.

To protect us from these sorts of attacks we can use a **wireless shield**

The wireless shield will jam any communication attempt to the vulnerable devices except the ones from devices authorised by the owner of the shield

Before we can enable our shield though we need to be able to identify which traffic is the DoS and which is the normal traffic.

Enter the IP address of the attacker below. Once you get it right the shield will be enabled.

The IP address of the attacker is: □

Figure 5: Countermeasures - DoS

To enable a countermeasure, students first had to identify the attacking IP address. IP validation was performed on the client side to prevent incorrect IP address entry. Once the attacking IP address was accurately identified, the mitigation strategy was enabled. The countermeasures page used the "C2" port (TCP, 4242) to execute commands on the CPS Pi server. Internally, this process invoked simple iptables rules to block the attacking IP address.

4 ACTIVITY

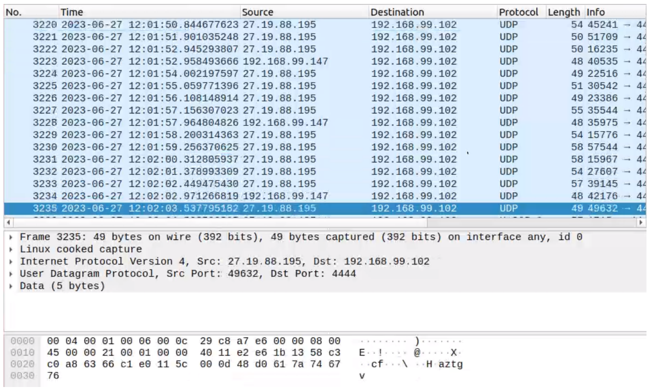
The activity was designed to introduce students to the CyBOK & CPS security. Designed for an in-person delivery, all three attack types were aimed to be completed within 30 to 40 minutes. Students were organised into teams & assigned a specific kit. Prior to initiating any attacks, students were introduced to the UI & Wireshark, a network protocol analyser. The facilitator managing each kit would first familiarise the students with the UI & assess their pre-existing knowledge of CPS & cyber security before launching the attacks.

During the initial phase each of attack, "idle" traffic was generated to establish a baseline for normal network activity & expected behaviour of the target CPS (in this case, the LEGO ride). Once the attack commenced, students were encouraged to use both network traffic analysis & the observable changes in the CPS behaviour to investigate & understand the nature of the ongoing attack. They were expected to identify key elements such as the attacker's IP address & the attack's profile. For instance, in the DoS attack, a substantial amount of "junk" traffic from a single IP address overwhelmed the CPS, as depicted in Figure 6. This onslaught of traffic led to erratic behaviour in the LEGO ride, where normal operational commands could not be processed, resulting in the ride stopping & moving in a jerky manner.

Students with limited knowledge or prior experience were encouraged to use the information available within the UI to determine which of the three potential attacks was being executed. Once

Questions \ Responses	Strongly Disagree	Disagree	Neither	Agree	Strongly Agree
It was engaging			10	53	22
I learnt how cyber attacks can impact the physical world		1	6	42	36
I understand more about what a Cyber Physical System is now		1	7	45	32
I learnt more about the CyBOK		5	12	42	25
I would do this again	1	1	14	46	21
I learnt more about cyber security		2	3	37	42

Table 1: Survey Results



```
No.   Time                          Source          Destination     Protocol Length Info
 3220 2023-06-27 12:01:50.844677623 27.19.88.195    192.168.99.102  UDP      54 45241 → 44
 3221 2023-06-27 12:01:51.901035248 27.19.88.195    192.168.99.102  UDP      50 51709 → 44
 3222 2023-06-27 12:01:52.945293807 27.19.88.195    192.168.99.102  UDP      50 16235 → 44
 3223 2023-06-27 12:01:52.958493666 192.168.99.147  192.168.99.102  UDP      48 40535 → 44
 3224 2023-06-27 12:01:54.002197597 27.19.88.195    192.168.99.102  UDP      49 22516 → 44
 3225 2023-06-27 12:01:55.059771396 27.19.88.195    192.168.99.102  UDP      51 30542 → 44
 3226 2023-06-27 12:01:56.108148914 27.19.88.195    192.168.99.102  UDP      49 23386 → 44
 3227 2023-06-27 12:01:57.156307023 27.19.88.195    192.168.99.102  UDP      55 35544 → 44
 3228 2023-06-27 12:01:57.964804826 192.168.99.147  192.168.99.102  UDP      48 35975 → 44
 3229 2023-06-27 12:01:58.200314363 27.19.88.195    192.168.99.102  UDP      54 15776 → 44
 3230 2023-06-27 12:01:59.256370625 27.19.88.195    192.168.99.102  UDP      58 57544 → 44
 3231 2023-06-27 12:02:00.312805937 27.19.88.195    192.168.99.102  UDP      58 15967 → 44
 3232 2023-06-27 12:02:01.378993309 27.19.88.195    192.168.99.102  UDP      54 27607 → 44
 3233 2023-06-27 12:02:02.449475430 27.19.88.195    192.168.99.102  UDP      57 39145 → 44
 3234 2023-06-27 12:02:02.971266819 192.168.99.147  192.168.99.102  UDP      48 42176 → 44
 3235 2023-06-27 12:02:03.537795182 27.19.88.195    192.168.99.102  UDP      49 49632 → 44

▸ Frame 3235: 49 bytes on wire (392 bits), 49 bytes captured (392 bits) on interface any, id 0
▸ Linux cooked capture
▸ Internet Protocol Version 4, Src: 27.19.88.195, Dst: 192.168.99.102
▸ User Datagram Protocol, Src Port: 49632, Dst Port: 4444
▸ Data (5 bytes)

0000  00 04 00 01 00 06 00 0c  29 c8 a7 e6 00 00 08 00   ········ )·······
0010  45 00 00 21 00 01 00 00  40 11 e2 e6 1b 13 58 c3   E··!···· @·····X·
0020  c0 a8 63 66 c1 e0 11 5c  00 0d 48 d0 61 7a 74 67   ··cf···\ ··H·aztg
0030  76                                                 v
```

Figure 6: Network traffic capture during a DoS attack; junk traffic (27.19.88.195), legitimate traffic (192.168.99.147) & target CPS (192.168.99.102)

the students understood the nature of the attack & its key characteristics, they would use the UI to implement a corresponding countermeasure. Each of the three countermeasures, one for each type of attack, required both the CPS IP & the correct attacker IP for it to be "enabled".

Upon successful deployment of a countermeasure, the LEGO ride would resume normal operation. While the attack traffic could still be observed through Wireshark, the LEGO ride would no longer be adversely affected & would visibly return to normal operation. This allowed, & invited discussion about the countermeasure & its effectiveness.

With time permitting, students would engage with all three attacks, discussing the various attack profiles & countermeasures. The UI served as a guide throughout the activity offering insights into the attacks & countermeasures. Students were also encouraged to discuss the broader aspects of CPS security, their comprehension of the CyBOK, & the related reference materials. On conclusion of the activity, the students were invited to participate in an anonymous survey designed to gauge both their engagement with the activity, & the educational outcomes.

4.1 Survey Results

Table 1 presents the survey results from the conducted activity. Predominantly, students found the activity engaging & beneficial for enhancing their understanding of both CPS security & the CyBOK.

A notable point of interest is that the repeatability of the activity received a comparatively lower rating despite predominantly positive or neutral views on the activity's engagement level. Another area that received negative feedback was students increased understanding of the CyBOK.

Approximately 85% of participants completed a survey, though some surveys were missing responses to specific questions, resulting in inconsistencies in the numbers of respondents for some questions.

Additional comments were provided by some students. These were largely positive, with remarks such as "useful to learn", "very good experience" & "great session jam packed with exciting information". However not all comments were positive; one student queried "What is CyBOK?".

It is important to note that five surveys with uniform "Agree" responses, & four with "Strong Agree" for all questions were excluded from the results. The rationale behind this exclusion is that surveys with a single type of response across all questions might not accurately reflect student's genuine experiences, but rather represent perfunctory participation. The exclusion of this data which aims to ensure that only reliable responses are presented, primarily affects the positive feedback, which still remains overwhelmingly higher than neutral or negative feedback.

5 DISCUSSION

The survey results indicate that overall the activity was engaging & helped further understanding for CPS security, wider cyber security & the CyBOK. Table 2 shows the split of responses between negative, neutral, & positive as a percentage of the number of responses per question. The lowest positive response was 80% ("I learnt more about the CyBOK") whilst the highest was 94% ("I learnt more about cyber security").

Questions \ Responses	Negative	Neutral	Positive
It was engaging		12%	88%
I learnt how cyber attacks can impact the physical world	1%	7%	92%
I understand more about what a Cyber Physical System is now	1%	8%	91%
I learnt more about the CyBOK	6%	14%	80%
I would do this again	2%	17%	81%
I learnt more about cyber security	2%	4%	94%

Table 2: Survey Responses - By Percentage

Viewed as percentages it is clear that the activity had an overall positive impact with no negative views on the engagement at all. Improved understanding of both CPS & wider cyber security was clear, with over 90% of responses for these questions being positive.

The area with the highest negative response was around wider CyBOK education. Given that the primary focus of the activity was to engage students in CPS security & providing them with relevant information, it is likely that the references & acknowledgements to the CyBOK were in some cases insufficient to provide significant understanding & context of the wider CyBOK. Observations during the activity showed student focus was predominantly split between the LEGO rides & the network traces. While the UI was utilised by the students to complete the activity, students showed limited independent exploration of the UI & its resources, often requiring prompting. Future iterations of both the UI & the activity could aim to address this, however care needs to be taken to ensure that other areas or aspects are not negatively impacted by adding more focus to the wider CyBOK.

The repeatability of the activity received the highest neutral responses & significantly lower positive response rate compared to the activity's overall engagement. This indicates that while the activity was itself engaging, it had limited repeatability. Such a finding is not unexpected given that the activity is limited to three attacks, all of which are showcased & fully explained as part of the activity. While there would be some novelty to repeating the activity with different configurations of the physical LEGO rides, the fundamental attack profile & network traffic would remain consistent. Potential strategies for improving activity's repeatability are discussed in the following section.

6 CONCLUSIONS & FUTURE WORK

Using the LEGO rides as examples of CPS effectively demonstrated the impact that cyber attacks have on the physical world, "bringing to life" CPS security as a subject. The survey results show that over 90% of all responses relating to CPS security & wider cyber security indicated an increase of student learning as a result of the activity. Knowledge of the CyBOK was also overall improved, with 80% of responses showing that students gained more understanding of the wider CyBOK.

The combination of observing the LEGO rides behaviour & analysing network traffic provided context for each attack. The UI provided important in framing the context of the attacks & explaining the attack profiles & countermeasures. Moving from theoretical to practical demonstration in teaching this subject has helped to engage the students in the activity, as reflected by the absence of negative feedback regarding the activity's engagement. This engagement could be utilised to introduce students to the CyBOK, both as the predominate source of reference material used during the activity, & as a wider body of knowledge for cyber security.

One area of improvement is the need to to better assess & record students' awareness & knowledge of key areas such as CPS security & the CyBOK, both before & after the activity. Currently the survey is only conducted after the activity, & therefore students who already had significant pre-existing knowledge of both subjects would be unlikely to have learnt more during the activity, potentially contributing to some neutral or negative feedback. An assessment of student understanding before & after the activity could be a more effective measurement, replacing the current survey methodology. This approach was considered beyond the scope for this project, but could be considered by other educators. Careful design of such an assessment is important, especially if metrics like engagement are being measured.

Feedback also suggests that while the activity is engaging, its repeatability is limited. Introducing a wider array of attack scenarios & more fine tuned control over the existing attacks could improve the repeatability of the activity. This could include changes to the attack timings & introducing incremental speed changes (increase / decrease) adding a layer of challenge as students try to identify & mitigate the attack before it gets "worse".

Efforts have been made to make as much of the activity & its resources publicly available as possible, including tailored videos of each attack for schools without access to the necessary LEGO kits & Raspberry Pis. However, it is acknowledged that a key part of the success of this activity was its interactive & physical nature. While video demonstrations can convey the attack behaviour & its impacts, it likely does not offer the same level of "engagement". We continue to work with schools in the region to enable them to showcase the physical nature of this activity for their students.

The code for the CPS (server + attack client) & UI have been made available at https://github.com/uwe-cyber/Future_Funfair. The Raspberry Pi images for both the CPS server & WLAN access point, as well as associated documentation have been made available at https://uwe-cyber.github.io/lego_funfair/. We encourage practitioners & teachers to utilise the source code, & we would welcome feedback on how this activity is being used in educational practice.

ACKNOWLEDGMENTS

We would like to thank the CyBOK (Cyber Security Body of Knowledge) project & the UK National Cyber Security Centre (NCSC) for funding this work.

REFERENCES

[1] Steve Coutinho, Alex Bollen, Claire Weil, Chloe Sheerin, Dejon Silvera, Sam Donaldson, and Jade Rosborough. 2023. *Cyber security skills in the UK labour market 2023*. Technical Report. Department for Science, Innovation & Technology. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1173325/Cyber_security_skills_in_the_UK_labour_market_2023.pdf

[2] Tom Crick, James H. Davenport, Paul Hanna, Alastair Irons, and Tom Prickett. 2020. Overcoming the Challenges of Teaching Cybersecurity in UK Computer Science Degree Programmes. In *2020 IEEE Frontiers in Education Conference (FIE)*. IEEE, 1–9. https://doi.org/10.1109/FIE44824.2020.9274033

[3] Unlock Cyber. 2023. *Success Story*. Retrieved July 27, 2023 from https://www.unlockcyber.com/mission/

[4] CyBOK. 2023. *CyBOK - Cyber Security Body Of Knowledge*. Retrieved July 27, 2023 from https://www.cybok.org/

[5] LEGO Education. 2023. *LEGO Education SPIKE*. Retrieved July 27, 2023 from https://spike.legoeducation.com/#/

[6] NCSC. 2023. *About Cyber Essentials - NCSC.GOV.UK*. Retrieved July 27, 2023 from https://www.ncsc.gov.uk/cyberessentials/overview

[7] NCSC. 2023. *What we do - NCSC.GOV.UK*. Retrieved July 27, 2023 from https://www.ncsc.gov.uk/section/about-ncsc/what-we-do

[8] Denny Pencheva, Joseph Hallett, and Awais Rashid. 2020. Bringing Cyber to School: Integrating Cybersecurity Into Secondary School Education. *IEEE Security & Privacy* 18, 2 (2020), 68–74. https://doi.org/10.1109/MSEC.2020.2969409

[9] Nurul Amirah Abdul Rahman, Izzah Hanis Sairi, Nurul Akma M Zizi, and Fariza Khalid. 2020. The importance of cybersecurity education in school. *International Journal of Information and Education Technology* 10, 5 (2020), 378–382.

[10] Jonathan White, Phil Legg, and Alan Mills. 2023. Interactive Cyber-Physical System Hacking: Engaging Students Early Using Scalextric. In *Journal of The Colloquium for Information Systems Security Education*, Vol. 10. 6–6.