# “Hacking an IoT Home”: New opportunities for cyber security education combining remote learning with cyber-physical systems

Phil Legg, Thomas Higgs, Pennie Spruhan, Jonathan White and Ian Johnson
Computer Science Research Centre, University of the West of England, Bristol, UK
Email: Phil.Legg@uwe.ac.uk

***Abstract*—In March 2020, the COVID-19 pandemic led to a dramatic shift in educational practice, whereby home-schooling and remote working became the norm. Many typical schools outreach projects to encourage uptake of learning cyber security skills therefore were put on hold, due to the inability to physical attend and inspire. In this short paper, we describe a new approach to teaching cyber security with a view of inspiring a new generation of learners to the subject. Traditional Capture-The-Flag exercises are widely used in cyber security education, whereby a series of challenges are completed to gain access and obtain a passphrase from a computer system. We couple this approach with interactive sessions made possible via video conferencing platforms such as Microsoft Teams and Zoom, along with the very nature of being in the home environment, where home IoT devices are now commonplace. We develop an integrated CTF for the home IoT environment, where students can observe the impact of submitting flags via online video, to physical adjust the home environment - ranging from switching off lights, playing music, or controlling an IoT-enabled robot. The result is a highly interactive and engaging experience that benefits from the very nature of remote working, inspiring the notion of “hacking an IoT home”.**

## I. Introduction

Cyber security is concerned with the protection of systems and their data. Technological advances, such as IoT, smartphones and cloud computing, and the ways in which society and business utilise this technology through Internet connectivity means that how we protect such systems and their data continues to adapt.

The COVID-19 pandemic brought an unprecedented shift to online learning for many education institutions across the globe. In the UK, government ordered schools and universities to rapidly move to remote online delivery of lectures and classes, causing a sudden uptake of online video conferencing platforms such as Microsoft Teams and Zoom. Prior to lockdown, our team had developed outreach projects on cyber-physical systems that we had taken to a number of regional schools. Figure 1 shows our Scalextric challenge, where students have to brute force their way in to the scoreboard system, to compromise the lap counter sensor to change how the scores increment, and also aim to reset the opposition’s score. The use of physical kit for teaching cyber security concepts proved to create a high energy session for students to enjoy and learn from. The introduction of the UK lockdown inevitably caused a number of our outreach initiatives to be postponed, due to the requirement of physically attending a school to deliver practical sessions. We wanted to explore how we could continue to provide outreach experiences for schools and colleges, despite the shift to remote online learning.

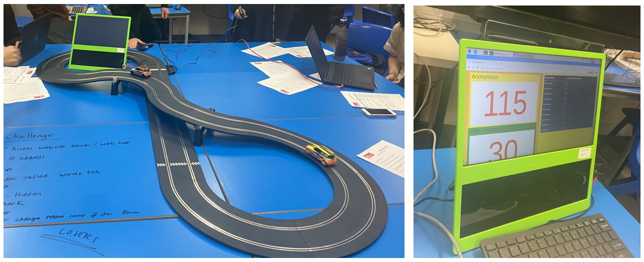


Fig. 1. Scalextric outreach project where students would hack the scoreboard system to modifying the lap counter sensor and reset the opponent’s score.

In this short paper, we explore new opportunities for cyber security education, reflecting on the experience of the UK lockdown. Physical locality should not be a barrier for cyber security education. Furthermore, cyber security is by its very nature, a subject that could potentially see benefit from remote teaching, due to the inherent remote operations that may be used to compromise systems (rather than specifically having physical access to systems). How then, can education providers thrive under these imposed conditions, and furthermore, are these aspects of teaching that may mean we change our practice going forward? We describe an approach that we have adopted for schools outreach, that explores the integration of IoT remote access and control with Capture-The-Flag (CTF) exercises for teaching cyber security. Incorporating these two aspects, whilst utilising a online video conferencing session, enables a highly immersive experience for students to solve challenges to control IoT devices remotely, of which their impact can be viewed by online video. We report on our initial pilot studies of running remote cyber workshops in this fashion, and we discuss lessons learnt and how this pandemic has introduced new ways of working for cyber security education that can greatly enhance how we approach the subject compared to pre-pandemic. We propose that remote learning can offer experiences that actually complement the subject domain, rather than their in-person counterpart which do not convey a true reflection of a system.

## II. Background

Cyber security education has been well-established over recent years [1] [2], recognising the increasing importance of systems security and the wider context of society that attacks on technology and data can have. In recent years a wealth of online resources have been developed and offered up by the cyber security education community. Resources such as ImmersiveLabs [3] employ gamification techniques to give step-by-step lessons for students to follow. VulnHub [4] provides downloadable virtual machines that are specifically designed as vulnerable, to support ethical hacking exercises. More recently, HackTheBox [5] provides VPN-based access to online vulnerable machines, as does TryHackMe [6], which also integrates gamification and guiding questions to support student learning. There is a very active online community that contributes towards the development of these exercises. These resources all adopt gamification techniques which divide learning into smaller chucks, and motivating students through small positive reinforcements such as visual displays and badges [7]. Research has shown the exposing students to meaningful and relevant assignments, with collaborative learning opportunities is key to providing student retention [8] and Burguillo [9] shows that competition has a constructive effect on participation and learning that will result in higher learning through social pressure to achieve.

Studies such as those by Hanus & Fox [10] and De-Marcos *et al.* [11] assess gamification as a means of increasing students' intrinsic motivation to learn. They state that gamification allows students to learn in new ways, to enjoy what may otherwise be tedious tasks. Their research show differing results. De-Marcos *et al.* demonstrated increased learning, whilst Hanus & Fox showed positive student attitudes towards new tools, but a decrease in knowledge acquisition when measured using traditional exams. Conversley, Carlise *et al.* utilised CTFs as part of their formal undergraduate curriculum and found the motivation and learning impact for students and staff with CTF gamification on their course was so great, that some cyber courses are now taught at their institution entirely based on CTF's [12].

Home-schooling during the COVID-19 pandemic has presented its own unique set of challenges. Students have had to engage in online lessons via video conferencing tools such as Microsoft Teams and Zoom [13] [14]. 'Zoom fatigue', where students struggle to maintain concentration over long periods of time when interacting via online video, means that traditional face-to-face teaching methods may not translate well to online delivery. Therefore, it is important to consider how online video can be used to further motivate learning. In particular, whilst existing resources are good for those students who already have an active interest, how can online video conferencing platforms help to develop new interest in the subject for students that have not yet had much exposure to cyber security.

Traditional teaching of cyber security has been in classrooms and labs [15], and yet by it's very nature, remote connectivity of devices is a fundamental aspect. The nature of remote delivery provides an opportunity to explore this further, as students are able to remotely exploit specifically-intended systems, creating a greater realisation of how connected and dependent on technology our society has become.

## III. Method

To summarise our approach, we propose the integration of remote IoT device control with the submission of flags from a CTF competition. By coupling this with a live online video that students can access via Microsoft Teams or Zoom, students can complete CTF challenges, and actually see the consequence of their actions as IoT devices respond to their submitted answers. Compared to a typical CTF, this provides an opportunity to illustrate remote consequences of an attacker's actions online, and to create an immersive experience as part of home schooling that is different to traditional forms of learning and that can help inspire new learners to explore cyber security as a subject.

For our outreach work with schools, we developed a simple CTF challenge that covers some initial password cracking and encoding tasks, such as the challenge card shown in Figure 2. Here, one may notice that the numbers are ASCII values and can be converted to text to reveal the flag 'UWE{Robo_Go}'. Whilst a relatively simple example, the use of flags provides a flexible approach for integrating more challenging activities, depending on the target audience and the session duration. We specifically focus on a flag-based approach as there are a wealth of existing CTF challenges available online, meaning that our concept is extensible to other learning activities.

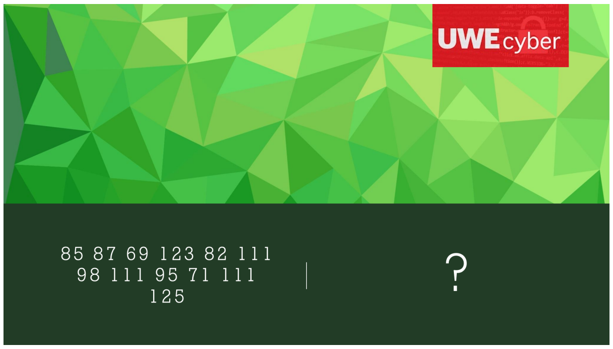
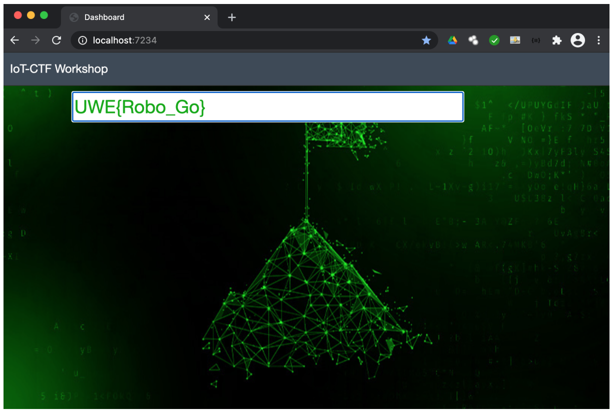


Fig. 2. CTF challenge card. As an example, here students need to identify that a secret message is encoded in ASCII to recover a flag.

At the core of our approach is a Raspberry Pi device that runs a Python Flask web server, that receives input from students and also communicates with home IoT devices. The use of the Pi makes for a highly portable and low cost solution. There is a need for some networking configuration to support port forwarding, so that users can access the web server externally. Having the server run on a low cost device such as Raspberry Pi helps to maintain separability from other systems that an instructor may not wish to make accessible to external clients. The server runs a simple web page where students are able to submit flags using the text box, shown in Figure 3.



UWE{Robo_Go}

Fig. 3. Web interface for flag submission, hosted as a Python Flask application. If a valid flag is submitted, then the Flask server will make a request to the Tuya IoT network to trigger an IoT action.

On submission of flags, our Flask application is also responsible for the interaction with our IoT devices. TinyTuya [16] is a Python library that provides access to smart devices that are configured using the Tuya IoT platform [17]. Many consumer Wi-Fi devices rely on Tuya as their support for IoT functionality, and there exist a number of third-party applications that extend on Tuya (e.g., Smart Life). Any devices that can be controlled using the Smart Life mobile phone application can effectively be integrated with our proposed system. This would enable ‘simple’ devices such as light bulbs and power switches that have a relatively limited number of possible states, through to more sophisticated devices such as a robot vacuum cleaner or a smart camera. The use of TinyTuya does require that an application is registered via the Tuya API to enable the access of a user’s devices.

```
import tinytuya
d = tinytuya.BulbDevice(DEVICE_ID, IP_ADDR, LOCAL_KEY)
d.set_version(3.3)
data = d.status()
```

This code sample briefly illustrates how we can access a light bulb device using the library. The output variable `data` will then consist of the following JSON output:

```
{'devId': '11768787500291b37c71',
 'dps': {'1': False,
  '2': 'white',
  '3': 255,
  '4': 255,
  '5': 'ff0000000ffff',
  '6': 'bd76000168ffff',
  '7': 'ffff500100ff00',
  '8': 'ffff8003ff000000ff000000ff000000000000000000',
  '9': 'ffff5001ff0000',
  '10': 'ffff0505ff000000ff00ffff00ff00ff0000ff000000'}}
```

We can manipulate these parameters directly, or we can utilise the Python API for performing typical operations such as changing colour and brightness options. It also allows for the control of more complex lighting devices, such as LED strip lights.

```
d.set_colour(255,255,0)
d.set_brightness(100)
d.set_white(255,255)
d.set_value(value=True, index='20')
```

The same API call can actually be applied to capture the state of more sophisticated devices, such as an IoT-enabled robot vacuum, which provides the following JSON output:

```
{'1': True, '2': False, '3': 'standby', '4': 'stop',
'5': 'Standby', '6': 100, '7': 96, '8': 98,
'9': 96, '10': False, '11': False, '12': False,
'13': False, '14': '3', '15': '20210202085102102700782',
'16': 297, '17': 0, '18': 0, '101': '3',
'102': '900235', '103': '00000000000000000000',
'105': '0000000000', '106': 7123456, '107': 3}
```

We can use the *set_value* command to modify an index-value pair and control the device directly. Our Flask web server is configured such that a series of common IoT functions are included, and a configuration file can be used to associate a flag value to a function call. Figure 4 shows the example IoT devices that we have tried integrating using the Tuya IoT platform.

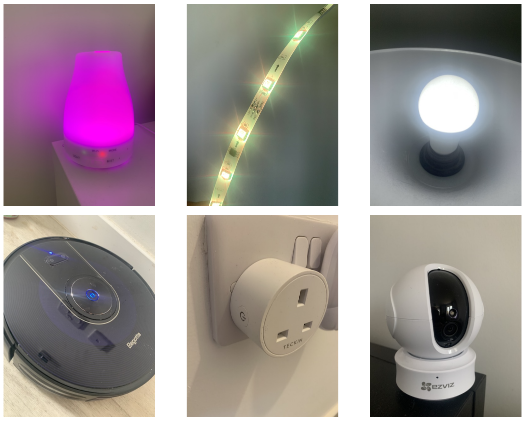


Fig. 4. Consumer devices connected using the Tuya IoT network. Top row: LED Humidifier, LED strip light, LED bulb. Bottom row: Robot vacuum, Power socket, PTZ Camera.

The final aspect of the approach is to enable an online video call using Microsoft Teams whereby students can actually observe the IoT devices that can be controlled through the submission of flags. Figure 5 shows two examples ‘IoT scenes’ using Microsoft Teams. In the first instance, we had a single camera capture a full scene that students can observe to see which device will trigger when a flag is submitted. An instructor can join the call from both a laptop device for their main interactions with a class, and from a mobile device such as an iPhone, where the device camera is pointed at the ‘IoT scene’ as deemed appropriate. In the second, we use multiple cameras pointed at various devices, and combined the video feeds (including the presenter) to a single feed using OBS, shared using the OBS Virtual Camera. This is useful when delivering a more guided workshop, whereas the full scene is useful when flags are explored in any chosen order.

## IV. Discussion

The primary motivation for this project was to develop a means to continue our outreach work with regional schools

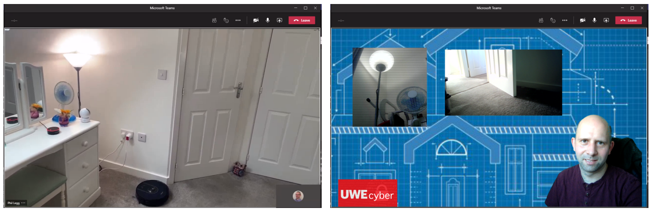


Fig. 5. Two examples of ‘smart scenes’ accessible via Microsoft Teams video call. In the first, a fixed camera is used to capture a scene consisting of a lamp, fan (controlled by smart socket), PTZ camera, speaker, and vacuum. In the second, we use multiple cameras pointed at devices and the workshop presenter, and use OBS to provide a single online video feed.

when the global pandemic required a shift to online delivery of teaching. We wanted to identify suitable activities that were relevant for the subject matter, yet would create a sense of engagement and excitement that could inspire students to pursue further study of cyber security. Early trials found that schools are keen to engage with new ways of working online for teaching cyber security, and we are currently exploring how we can offer workshops for more schools in our region.

One of the main challenges of this proposed approach that we recognise is scalability. As a team, we have been able to deliver online sessions with schools and teachers, and support them in completing tasks. The IoT aspects of the project require a dedicated space for IoT devices to be set up and configured within, which currently involves the use of a home working space that the instructor is happy to make visible for students. Furthermore, this approach requires the configuration of the home network to enable port forwarding to the Raspberry Pi server. Having a team of academics that work closely with schools has helped for developing the proof-of-concept system, although it does require a team to deploy as a live event, and so further work will need to explore how feasible it is for school teachers to deploy their own configuration of this approach. Our focus of this activity has been to encourage uptake of cyber security for those who may be new to the subject, whilst also supporting teachers who may not necessarily know how to provide such an activity. We continue to work with schools and teachers to upskill in these activities, such that teachers could potentially deploy this form of activity for their own classes given appropriate training. The objective is for the workshop to provide inspiration for students, to then explore further learning opportunities from the wealth of existing online resources.

More generally, the global pandemic has caused us to rethink our approach to academic teaching and outreach. Examples include how students may utilise Raspberry Pi devices remotely to control simulation systems hosted on campus, further illustrating how remote exploitation of devices can be performed. Given the significance of this in the field of cyber security, there are opportunities that have been presented by remote working that are yet to be fully realised in terms of how we work with and demonstrate attacks on remote systems.

## V. Conclusion

In this short paper, we describe an approach for combining CTF and IoT device control to create a unique teaching experience for students whilst under remote working restrictions. Using a web server for CTF flag submission, the server is able to trigger IoT actions on correct flag submission, such that students can observe physical consequences of their actions via Microsoft Teams. Our early feedback from schools and from the research community is that this would serve as an engaging and exciting outreach opportunity for students, whilst also helping to upskill teachers to be able to deploy their own similar workshop activities. The integration of flag submission means that the approach can be easily extended to other learning tasks.

Future work will continue to explore how we can provide innovative learning opportunities for teaching cyber security concepts. We will continue our development of remote-based outreach activities, as online learning is likely to be much more integrated in future teaching initiatives going forward. We will seek to explore how our on-campus IoT laboratory can be utilised to support remote access for future workshops, with a view of scaling this offer out to more schools across our region. Furthermore, we will explore how other opportunities for remote learning can benefit our other teaching provisions, such as remote control of Industrial Control Systems.

## References

[1] F. B. Schneider, “Cybersecurity education in universities,” *IEEE Security Privacy*, vol. 11, no. 4, pp. 3–4, 2013.

[2] A. McGettrick, “Toward effective cybersecurity education,” *IEEE Security Privacy*, vol. 11, no. 6, pp. 66–68, 2013.

[3] ImmersiveLabs. [Online]. Available: http://www.immersivelabs.com

[4] VulnHub. [Online]. Available: http://www.vulnhub.com

[5] HackTheBox. [Online]. Available: http://www.hackthebox.eu

[6] TryHackMe. [Online]. Available: http://www.tryhackme.com

[7] K. M. Kapp, *The gamification of learning and instruction: game-based methods and strategies for training and education*. John Wiley & Sons, 2012.

[8] L. Barker and J. Cohoon, “Key practices for retaining undergraduates in computing,” *National Center for Women and Information Technology, www. ncwit. org/retainundergrads*, 2009.

[9] J. C. Burguillo, “Using game theory and competition-based learning to stimulate student motivation and performance,” *Computers & education*, vol. 55, no. 2, pp. 566–575, 2010.

[10] M. D. Hanus and J. Fox, “Assessing the effects of gamification in the classroom: A longitudinal study on intrinsic motivation, social comparison, satisfaction, effort, and academic performance,” *Computers & education*, vol. 80, pp. 152–161, 2015.

[11] L. De-Marcos, A. Domínguez, J. Saenz-de Navarrete, and C. Pagés, “An empirical study comparing gamification and social networking on e-learning,” *Computers & education*, vol. 75, pp. 82–91, 2014.

[12] M. Carlisle, M. Chiaramonte, and D. Caswell, “Using ctfs for an undergraduate cyber education,” in *2015 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*, 2015.

[13] A. Stefanile, “The transition from classroom to Zoom and how it has changed education,” *Journal of social science research*, vol. 16, pp. 33–40, 2020.

[14] A. Alam, “Challenges and possibilities of online education during covid-19,” 2020.

[15] D. Pencheva, J. Hallett, and A. Rashid, “Bringing cyber to school: Integrating cybersecurity into secondary school education,” *IEEE Security Privacy*, vol. 18, no. 2, pp. 68–74, 2020.

[16] TinyTuya Python Library. [Online]. Available: https://pypi.org/project/tinytuya/

[17] Tuya IoT Platform. [Online]. Available: https://www.tuya.com