UWE Bristol University of the West of England
in association with National Cyber Security Centre Department for Digital, Culture, Media & Sport
Academic Centre of Excellence in Cyber Security Education
UWE cyber Gold Award

Presentation by:

Jonathan White
Senior Lecturer in Cyber Security
Jonathan6.White@uwe.ac.uk
@CyberJonWhite

Co-Authors:

Phil Legg
Professor in Cyber Security
Phil.Legg@uwe.ac.uk
@dr_plegg

Alan Mills
Lecturer in Cyber Security
Alan.Mills@uwe.ac.uk
@amill157

14th November 2022

Interactive Cyber-Physical System Hacking: Engaging Students Early Using Scalextric

CISSE – 26th Colloquium

Cyber Security Education Outreach

- The University of the West of England (UWE) is a UK National Cyber Security Centre (NCSC) accredited Academic Centre of Excellence for Cyber Security Education (ACE-CSE).
- In addition to having an NCSC certified degree accreditation holders must also be able to demonstrate:
  - Developing an influential and growing community of cyber security educators
  - Shaping and supporting cyber security education
  - Engaging with industry, government, educators and students

Cyber Security Education Outreach

UWE Bristol University of the West of England

unlock cyber
OPENING FUTURES IN CYBER SECURITY

HARGREAVES LANSDOWN

CGI

BT

Nationwide

Arcanum CYBER SECURITY

QA

LEONARDO

BAE SYSTEMS

pwc

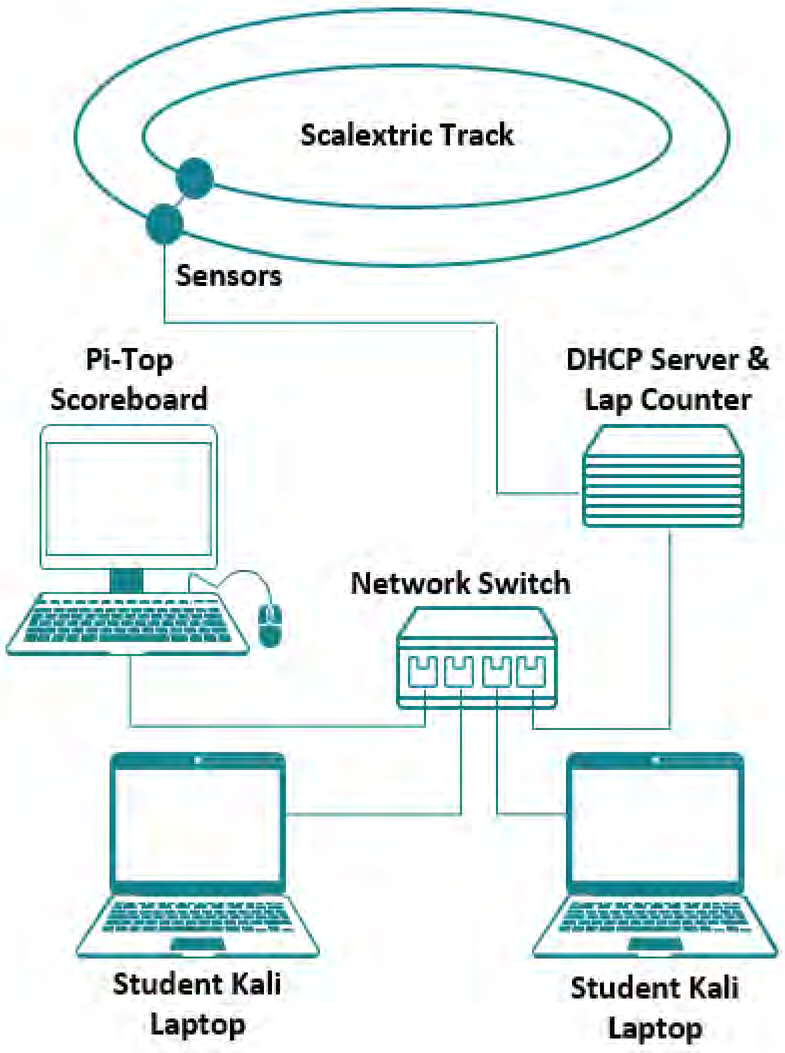
Related Work

- We analysed current trends and techniques for cyber security education
  - Virtual Platforms:
    - TryHackMe (https://tryhackme.com/)
    - HackTheBox (https://www.hackthebox.com/) and HackTheBox Academy (https://academy.hackthebox.com/)
  - Practice-based Learning
    - **Pencheva et al. (2020)** - Bringing cyber to school: Integrating cybersecurity into secondary school education
    - **Crick et al. (2020)** - Overcoming the challenges of teaching cybersecurity in UK computer science degree programmes
    - **Legg *et al.* (2020)** - Hacking an IoT Home”: New opportunities for cyber security education combining remote learning with cyber-physical systems

Our Approach

- Inspired by the London Olympic Games 2012 where cyber security around the digital scoreboards was considered
- Activity based around a slot-car track to draw-in and engage students
- Coupled hands-on practice-based exercise with multiple networked systems including a scoreboard system and motion sensors to provide connectivity with the physical environment
- Working in teams, students can immediately observe the consequences of their actions on the local scoreboard.
- Ultimate aim is to compromise the scoreboard, ensure their team win, and the other lose.

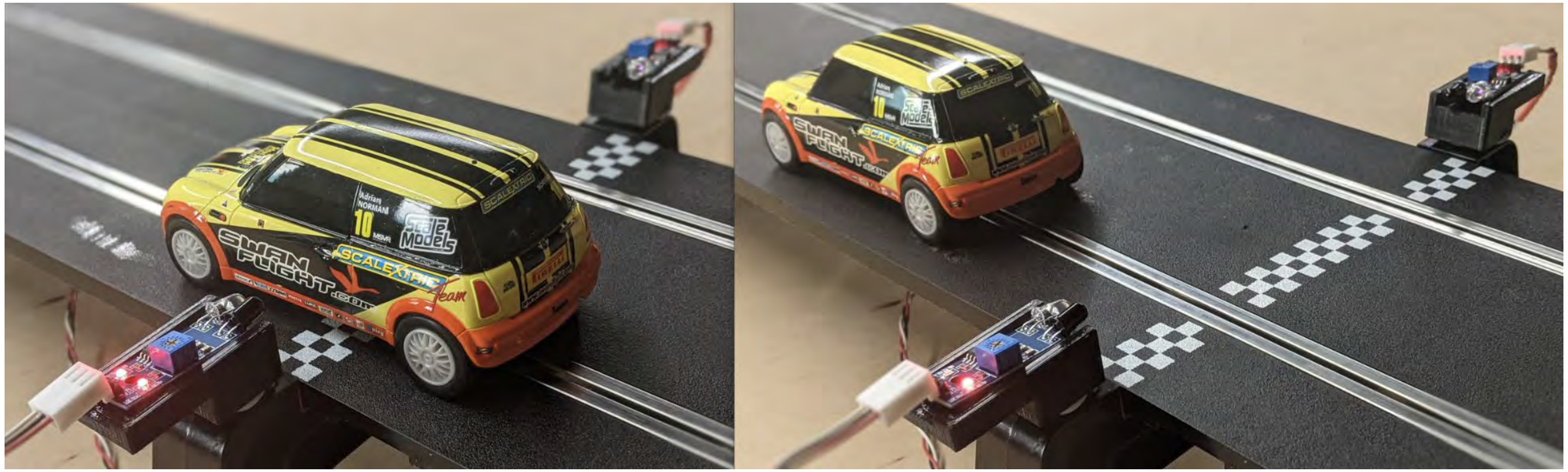
System Design



- One Scalextric slot-car racing track
- Two HW-201 object detection IR sensors
- One Raspberry Pi Model 3b+ acting as a combined DHCP server and lap counter
- One pi-Top CEED incorporating a second Raspberry Pi Model 3B+ to display the scoreboard via a Flask-based Web Server
- Two Laptops running Kali Linux
- One network switch connection all devices together on a local network

System Design - Sensors

- Connectivity of the slot-car track to the scoreboard was achieved through IR object-detection sensors
- Created a 3D printed housing to mount the sensors to the track



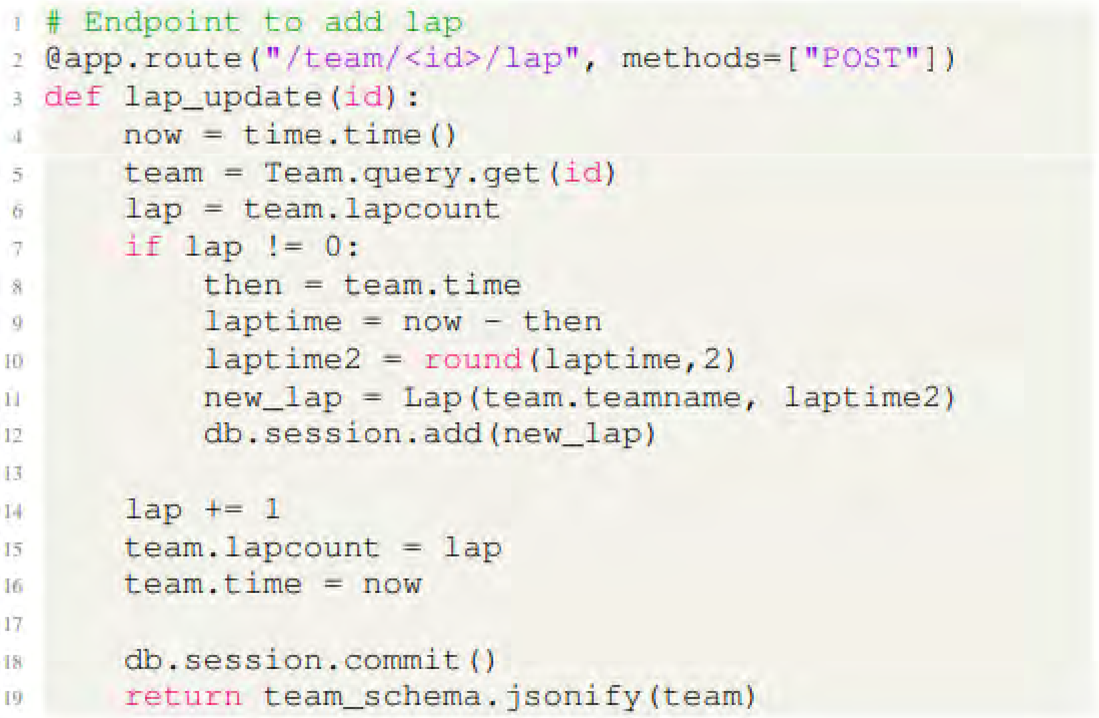
- Developed a small Python script that ran on the Raspberry Pi to detect the motion and send a POST update to the web server.

System Design – Lap Counter and DHCP Server

- Lap Counter and DHCP functionality was combined on a single headless Raspberry Pi 3b+ to reduce the required equipment.
- Out of scope for student attacks, so device was hardened against attack
- Lap counter script configured to run at boot to allow for minimal user interaction to start the activity.
- Static IP addresses used for DHCP server and Web server to allow for consistency between sessions
- DHCP server required for student laptop connectivity, and to support any additional staff machine.

System Design – Web Server

- The Web Server is the target device for students to attack
- Intentionally designed to have several vulnerabilities and attack paths, facilitating multiple ways to compromise the service and scoreboard.
- Services Exposed:
  - HTTP
  - FTP
  - SSH
  - VNC



```python
# Endpoint to add lap
@app.route("/team/<id>/lap", methods=["POST"])
def lap_update(id):
    now = time.time()
    team = Team.query.get(id)
    lap = team.lapcount
    if lap != 0:
        then = team.time
        laptime = now - then
        laptime2 = round(laptime,2)
        new_lap = Lap(team.teamname, laptime2)
        db.session.add(new_lap)

    lap += 1
    team.lapcount = lap
    team.time = now

    db.session.commit()
    return team_schema.jsonify(team)
```

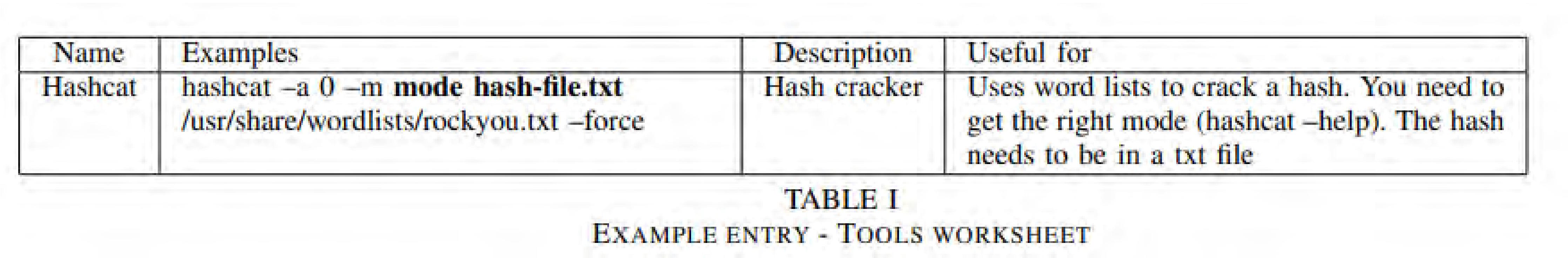
Listing: Python example

System Design – Laptops

- Each team received a laptop with Kali OS installed.
- Allows easy access to common penetration tools such as:
  - **Nmap** – Service Discovery and Reconnaissance
  - **DIRB** – Web Directory and File Enumeration
  - **Hashcat** – Password Hash Cracking
  - **Rockyou.txt** – Text file with 14 million common passwords
- Other tools are required for students to progress along with common Linux utilities such as:
  - **Curl**
  - **FTP**
  - **Python**

System Design – Worksheets

- Different worksheets have been designed with the target age range and experience in mind.
- Students with no Linux or cyber security experience can be given much more guidance and explanation.
- Students with more experience can be given worksheets as a basic steer with hints



Name	Examples	Description	Useful for
Hashcat	hashcat –a 0 –m **mode hash-file.txt** /usr/share/wordlists/rockyou.txt –force	Hash cracker	Uses word lists to crack a hash. You need to get the right mode (hashcat –help). The hash needs to be in a txt file

TABLE I
EXAMPLE ENTRY - TOOLS WORKSHEET

The Activity

- Students split into two teams (max 5 per team) – competing to beat the other team’s score
- Designed to walk through the common steps of any CTF
  - Initial Recon – Own IP and mapping the network
  - Locate the web server and enumerate using DIRB:
    - **admin** - Where they could easily reset the other team’s score
    - **test** - A “debugging” curl command that can be used to manually increase their score (by 1)
    - **teams** - The target URI for increasing their own score
    - **console** - The Python Werkzeug console, this could be used by teams to achieve a root reverse shell
  - Explore other services such as FTP – leads to a password hash that when cracked allows for direct SSH access.
  - With terminal access, a .txt file can be found containing a Python script that automates score updates

Engagement

- Initial engagement would often be focused on the physical aspects of the setup, one or two students would take the lead on working through the worksheets and others would join in.
- A common factor was an increase in cyber engagement when a team was able to reset the opposing team's score to 0. Quickly draws attention to the "real world impact".
- In some cases, teams completely moved away from the physical slot car racing when they realised that physical input was no longer required to trigger a score update.
- Key milestones were manual or scripted updates of the scoreboard.
- Common questions were around how to not only improve their own score, but ensure the other team were unable to do so – Showing preventing the progress of other was a strong motivation
- Initial feedback suggests that students particularly enjoyed the activity.
  - "*…had to literally tear the last group away from the Scalextric activity as they were glued to it*"
  - "*The pupils were totally engaged and couldn't stop talking about it on the way home*"

Challenges and Further work

- Scalability – significant footprint and support required.
- Examine the psychological motivators for students whilst engaging with the activity
- Containerisation of the application using Docker to enable easy reset of the activity.
- Develop other exploitation avenues for event reuse
- Extend the worksheets further to cater for wider audiences and range of activity times

- The Raspberry Pi images and worksheets have been made available at https://go.uwe.ac.uk/scalextric

Q&A

Jonathan White, Phil Legg and Alan Mills

Jonathan6.White@uwe.ac.uk
@CyberJonWhite

Phil.Legg@uwe.ac.uk
@dr_plegg

Alan.Mills@uwe.ac.uk
@amill157

UWE Bristol University of the West of England