UWE Bristol | University of the West of England

IEEE C-MRiC Centre for Multidisciplinary Research, Innovation and Collaboration

Cyber Science 2021

Phil Legg
Thomas Higgs
Pennie Spruhan
Jonathan White
Ian Johnson

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

UWE cyber Gold Award

in association with National Cyber Security Centre

Department for Digital, Culture, Media & Sport

Academic Centre of Excellence in **Cyber Security Education**

Cyber Security Outreach

- Cyber Security Outreach is a key part of UWE's regional education strategy to promote cyber security as a future career path

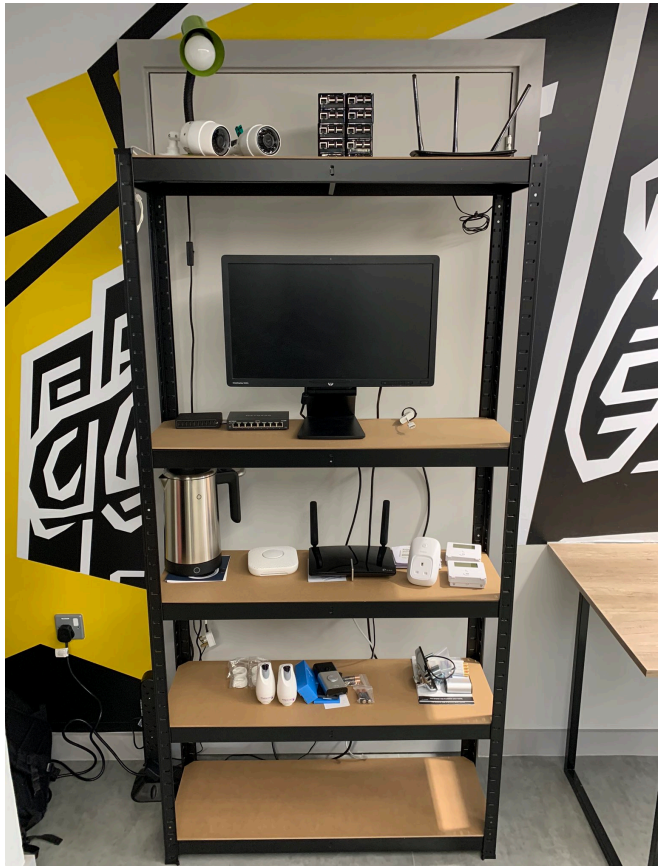
- Large-scale workshop events, school visits and clubs, University "taster days".

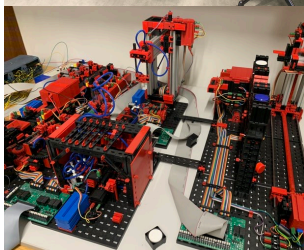
- Sphero challenge
- Scalextric scoreboard hacking
  - Skills: Raspberry Pi, Kali Linux, Nmap, Hydra, Python, Packet Capture/Spoofing…

Cyber Foundry

- Physical space at Frenchay to get students working on extra-curricula activities such as industry projects

- IoT Workbench for smart home security
  - Cameras, doorbells, light bulbs, kettles, temperature sensors, door locks
  - CTF server, SOC setup, Factory simulator, lots of toys to play with…





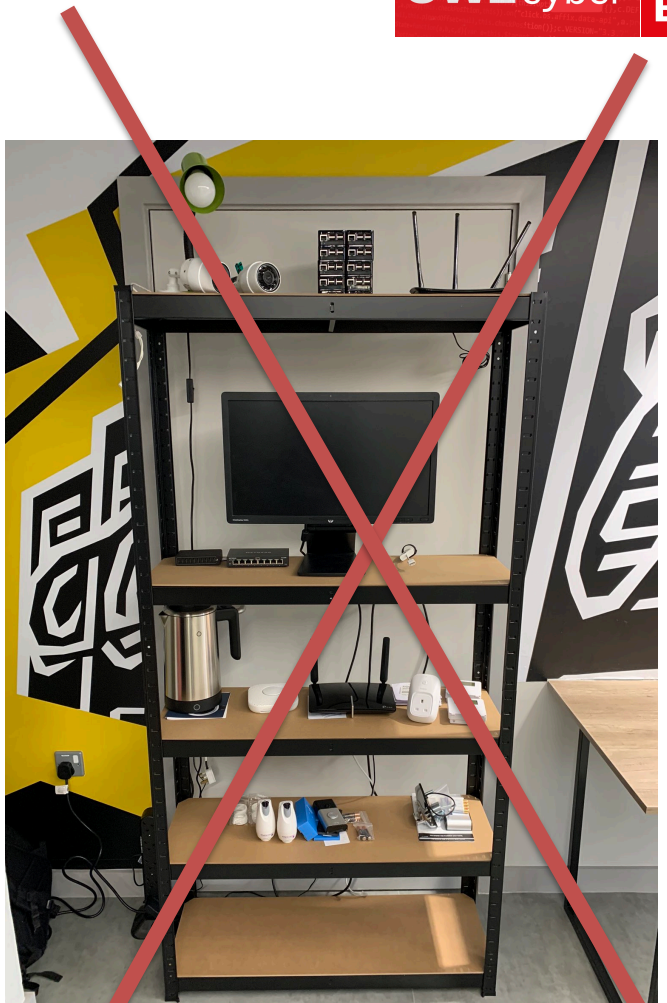
UWE cyber | UWE Bristol University of the West of England

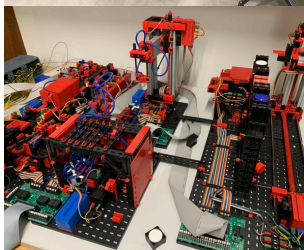
COVID-19 ☹

UWE cyber | UWE Bristol University of the West of England

Project Aims

- How can we continue to deliver outreach activities during lockdown?
- What are the new ways of working that we need to think about – both now and post-pandemic?
- We don't have physical access to our kit, and all staff and students are working from home.





IoT Home Hacking

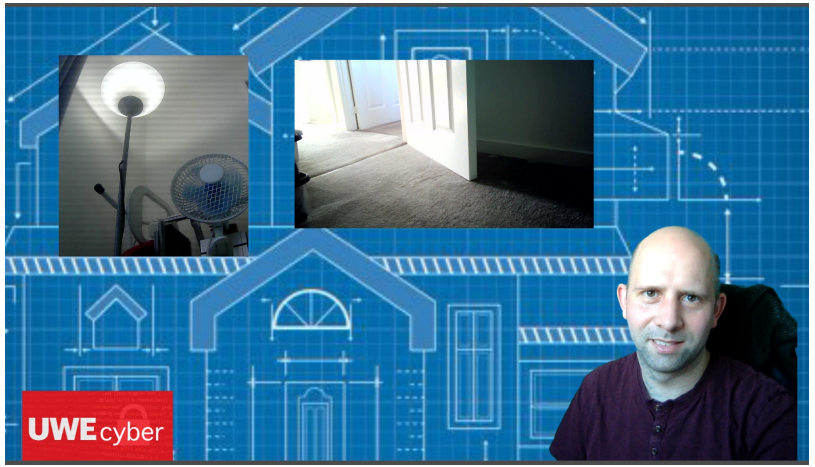
- We developed a "**Hacking the IoT home**" workshop, that can be delivered remotely.
- Based on a CTF-style meaning that challenges could be suited to all levels.
- CTF flags link to IoT device control - remote control of physical devices observed via online video
- CTF-IoT Server can be deployed on a Raspberry Pi – cheap (and separate!)

IoT Home Hacking

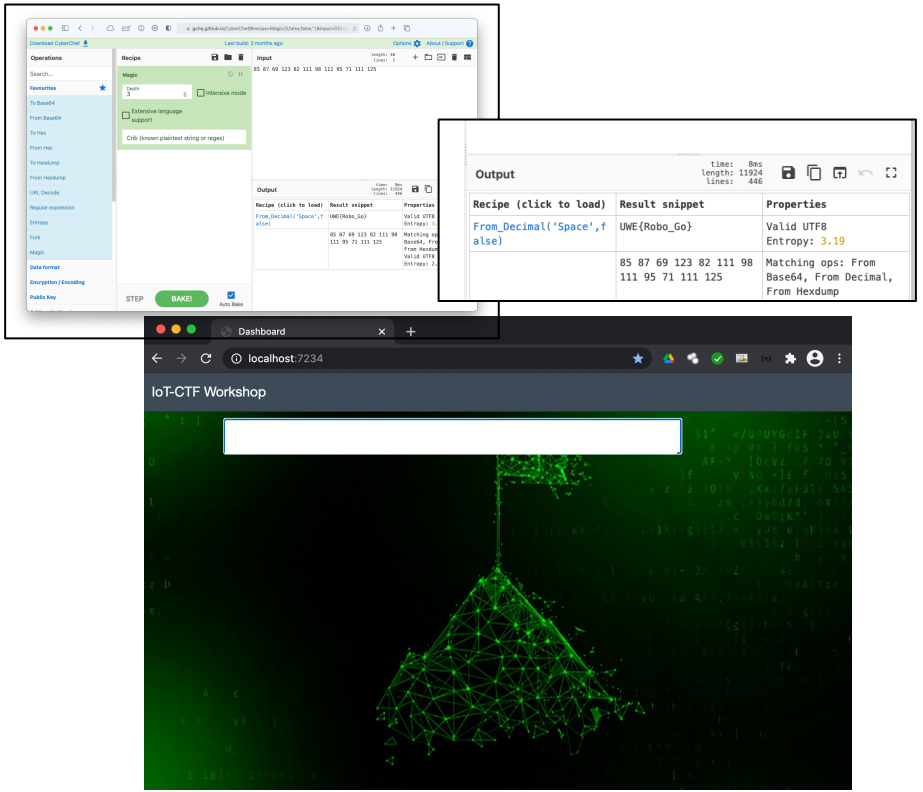
- Requires:
  - Raspberry Pi IoT-CTF server
  - Webcams (I have lots of cheap ones!)
  - IoT devices (running on Tuya network)
  - A (little) bit of home networking knowledge to set up port forwarding

- Intention was for a relatively simple home setup that teachers could easily imitate

- Small Python Flask Server that hosts the CTF webpage and communicates with the Tuya IoT network – all hosted on a Pi.



IoT Home Hacking

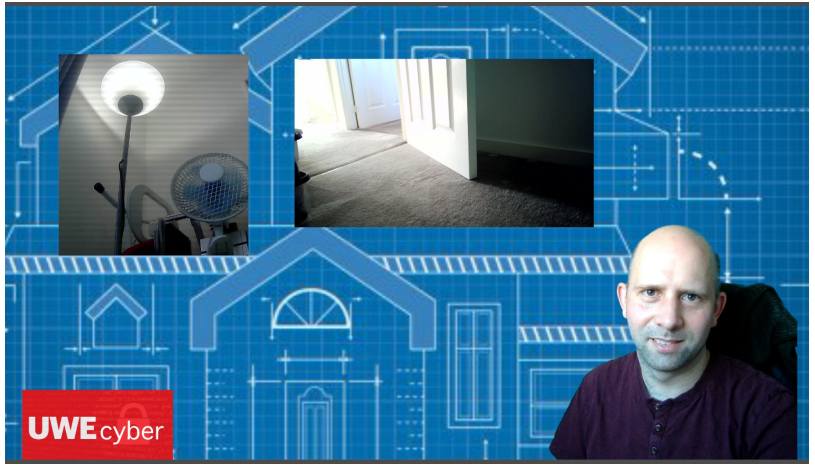


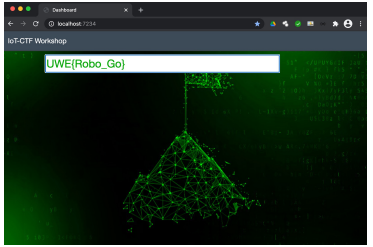
Code breaker! Can you decipher the code?

If you are stuck, why not visit the CyberChef (https://gchq.github.io/CyberChef)

IoT Home Hack

- We hosted some small pilot studies of online outreach in Summer 2020 and March 2021.
- Initial response from students was that it was "cool" to control devices remotely, and to see things happening in someone else's home!
- Turns WFH into an advantage – we actually have an IoT home to "hack".
- Increases online engagement and interactivity and may encourage further subject exploration.





IoT Gadgets

- Using the TinyTuya Python library we experimented with different IoT gadgets available at home.
  - Lighting (bulb and strip) and plug sockets well supported by the library and documentation
  - Other devices like the robot vacuum work – *however are not documented and have to be described as a Bulb or Switch! Some experimentation was required!*
  - We want to link with more devices - *like the IoT kettle and the heating controllers we have which has been locked away on campus!*

```
"""
RGB Bulb Device
"""
d = tinytuya.BulbDevice('DEVICE_ID_HERE', 'IP_ADDRESS_HERE', 'LOCAL_KEY_HERE')
d.set_version(3.3)  # IMPORTANT to set this regardless of version
data = d.status()

# Show status of first controlled switch on device
print('Dictionary %r' % data)

# Set to RED Color - set_colour(r, g, b):
d.set_colour(255,0,0)

# Brightness: Type A devices range = 25-255 and Type B = 10-1000
d.set_brightness(1000)

# Set to White - set_white(brightness, colourtemp):
#    colourtemp: Type A devices range = 0-255 and Type B = 0-1000
d.set_white(1000,10)
```

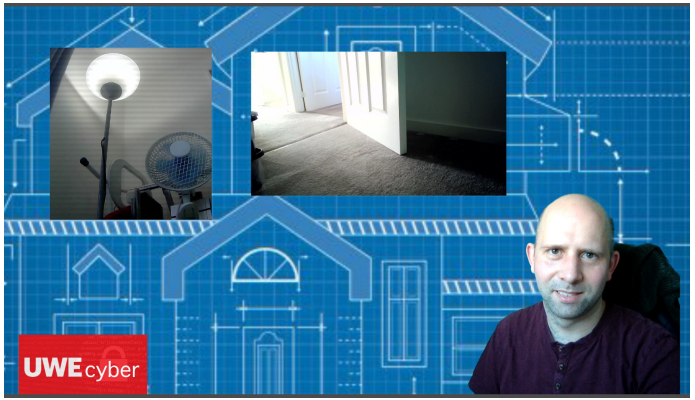
https://pypi.org/project/tinytuya/

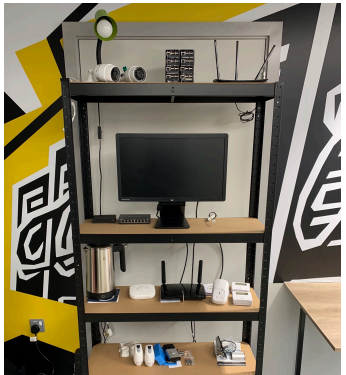
Post-Covid Cyber Security Outreach

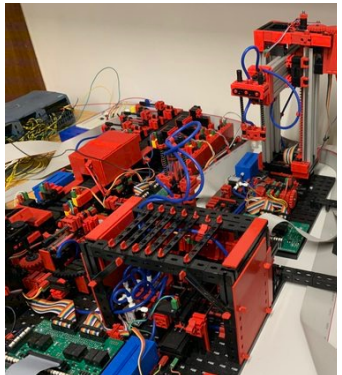
- We developed a suitable immersive online workshop – different to existing offers – that we have trialed and ran some small pilot studies with.

- Remote access of devices is a key component in many cyber 'issues' - workshop content works **because** it is remote, and it's not the same room as where the students are situated.

- How do we design teaching experiences that capture their imagination in this manner?

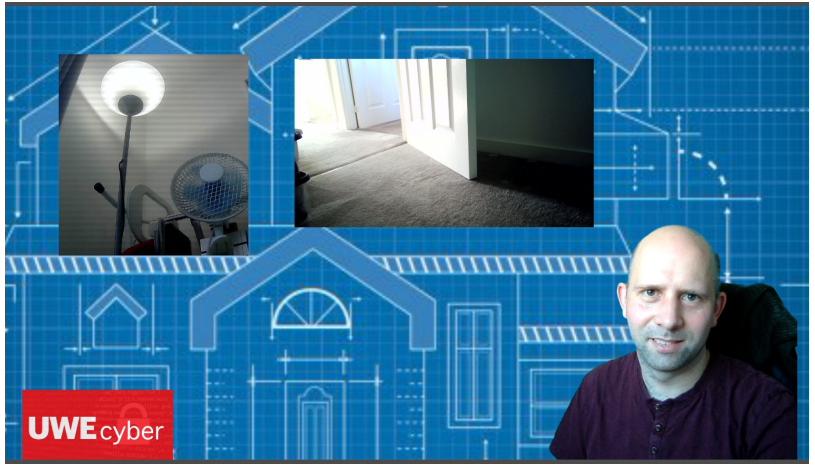






Thank you for listening

Phil.Legg@uwe.ac.uk
http://www.plegg.me.uk
http://go.uwe.ac.uk/phil



Want to see the clip?
https://youtu.be/WxITdr2MbKk