USABLE SANDBOXING

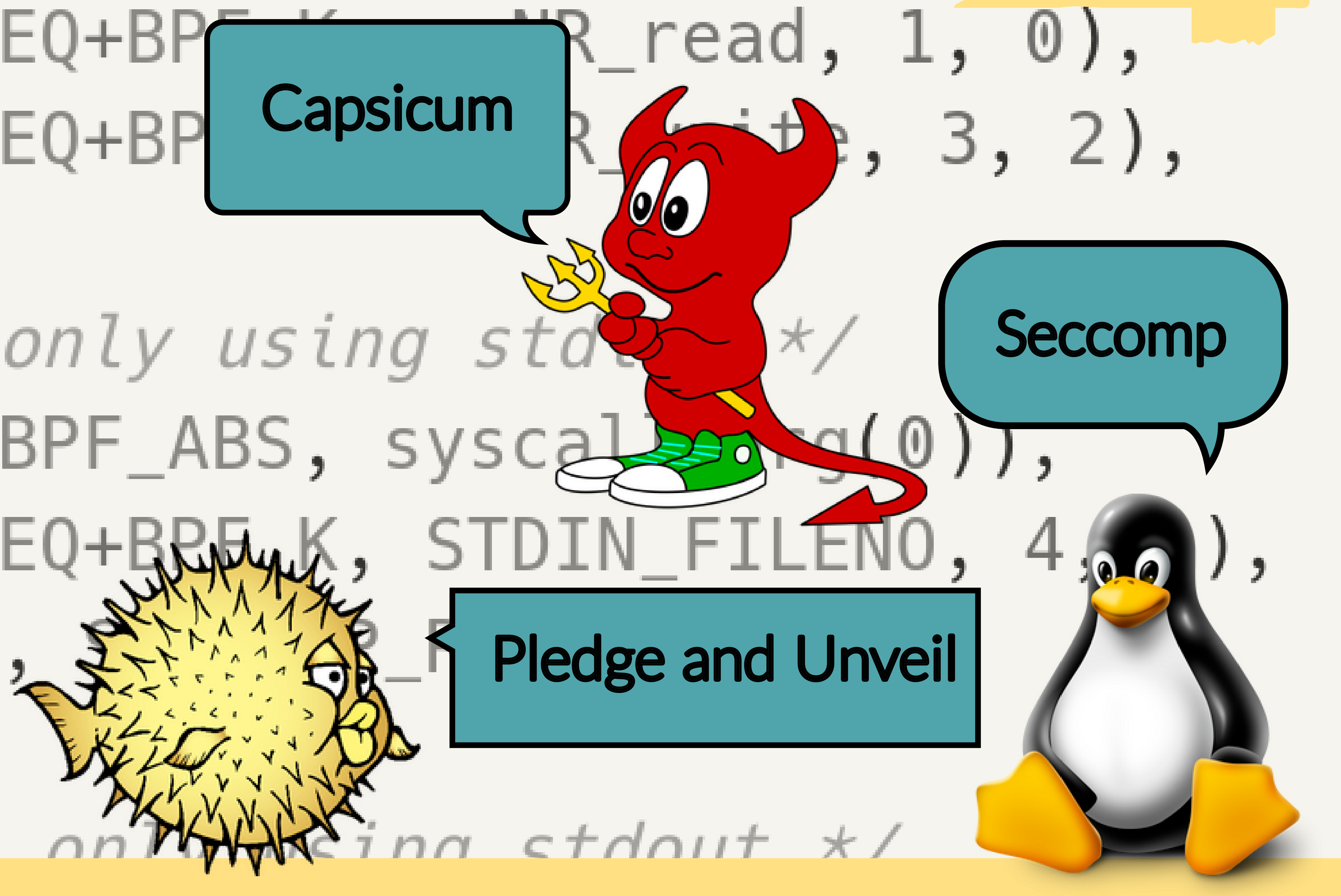
FOR EMBEDDED OPERATING SYSTEMS

Sandboxing and privilege separation mechanisms are essential security concepts that enable resilience by isolating and limiting what a program can do.

While desktop OSs have various sandboxing APIs and libraries, embedded and real-time OSs have a limited set of options.

Embedded OSs can significantly benefit from solutions that enable a more granular and specific privilege separation mechanisms.

The research aim is to harden operating systems' security by studying how developers use sandboxing mechanisms in their software and make further suggestions in order to improve the usability and security of operating systems.



```
pledge("stdio");
```

RQ1: What are the usability challenges of sandboxing mechanisms and how do they contrast across different classes of operating systems?

RQ2: To what extent are the sandboixng mechanisms adopted by the developers? And what are the challenges of adoption with regards to embedded operating systems?

RQ3: Can we harden the security of embedded OSs by implementing mechanisms inspired by the ones in desktop OSs?

Maysara Alhindi
maysara.alhindi@bristol.ac.uk

Supervised by: Dr Joseph Hallett
joseph.hallett@bristol.ac.uk

University of BRISTOL
Bristol Cyber Security Group