University of BRISTOL

Systems & Software Security

COMSM0050

2020/2021

bristol.ac.uk

University of BRISTOL

Attack Surface & Trusted Computing Base

bristol.ac.uk

Attack Surface

- The attack surface is all the possible way for an attacker to compromise a “system”
  - Users;
  - Network;
  - Operating Systems;
  - Software;
  - Hardware;
  - etc.

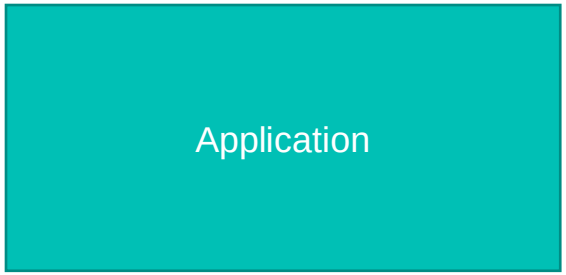
University of BRISTOL

Reducing Attack Surface

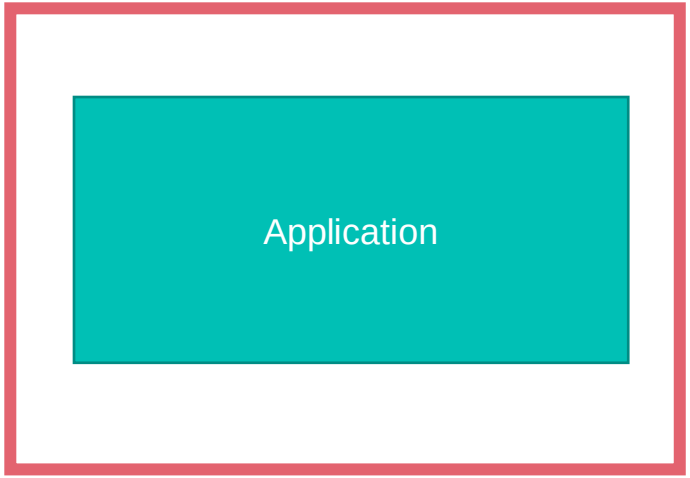
Example: sandboxing

bristol.ac.uk

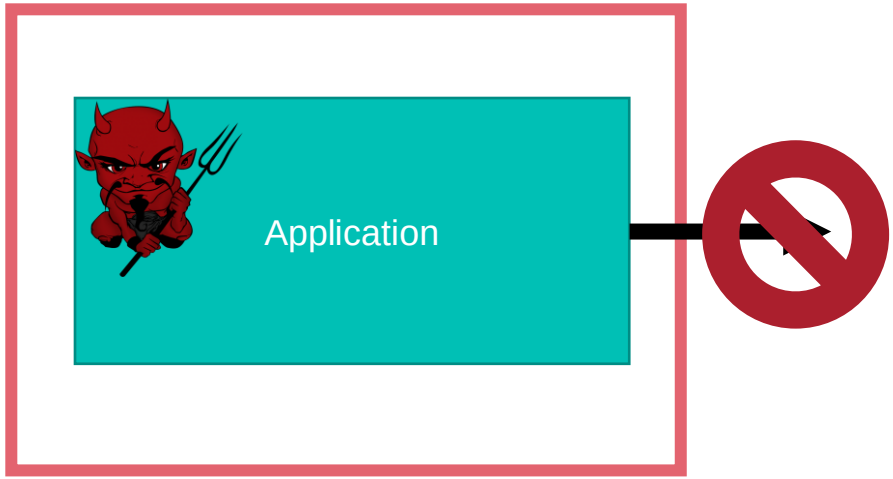
Sandboxing



Sandboxing

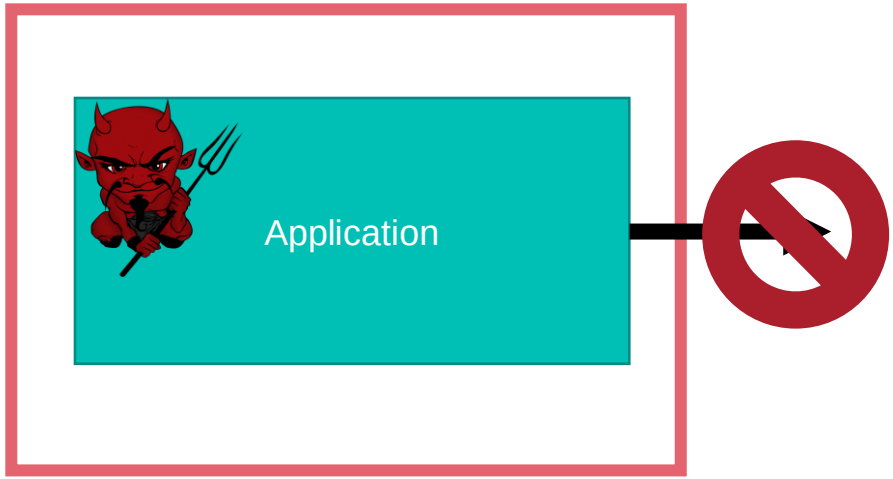


Sandboxing

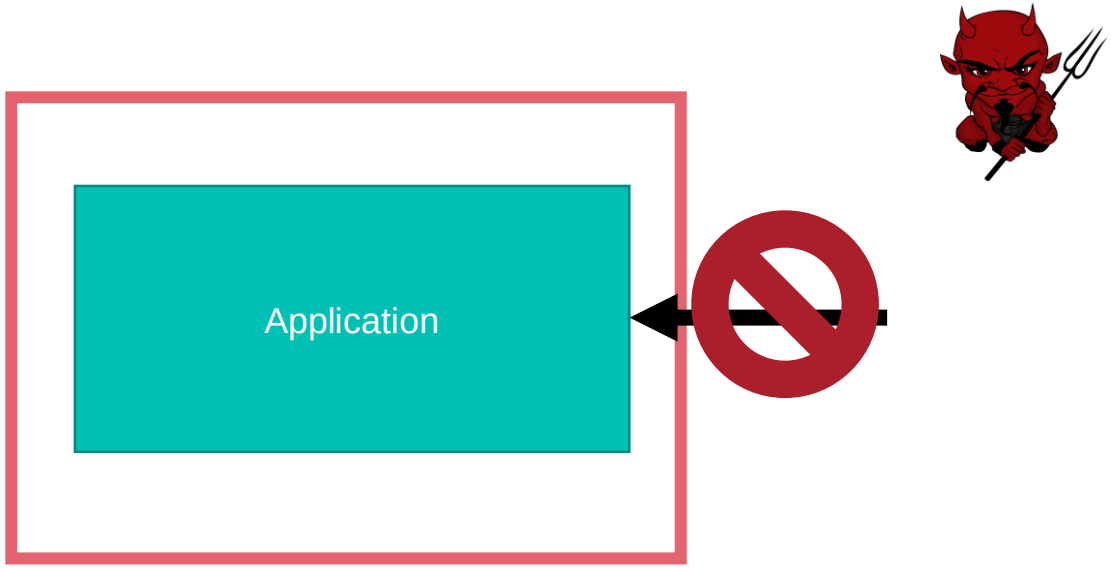


Sandboxing

e.g. Browser Sandbox
chrome://sandbox

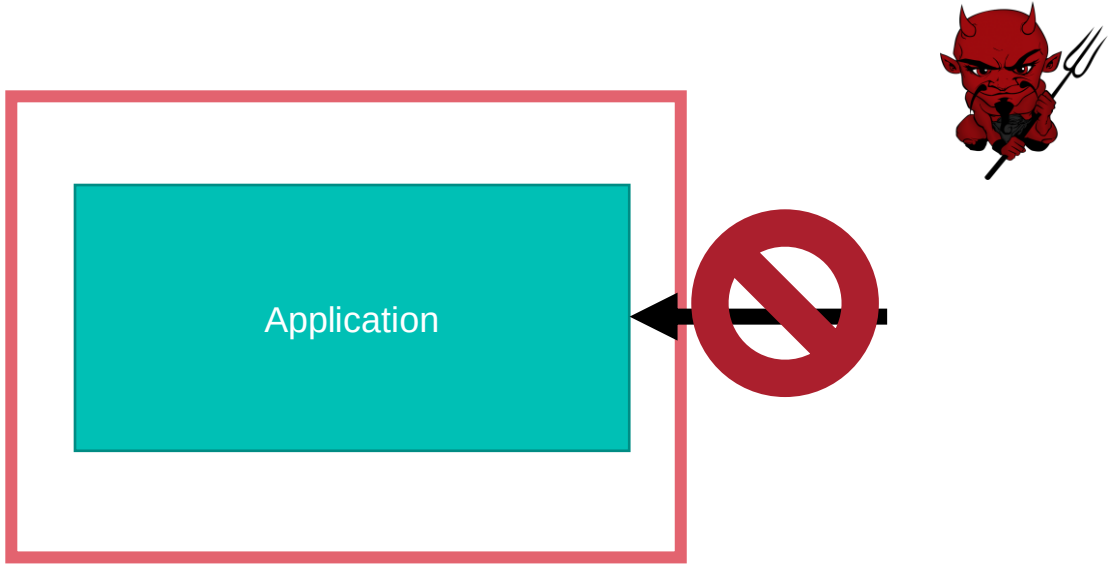


Trusted Execution Environment



Trusted Execution Environment

e.g. SGX enclave
see future video



University of BRISTOL

How to define your sandbox?

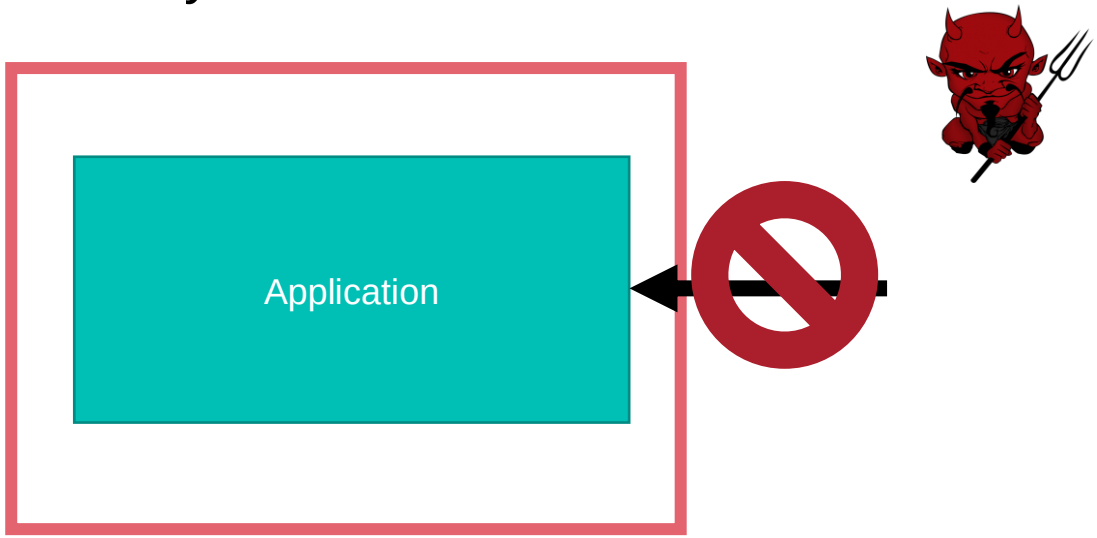
bristol.ac.uk

What is security?

- Security: Goal vs Adversary
- Policy: goal you want to achieve
  - Confidentiality (e.g. only the lecturers can see exams)
  - Integrity (e.g. only the lecturers can enter/change grades)
  - Availability (e.g. the student must be able to submit their coursework)
- Threat Model: assumption about the adversary
  - Reasonable assumptions
  - Attacker omnipotent nothing can be done
  - … but, need to not be too weak
- Mechanism: how you implement your policy

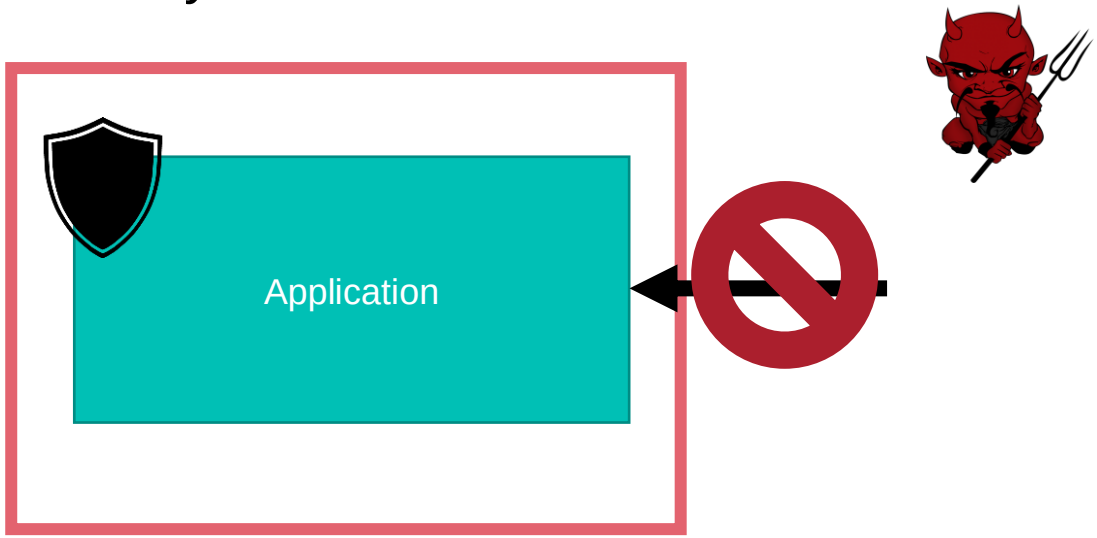
Trusted Computing Base (TCB)

- What part of the system do I need to trust in order to achieve my objective



Trusted Computing Base (TCB)

- What part of the system do I need to trust in order to achieve my objective

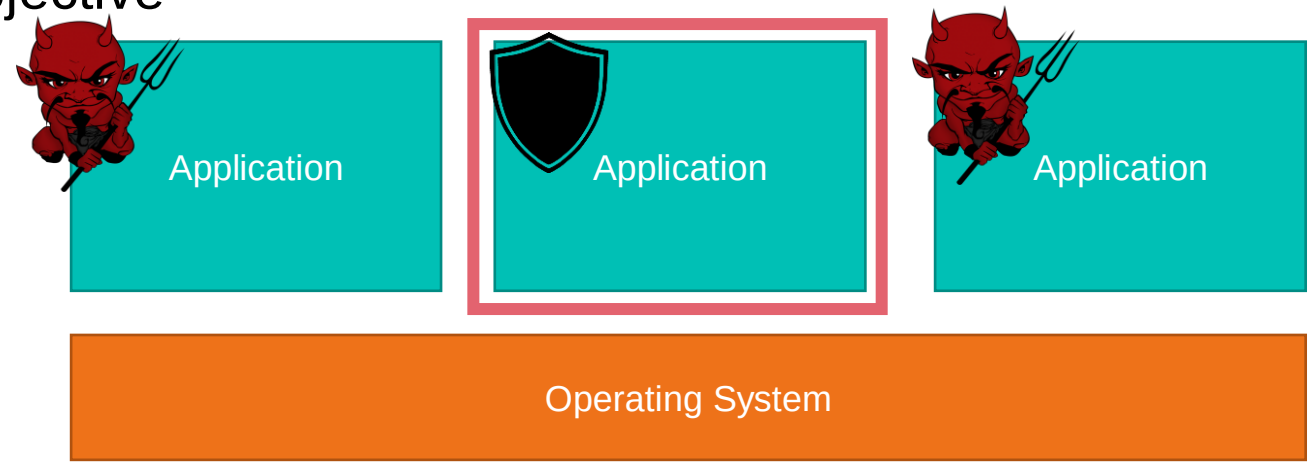


Trusted Computing Base (TCB)

- What part of the system do I need to trust in order to achieve my objective

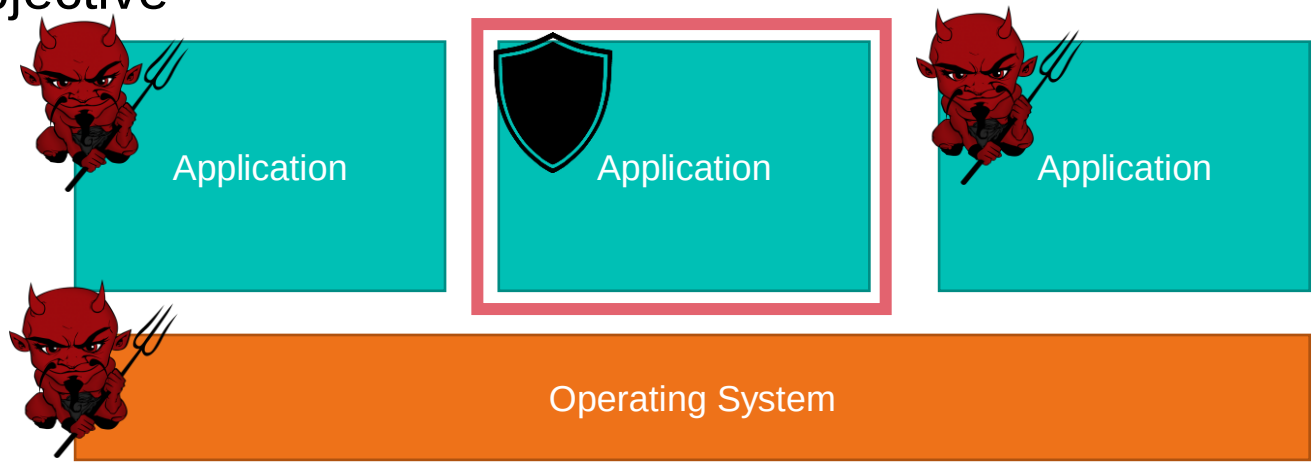
Trusted Computing Base (TCB)

- What part of the system do I need to trust in order to achieve my objective



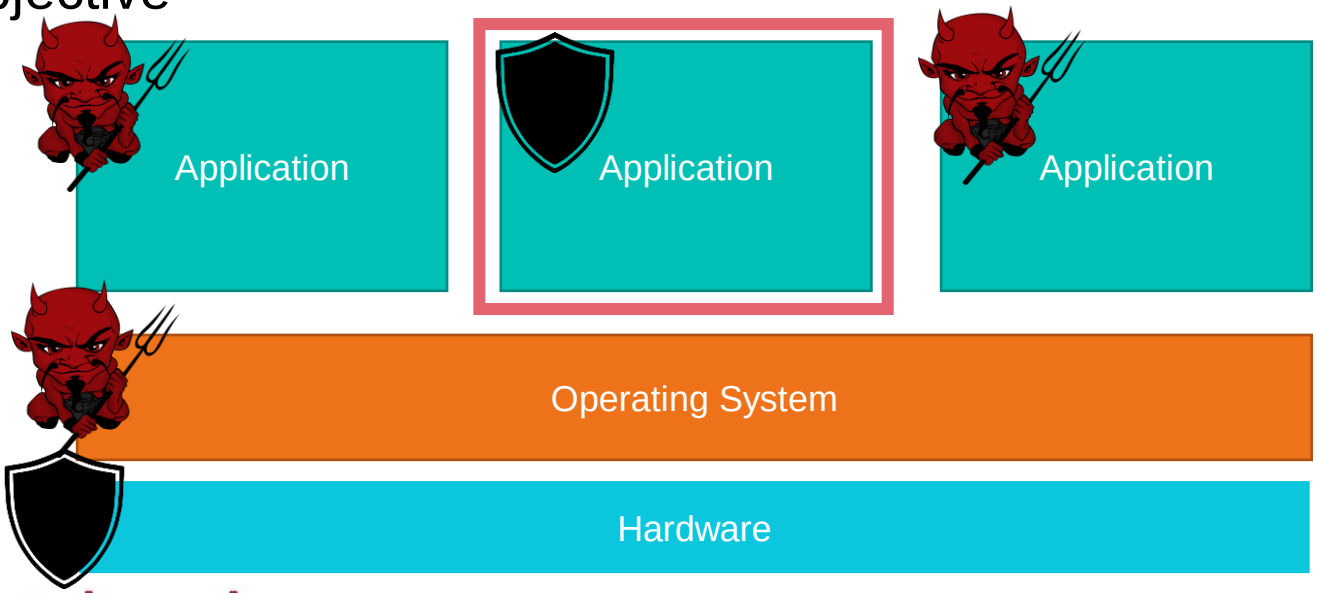
Trusted Computing Base (TCB)

- What part of the system do I need to trust in order to achieve my objective



Trusted Computing Base (TCB)

- What part of the system do I need to trust in order to achieve my objective



Trusted Computing Base (TCB)

- What part of the system do I need to trust in order to achieve my objective

SGX:
CPU
Application itself