University of BRISTOL

Systems & Software Security

COMSM0050

2020/2021

bristol.ac.uk

University of BRISTOL

Rootkit

bristol.ac.uk

Purpose

- Give attacker a permanent root access to a system
- Hide its presence
  - Hide from filesystem
  - Hide its activity
  - etc…
- Steal information
- Allow remote code execution

Typical attacker steps

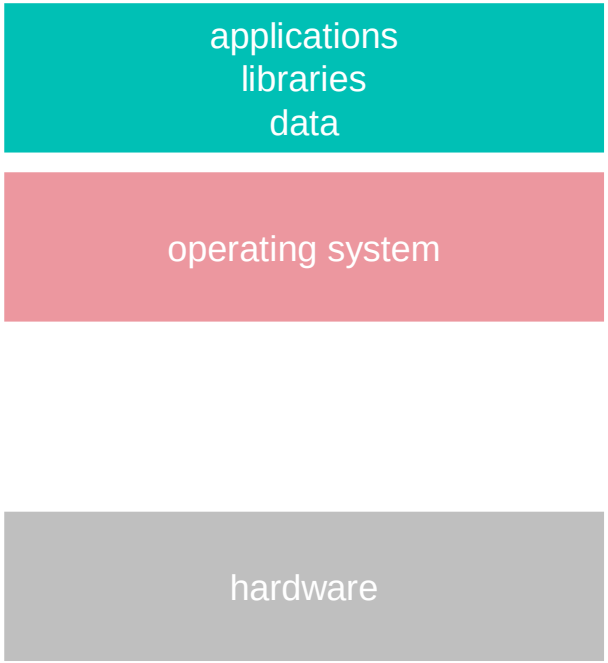
- Initial intrusion (e.g. exploit remote execution)
- Open remote access (e.g. reverse shell)
- Privilege escalation (e.g. see Lecture 1)
- Download the malicious payload (our rootkit)
- Install rootkit
- Perform malicious action on command
  - DDOS
  - Steal data
  - etc…

University of BRISTOL

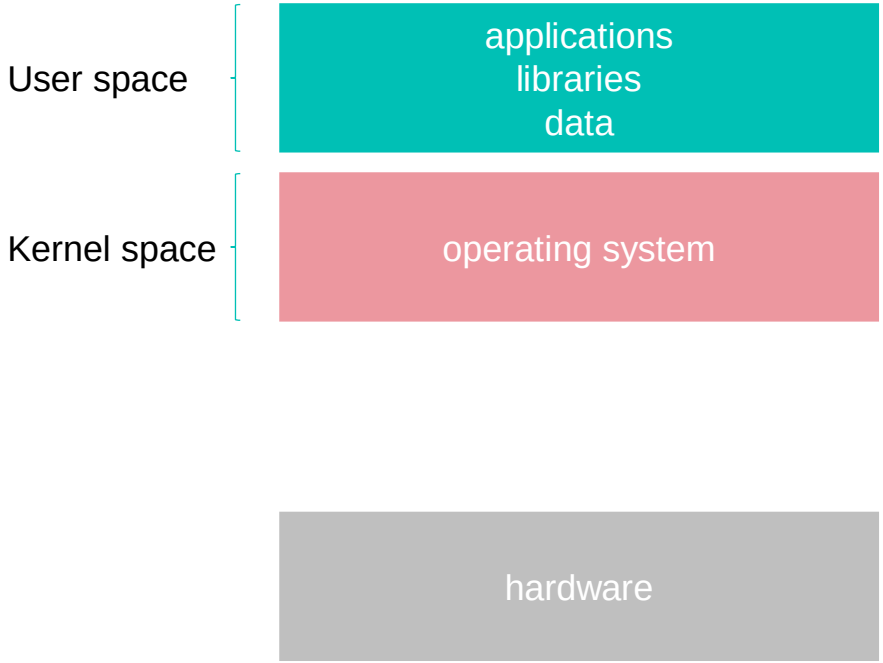
Kernel rootkit

bristol.ac.uk

Rootkit high-level understanding



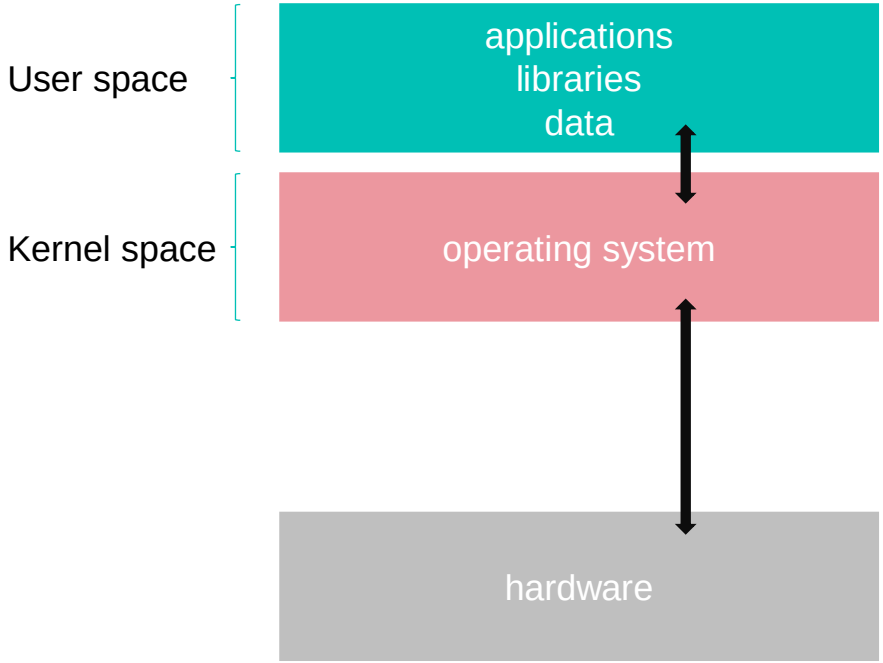
Rootkit high-level understanding



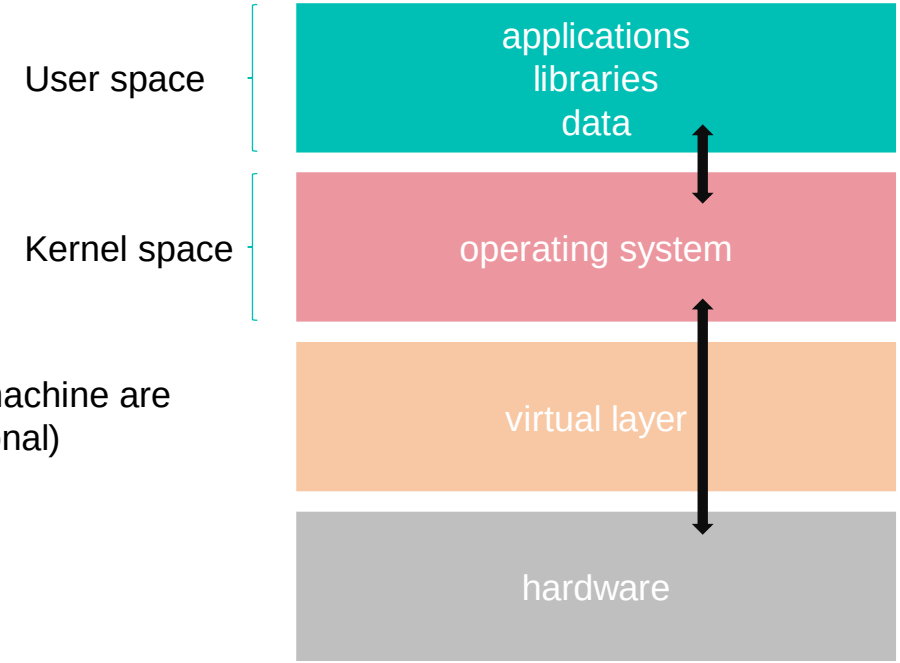
Where what user interact with exists

Where hardware can be controlled

Rootkit high-level understanding

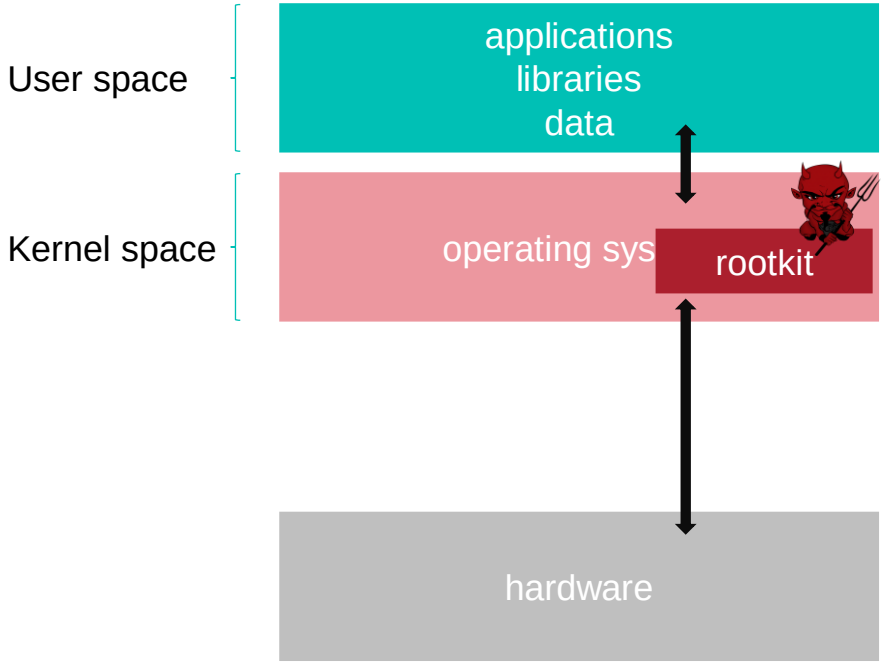


Rootkit high-level understanding



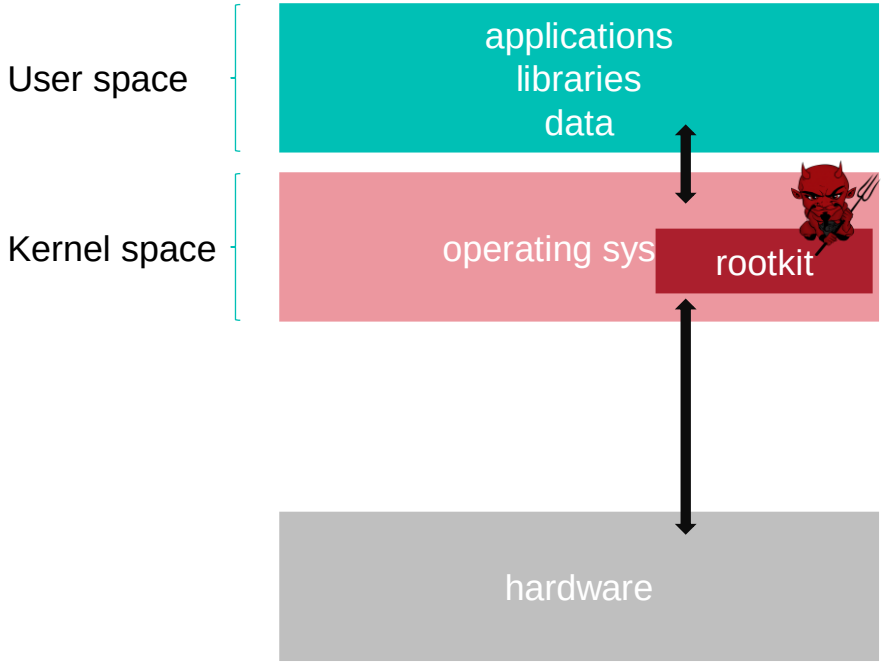
Where virtual machine are managed (optional)

Rootkit high-level understanding



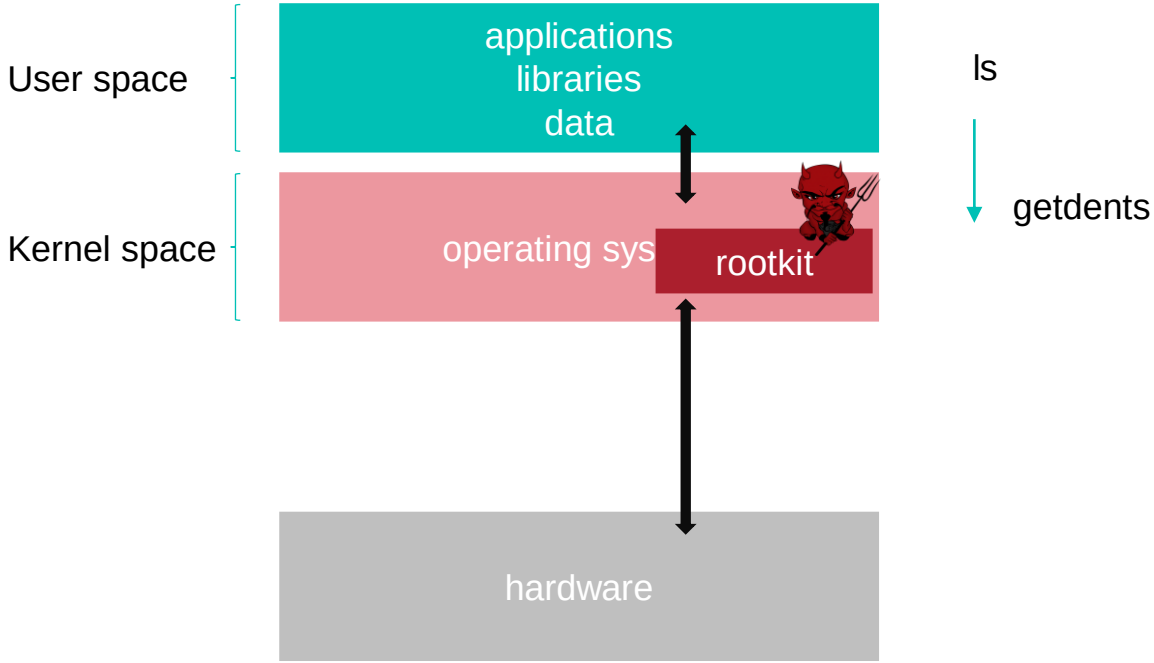
Goal hide malicious file/process etc.

Rootkit high-level understanding



ls

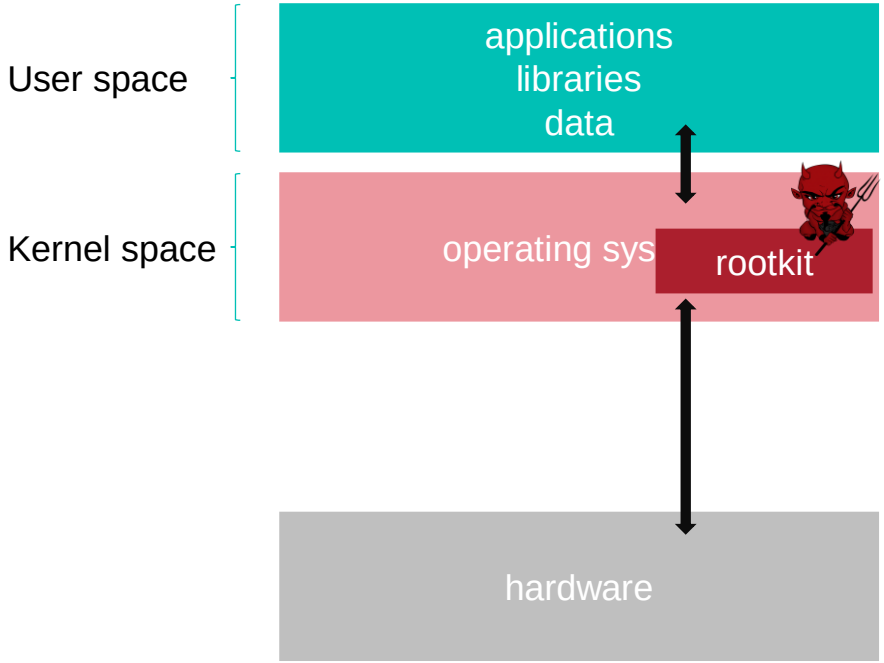
Rootkit high-level understanding



```
int getdents(unsigned int fd, struct linux_dirent *dirp, unsigned int count);
```

The system call **getdents**() reads several *linux_dirent* structures from the directory referred to by the open file descriptor *fd* into the buffer pointed to by *dirp*. The argument *count* specifies the size of that buffer.

Rootkit high-level understanding

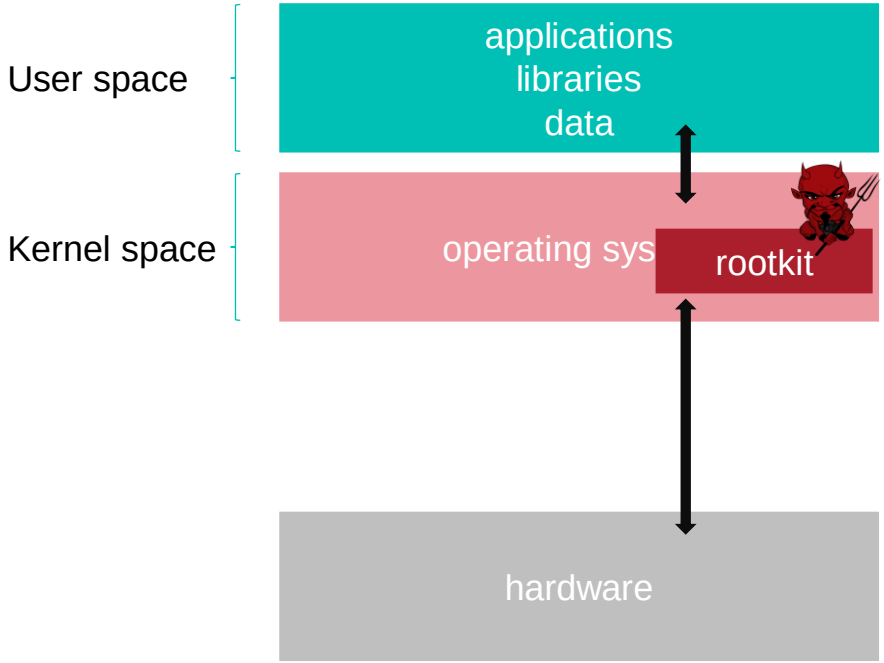


ls

getdents

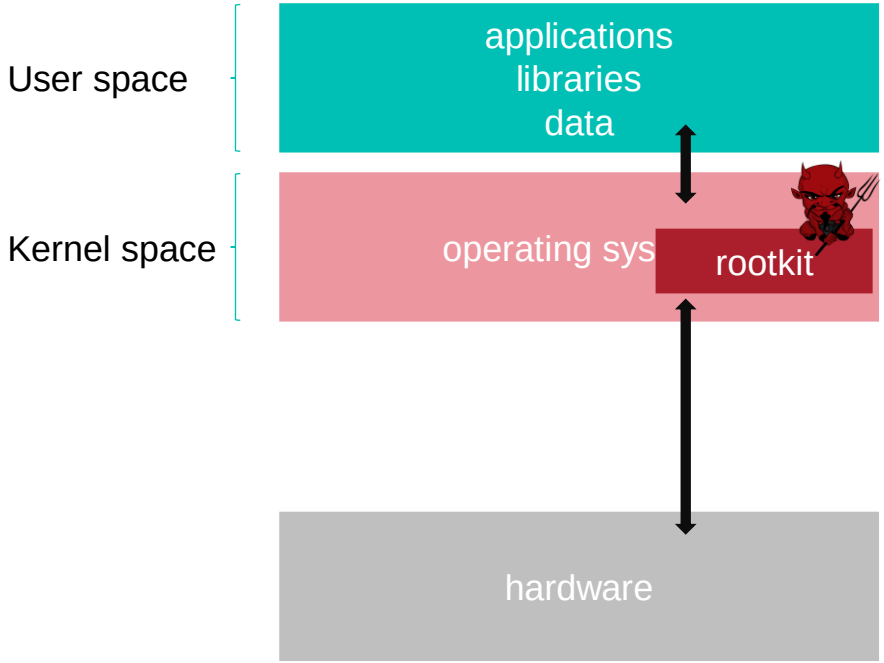
modify returned value to exclude ../malicious/

Rootkit high-level understanding



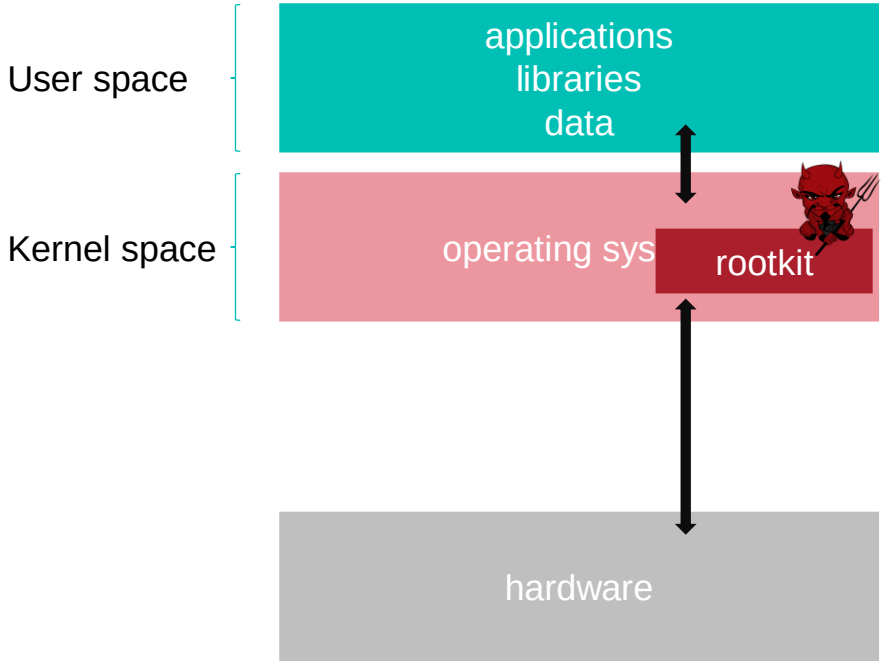
- Modify the behaviour of anything that could reveal malware presence, e.g.:
  - ls
  - ps
  - lsmod
  - etc…
- Give an easy mean to obtain root privileges, e.g.:
  - modify fork behaviour

Rootkit high-level understanding



- Roughly three techniques
  - Modify the kernel code;
  - “Hooking” modify where certain functions point to;
  - Modify data structure (e.g. active process list)
- More details during the lab!

Rootkit high-level understanding



You will build your own kernel rootkit during the lab!

Types of rootkit

- Application rootkit
- Kernel rootkit
- Virtualized rootkit
- Bootloader rootkit
- Hardware & firmware rootkit

Types of rootkit

- Application rootkit
- Kernel rootkit
- Virtualized rootkit
- Bootloader rootkit
- Hardware & firmware rootkit

They can be prevented/detected by going (at least) one layer down

Types of rootkit

- Application rootkit
- Kernel rootkit
- Virtualized rootkit
- Bootloader rootkit
- Hardware & firmware rootkit

See future video on TPM for an example

They can be prevented/detected by going (at least) one layer down