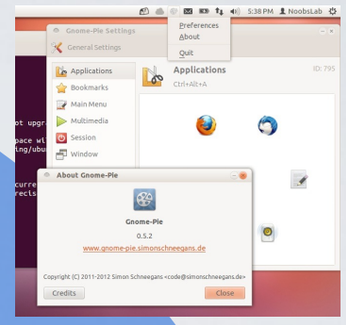
Operating Systems and Program (in)security

Thierry Sans

An Amateurish Introduction To Operating System

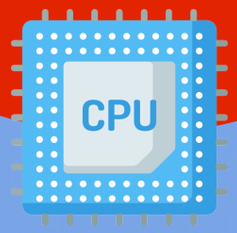
applications



user-space

system calls

Kernel



services (daemon)

Daemon

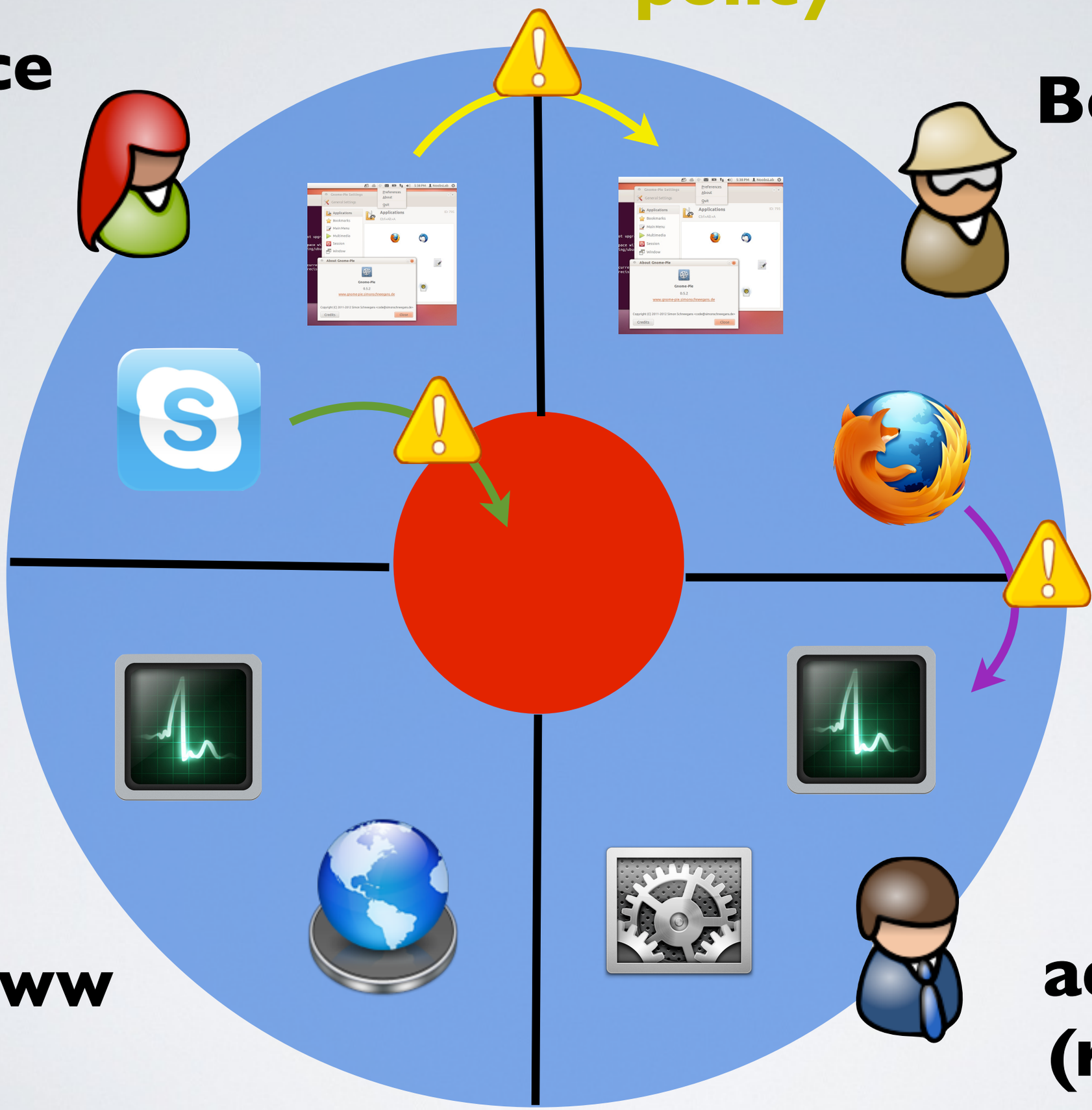
Daemons also called "services" are programs that run in the background

- System services
- Network services (servers)
- Monitoring
- Scheduled tasks

policy

Alice

Bob



www

admin
(root)

Hypothesis

➡ Programs are run by an authenticated user (authentication)

➡ Resources are accessed through programs (authorization)

➡ Every access is checked by the system (complete mediation)

✓ Everything is "secured" as long as long as the system is well configured and the programs behave as expected

◉ But ...

Threats

What can go wrong?

How can the security be compromised?

- A program can have an undesirable behavior either **by design** or **because of a bug**

Vulnerabilities

Malicious Program vs. Vulnerable Program

The program **has been** designed to compromise the security of the operating system

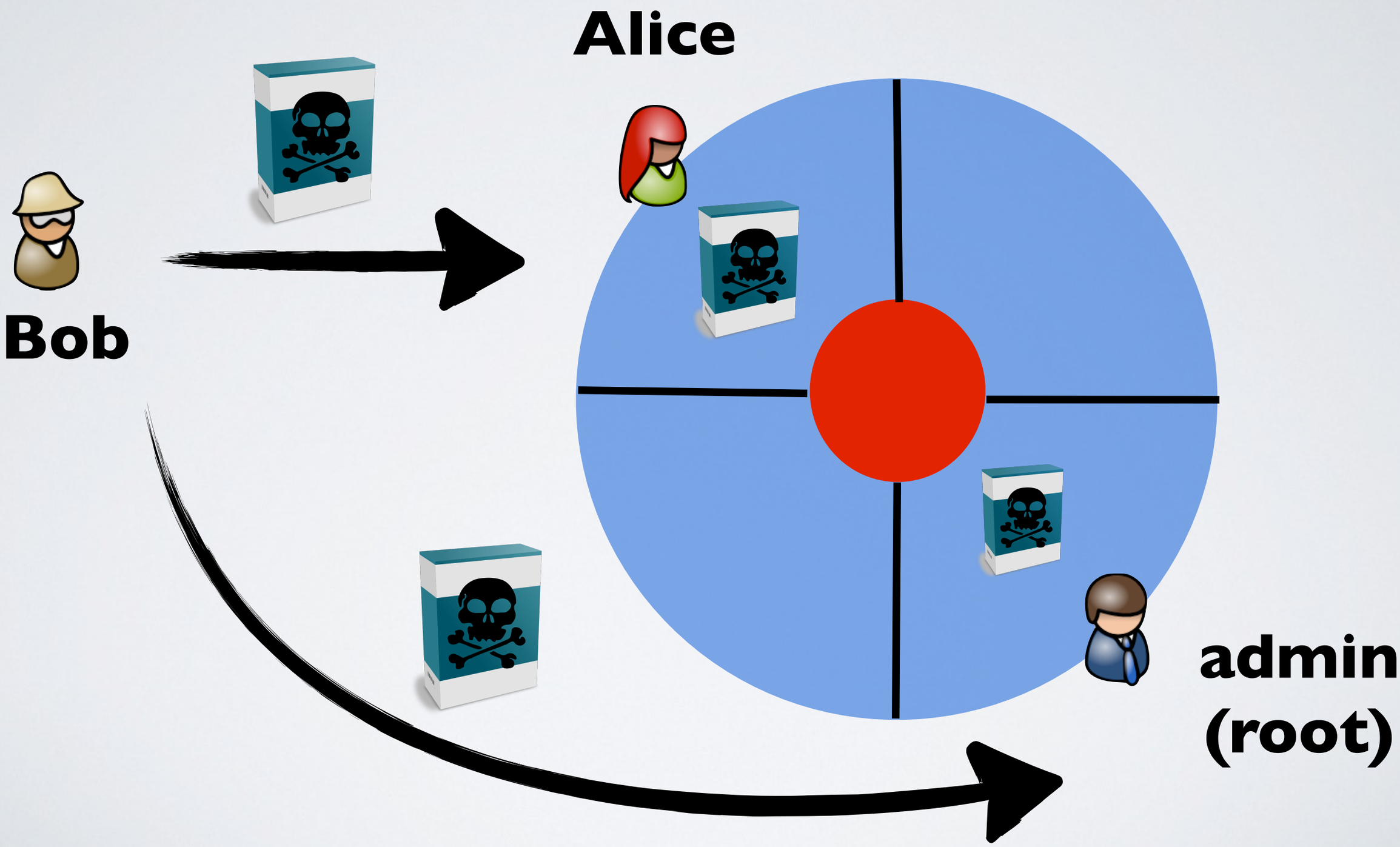
➡ The user executes a malware

The program **has not been** designed to compromise the security of the operating system

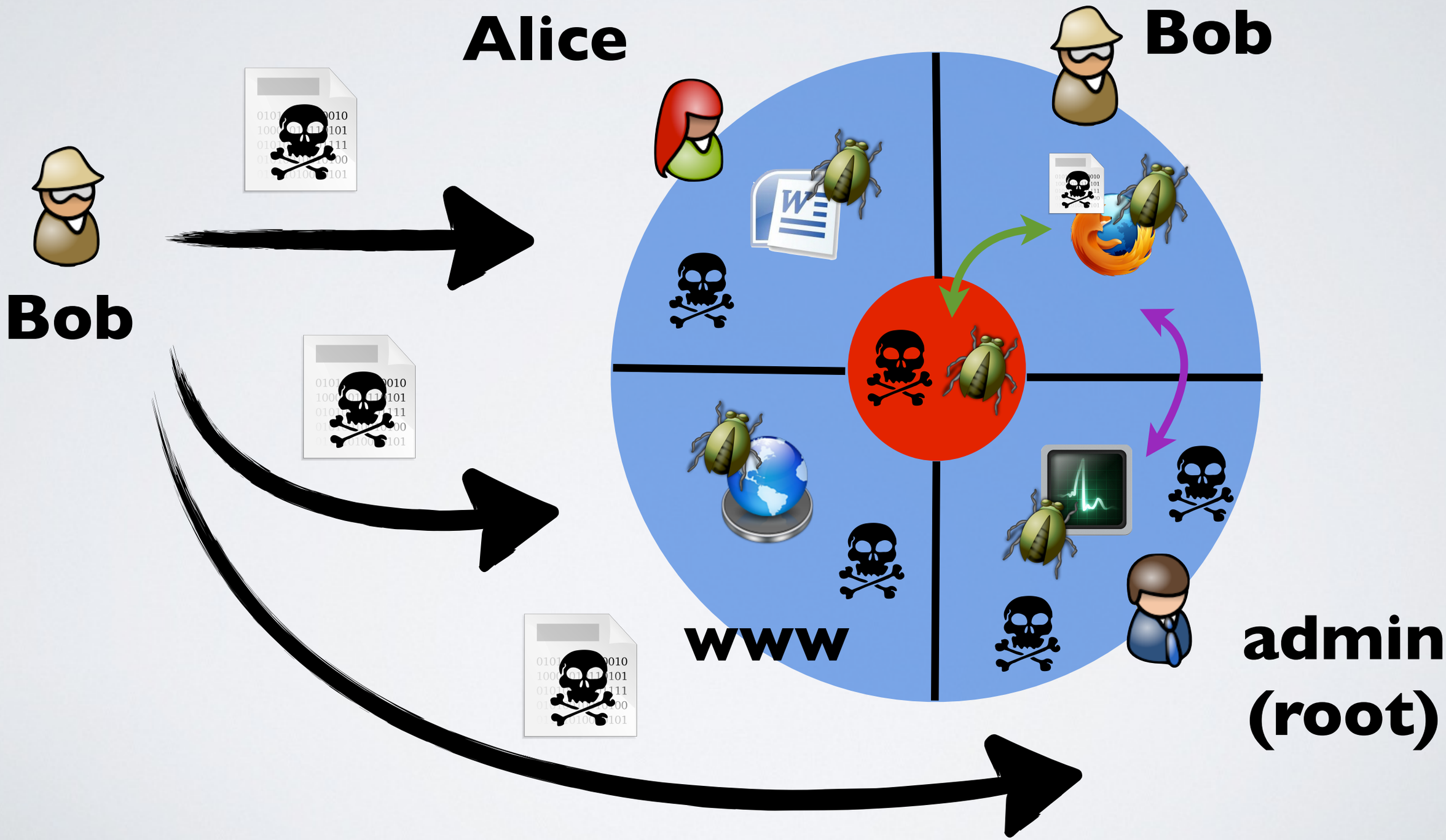
➡ The user executes a legitimate program that executes the malware

◉ **Code Execution Vulnerability** : a vulnerability that can be exploited to execute a malicious program

Malicious programs executed by the user



Malicious programs executed by other legitimate programs



What happen when a bug occurs?

Severity

- Nothing, the program and/or the OS are "fault tolerant"
- The program gives a wrong result or crashes but the security of the system is not compromised
- The resources are no longer accessible (locked) or the OS crashes
- The program computes something that it is not suppose to (malicious code)

How to find a program vulnerability?

- Find a bug yourself and investigate

- Take a look at CVE alerts
  (Common Vulnerabilities and Exposures)

Timeline of a vulnerability

The program is released with a vulnerability

A recommendation is issued

The patch is applied

The vulnerability is publicly disclosed (CVE alert)

A patch is released