

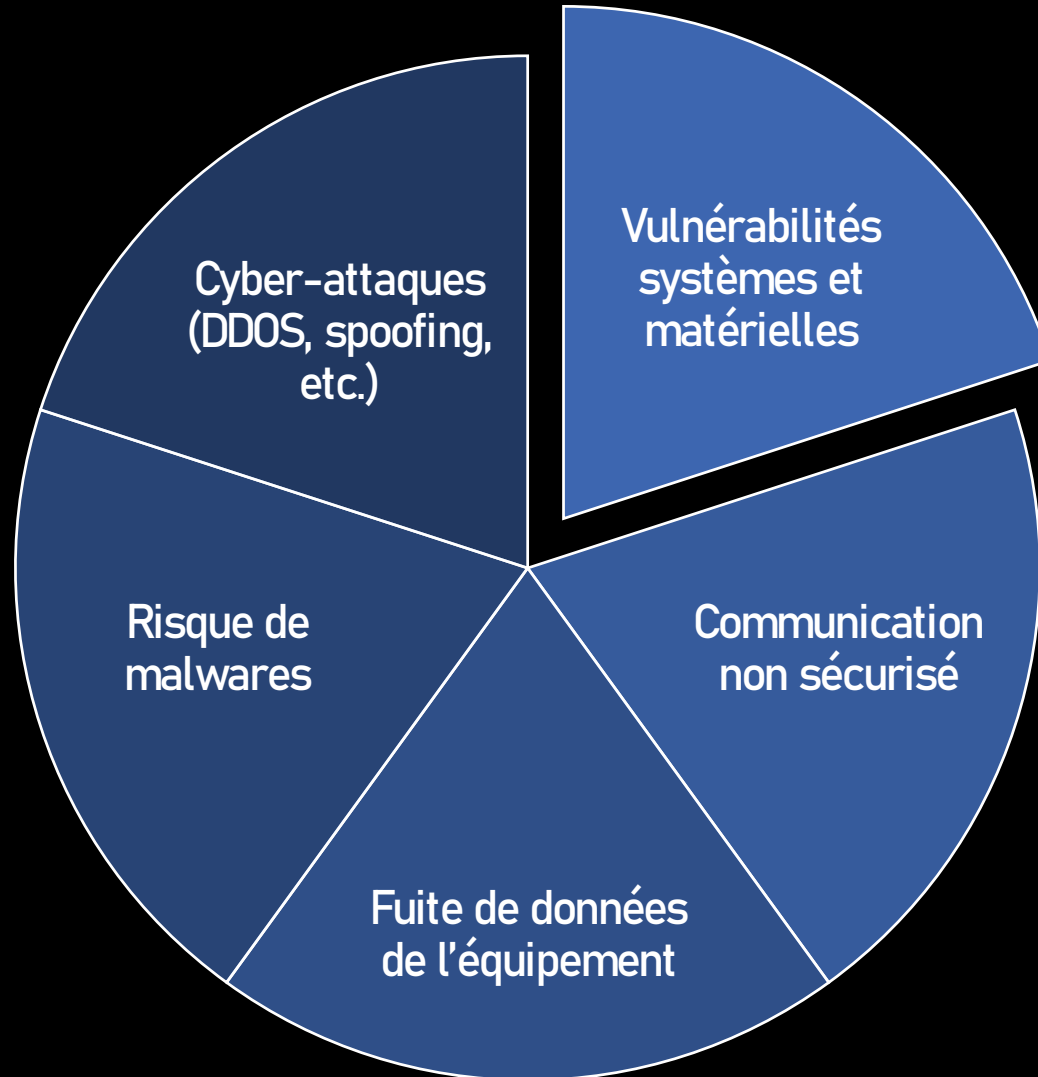
Vulnérabilité système et matérielle

ESIR2 – SRIO

Djob Mvondo

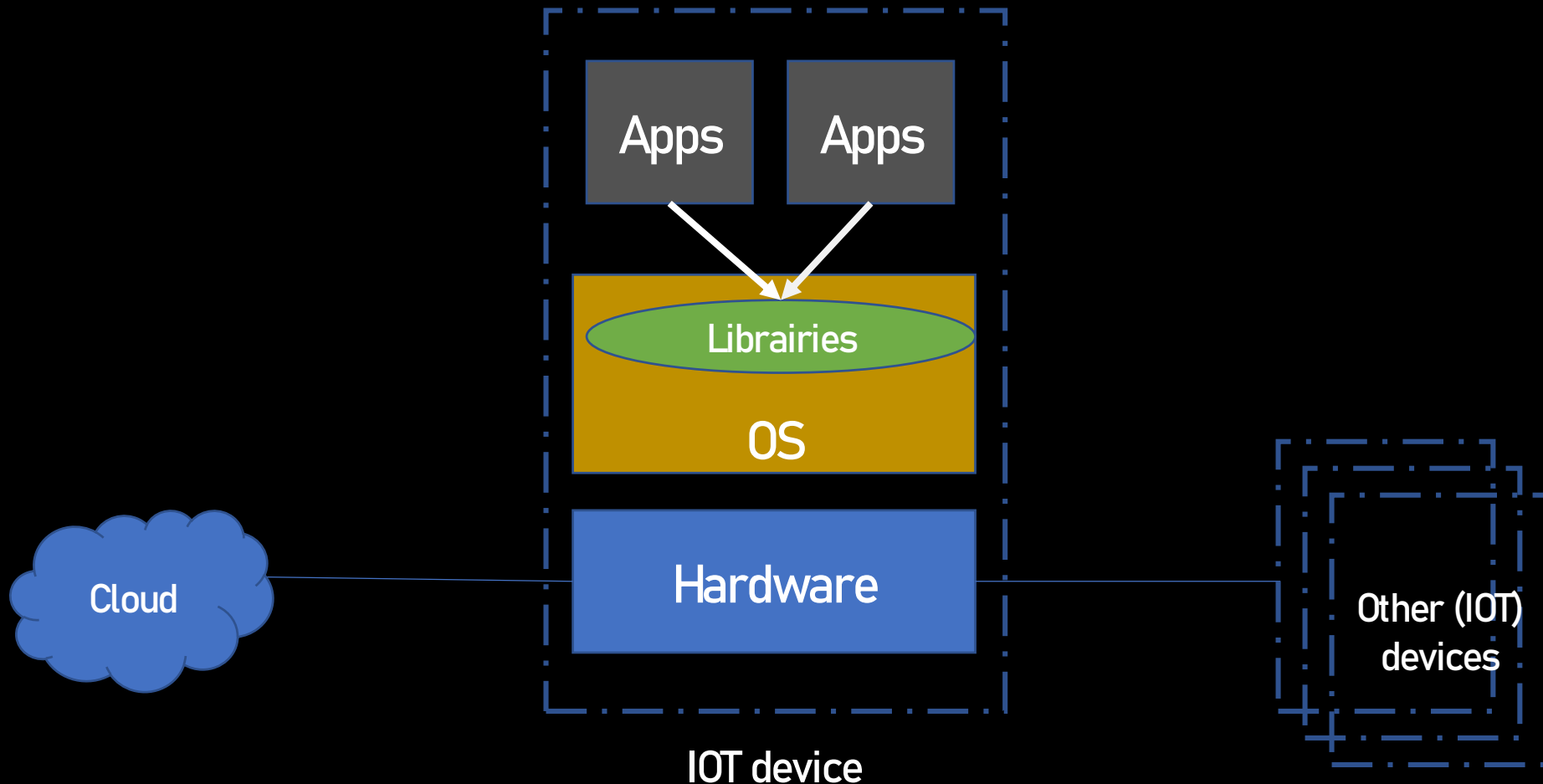
Rappel

Les problèmes de sécurités peuvent être groupés en **5** catégories



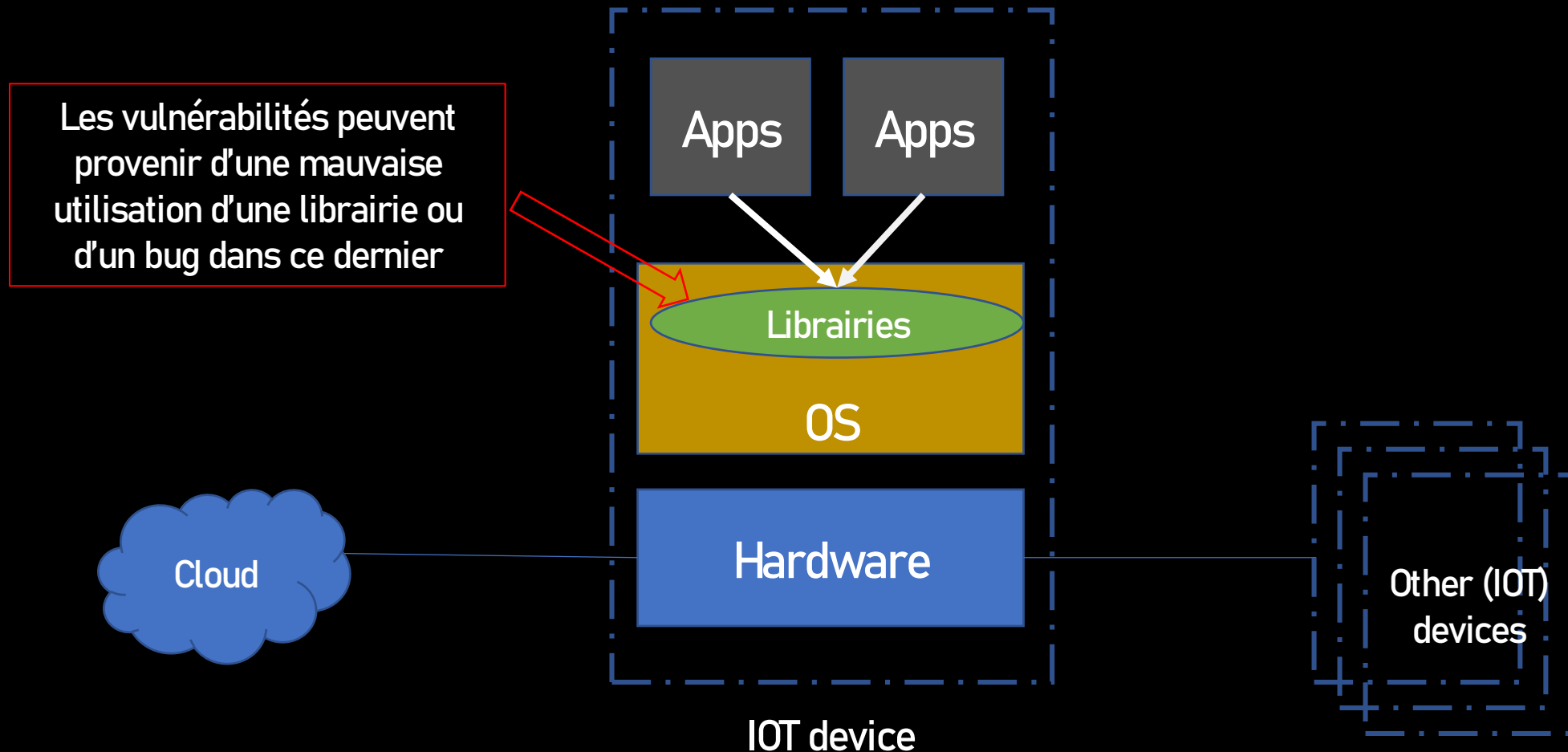
Ossature d'un équipement IOT

Un équipement IOT est composé d'une couche matérielle sur laquelle tourne un **système d'exploitation optimisé** pour l'équipement.

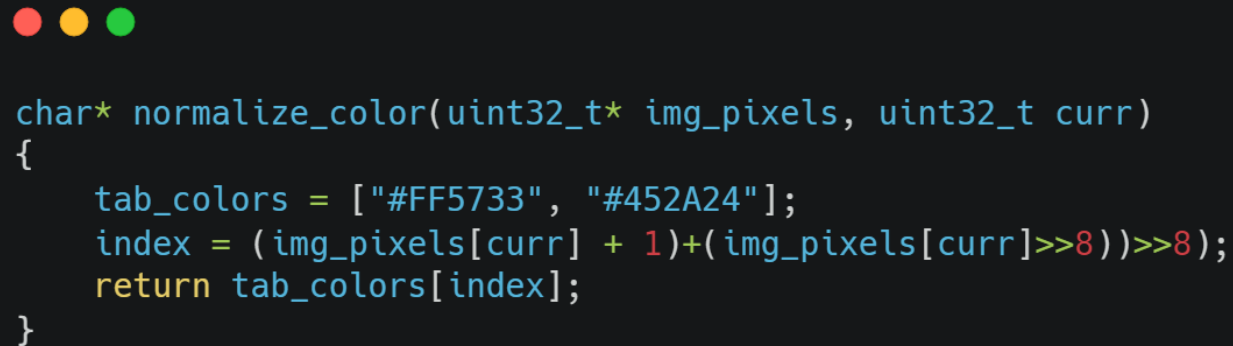


Ossature d'un équipement IOT

Un équipement IOT est composé d'une couche matérielle sur laquelle tourne un **système d'exploitation optimisé** pour l'équipement.



Exemple d'une vulnérabilité lié à l'utilisation d'une librairie



```
char* normalize_color(uint32_t* img_pixels, uint32_t curr)
{
    tab_colors = ["#FF5733", "#452A24"];
    index = (img_pixels[curr] + 1)+(img_pixels[curr]>>8)>>8);
    return tab_colors[index];
}
```

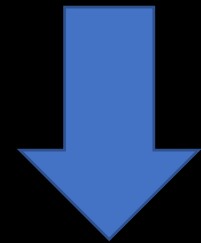
Prenez 10mn pour comprendre ce que le code essaye de faire

Exemple d'une vulnérabilité lié à l'utilisation d'une librairie



```
char* normalize_color(uint32_t* img_pixels, uint32_t curr)
{
    tab_colors = ["#FF5733", "#452A24"];
    index = (img_pixels[curr] + 1) + (img_pixels[curr] >> 8) >> 8;
    return tab_colors[index];
}
```

Quel est le problème avec ce code ?



Comment pouvez-vous le corriger ?

Imaginez les effets sur une caméra de sécurité 😞

```

import java.sql.*;
import java.io.*;

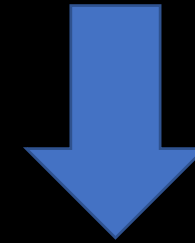
public class JDBCTransform
{
    @endpoint("/transform")
    void transform(String[] args)
    {
        System.out.println("transforming user inputs.");
        /* Logic to connect to the encrypted database */
        /* ... */
        String query = "select name, command, time from requests";
        String name, command, time = "";
        try
        {
            /* .... */
            ResultSet rs = stmt.executeQuery(query);
            while (rs.next())
            {
                name = rs.getString(1);
                command = rs.getString(2);
                time = rs.getString(3);
            }
            String fileName = "./useforEasyTransform.txt";

            // Write the content in file
            try(BufferedWriter bufferedWriter = new BufferedWriter(new FileWriter(fileName))) {

                bufferedWriter.write(name+"\n"+time);
            } catch (IOException e) {
                // Exception handling
            }
            /* ... Read the file and transform the file
             * then persist result in "transform" table
             */
            conn.close();
            System.out.println("Disconnected from database");
        } catch (Exception e)
        {
            e.printStackTrace();
        }
    }
}

```

Quel est le problème
avec ce code ?



Comment pouvez-vous
le corriger ?

```

import java.sql.*;
import java.io.*;

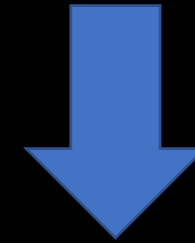
public class JDBCTransform
{
    @endpoint("/transform")
    void transform(String[] args)
    {
        System.out.println("transforming user inputs.");
        /* Logic to connect to the encrypted database */
        /* ... */
        String query = "select name, command, time from requests";
        String name, command, time = "";
        try
        {
            /* .... */
            ResultSet rs = stmt.executeQuery(query);
            while (rs.next())
            {
                name = rs.getString(1);
                command = rs.getString(2);
                time = rs.getString(3);
            }
            String fileName = "./useforEasyTransform.txt";

            // Write the content in file
            try(BufferedWriter bufferedWriter = new BufferedWriter(new FileWriter(fileName))) {

                bufferedWriter.write(name+"\n"+time);
            } catch (IOException e) {
                // Exception handling
            }
            /* ... Read the file and transform the file
             * then persist result in "transform" table
             */
            conn.close();
            System.out.println("Disconnected from database");
        } catch (Exception e)
        {
            e.printStackTrace();
        }
    }
}

```

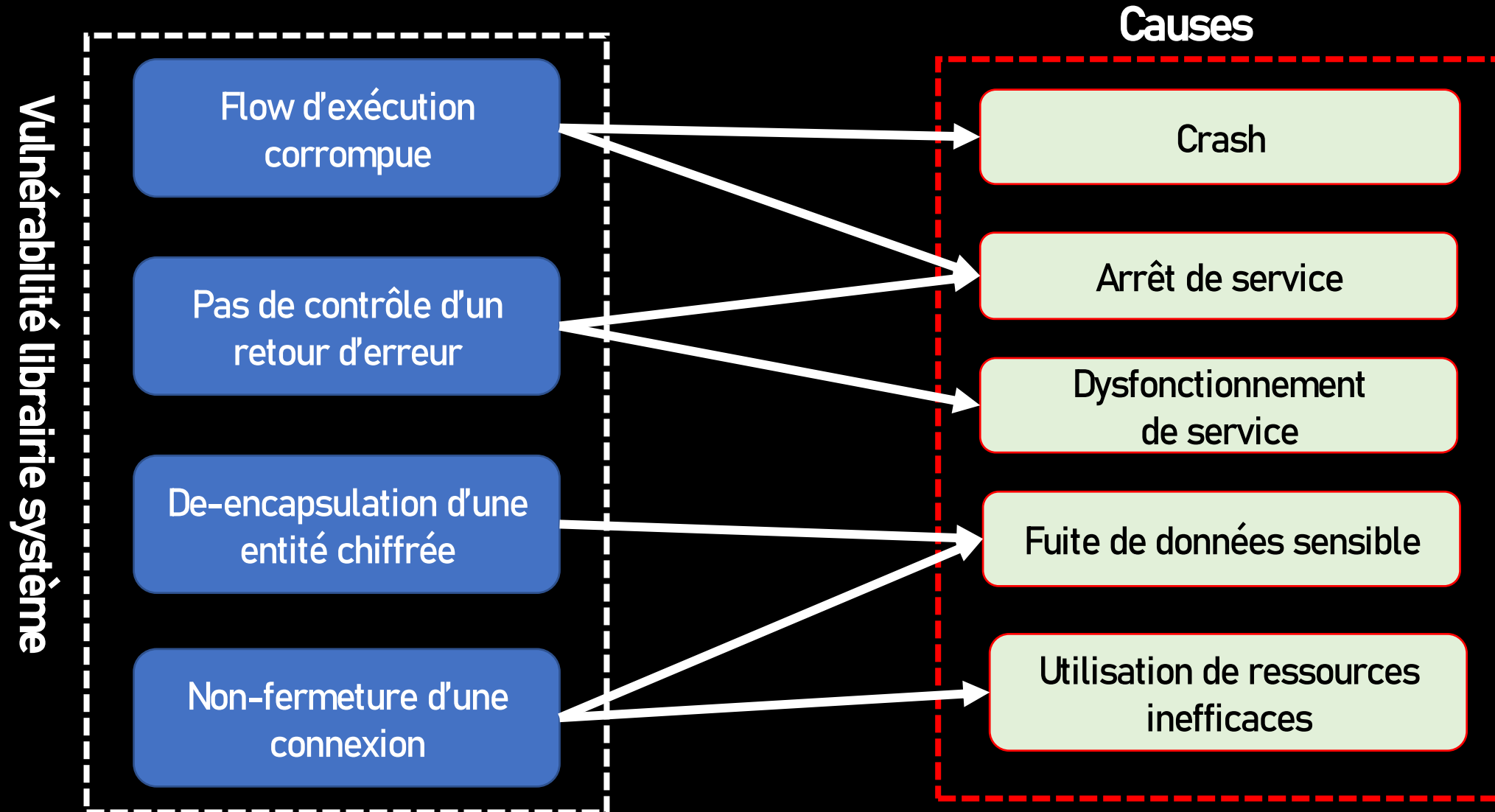
Quel est le problème
avec ce code ?



Comment pouvez-vous
le corriger ?

**Imaginez les effets sur
une assistant maison**

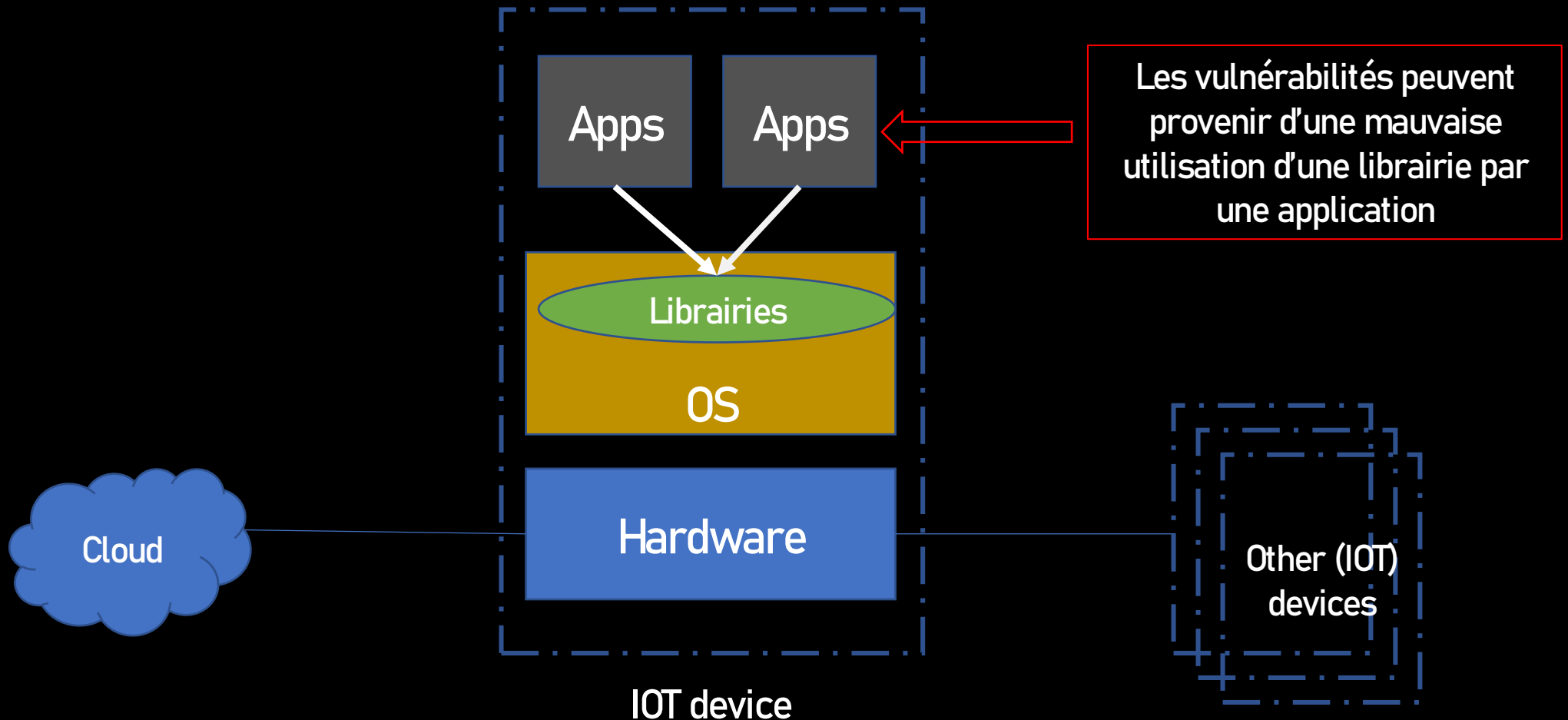
Les types de vulnérabilités systèmes



Essayons de faire correspondre

Ossature d'un équipement IOT

Au-delà d'une vulnérabilité dans les librairies systèmes, la cause peut venir d'une **mauvaise exploitation** par les applications.



Exemple: **First and second order Injection SQL (SQLi)**

Mauvaise exploitation des données d'entrée par l'application

User 1

Song=arianna grande

SELECT title, stream, author
FROM Songs WHERE song =
'arianna grande'

IOT device search routine

```
String query = "SELECT title, stream, author  
                FROM Songs WHERE  
                song = '"+ song + "'";  
Statement statement = connection.createStatement();  
ResultSet resultSet = statement.executeQuery(query)
```

Que va-t-il
arriver ? Pour
chaque utilisateur

...

No problem here



<https://myiotdevice?id=23411&songs=--->

Exemple: First and second order Injection SQL (SQLi)

Mauvaise exploitation des données d'entrée par l'application

User 2

Song=zamina zangalewa' or 1=1

```
SELECT title, stream, author
FROM Songs WHERE song =
'zamina zangalewa' or 1=1
```

Always true

Problem here:
All entries will be
retrieved by the user



IOT device search routine

```
String query = "SELECT title, stream, author
                FROM Songs WHERE
                song = '"+ song + "'";
Statement statement = connection.createStatement();
ResultSet resultSet = statement.executeQuery(query)
```

Que va-t-il
arriver ? Pour
chaque utilisateur
...

<https://myiotdevice?id=23411&songs=--->

Exemple: **First and second order Injection SQL (SQLi)**

Mauvaise exploitation des données d'entrée par l'application

User 3

Song='Ma 6t a craqué'

```
SELECT title, stream, author
FROM Songs WHERE song = "
Ma 6t a craqué
```

IOT device search routine

```
String query = "SELECT title, stream, author
                FROM Songs WHERE
                song = '"+ song + "'";
Statement statement = connection.createStatement();
ResultSet resultSet = statement.executeQuery(query)
```

Que va-t-il
arriver ? Pour
chaque utilisateur

...

Error, invalid syntax

Problem here:
Lead to an error if not
well handled



<https://myiotdevice?id=23411&songs=--->

Exemple: **First and second order Injection SQL (SQLi)**

Mauvaise exploitation des données d'entrée par l'application

User 4

IOT device search routine

Song='; update users set password='roboto' where user='administrator'---

SELECT title, stream, author
FROM Songs WHERE song =
"; update users set
password='roboto' where
user='administrator' craqué

```
String query = "SELECT title, stream, author  
                FROM Songs WHERE  
                song = '"+ song + "'";  
Statement statement = connection.createStatement();  
ResultSet resultSet = statement.executeQuery(query)
```

Que va-t-il
arriver ? Pour
chaque utilisateur
...

Problem here:
Database admin
password will be updated



<https://myiotdevice?id=23411&songs=--->

Exemple: **First and second order Injection SQL (SQLi)**

First order injection SQL

User 1

Song=arianna grande

User 2

Song=zamina zangalewa' or 1=1

User 3

Song='Ma 6t a craqué

User 4

Song='; update users set password='roboto' where user='administrador'--

Second order injection SQL

IOT device search routine

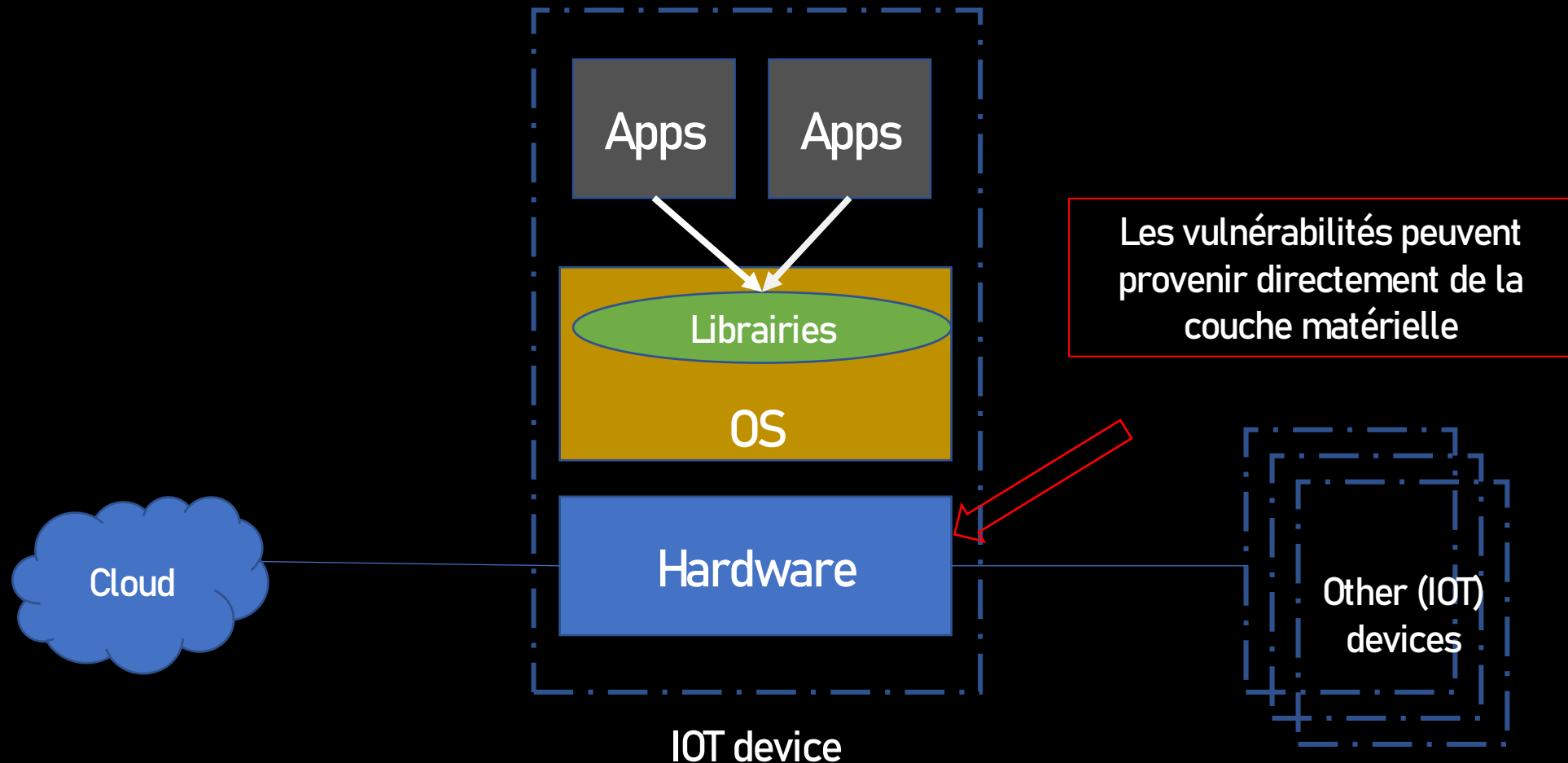
```
String query = "SELECT title, stream, author  
FROM Songs WHERE  
song = '"+ song + "'";  
Statement statement = connection.createStatement();  
ResultSet resultSet = statement.executeQuery(query)
```

Quelle est la différence ?

<https://myiotdevice?id=23411&songs=--->

Ossature d'un équipement IOT

Biensur il peut y avoir des vulnérabilités liés au matériel, **firmware défectueux, portes dérobées, accès par défaut**, etc.



Devoir 2

1. Documenter vous sur les mécanismes de préventions des SQLI pour votre langage préféré.
2. Mettre à jour la commande l'entrée de l'utilisateur quatre pour modifier le mot de passe du compte administrateur sans connaître le pseudo.
3. Choisissez deux équipements IOT de votre choix et ressortir des vulnérabilités matérielles connues (année de découverte, procédure d'exploitation, effets/conséquences).