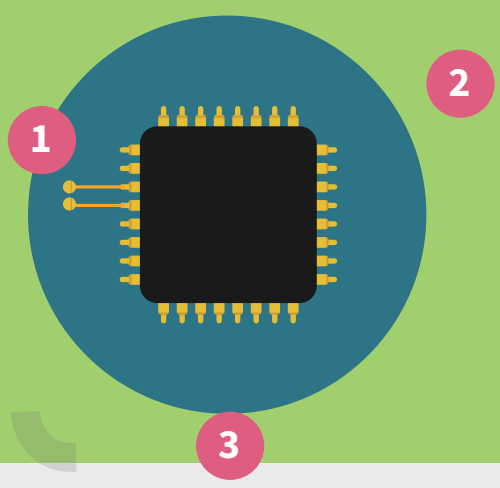
TOP 9

The Internet of Things

vulnerabilities and attack vectors

(And a few rules of thumb to mitigate the threats they pose)

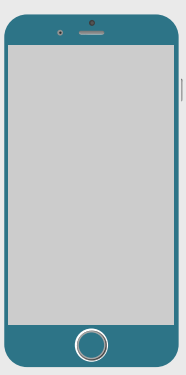
physical device



1 Exposed debug or serial headers
Avoid having JTAG/SWD headers or UART Terminals in production hardware

2 Side channels
Where available, use timing randomization in sensitive code to reduces the risk of exposing data on side channels

local ecosystem & WPAN

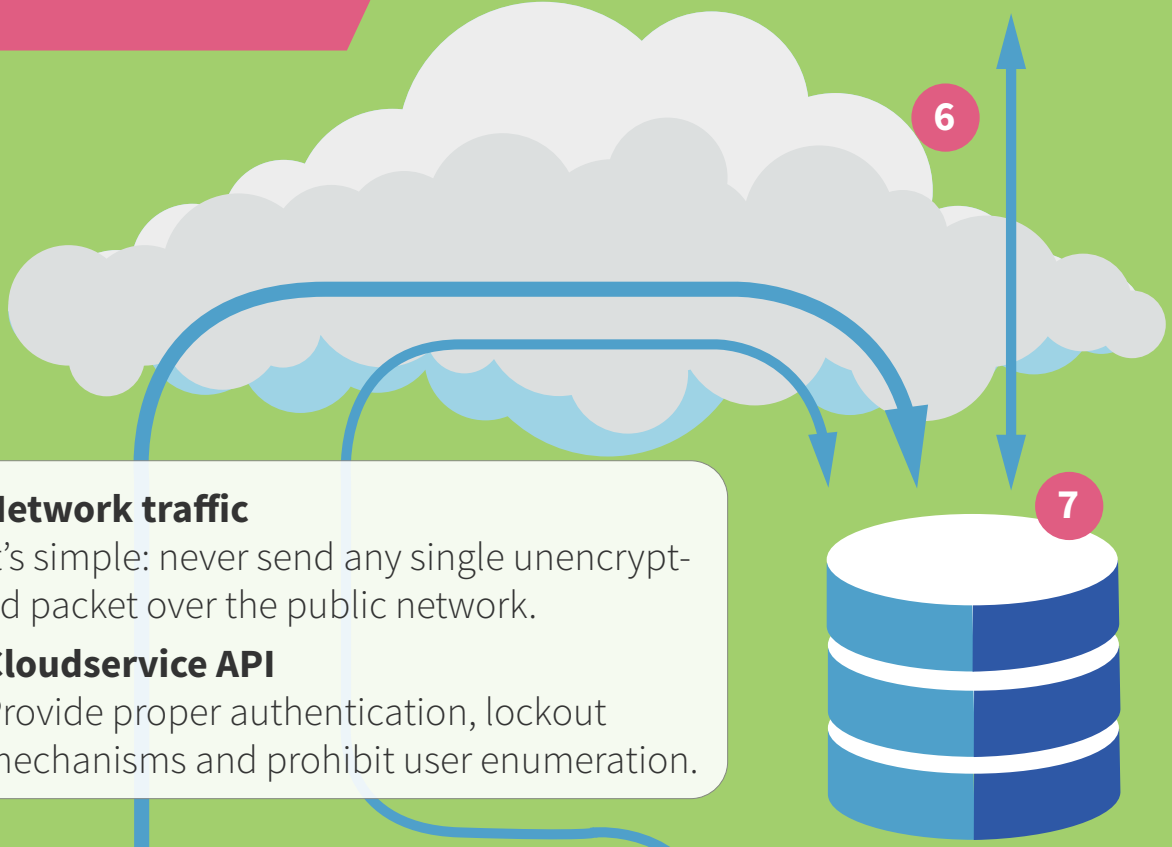


4 Wireless/mobile access
Implicit trust in local devices is a wildly underestimated risk. Identify and authenticate everything.

3 Network services
Disable any unused network services and keep everything else on the most recent patch level.

5 Edge device admin interface
Default credentials need to be changed, access restricted on network level.

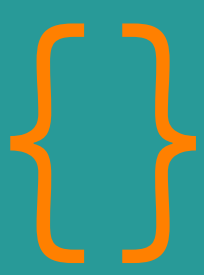
public Internet



6 Network traffic
It's simple: never send any single unencrypted packet over the public network.

7 Cloudservice API
Provide proper authentication, lockout mechanisms and prohibit user enumeration.

remote access



8 Web Interface
Authenticate, provide lockout mechanisms, adhere to general web app security standards.

9 REST APIs
Use rate-limiting, log requests and report suspicious usage patterns.

Laptop Image Designed by Freepik

imagine on