Telefónica

Ideas Locas CDO

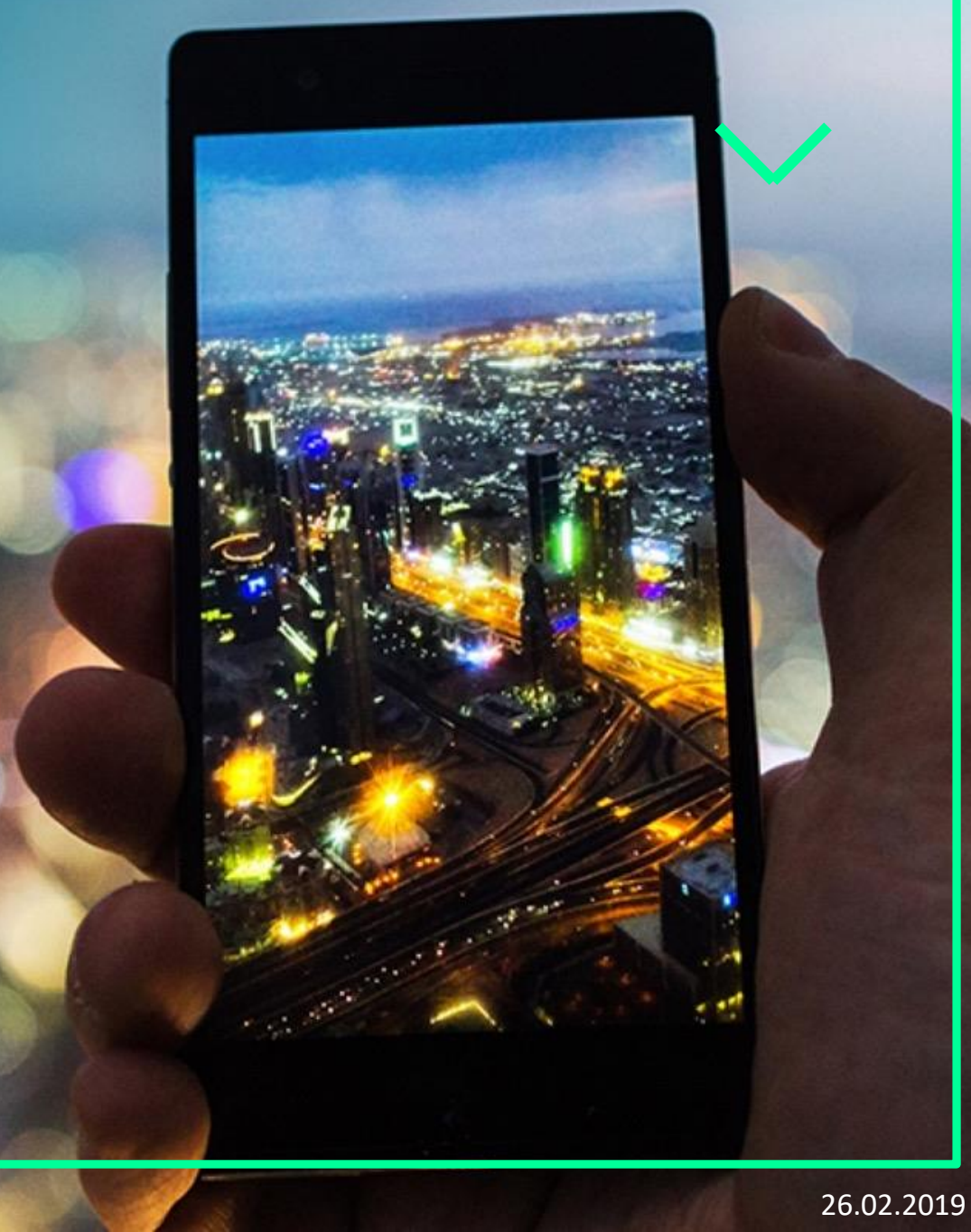
ElevenPaths

IoT SECURITY "Hack"

MOBILE WORLD CONGRESS 2019

Fran Ramírez
Security Researcher
Ideas Locas CDO Telefónica

Telefónica CYBER SECURITY UNIT



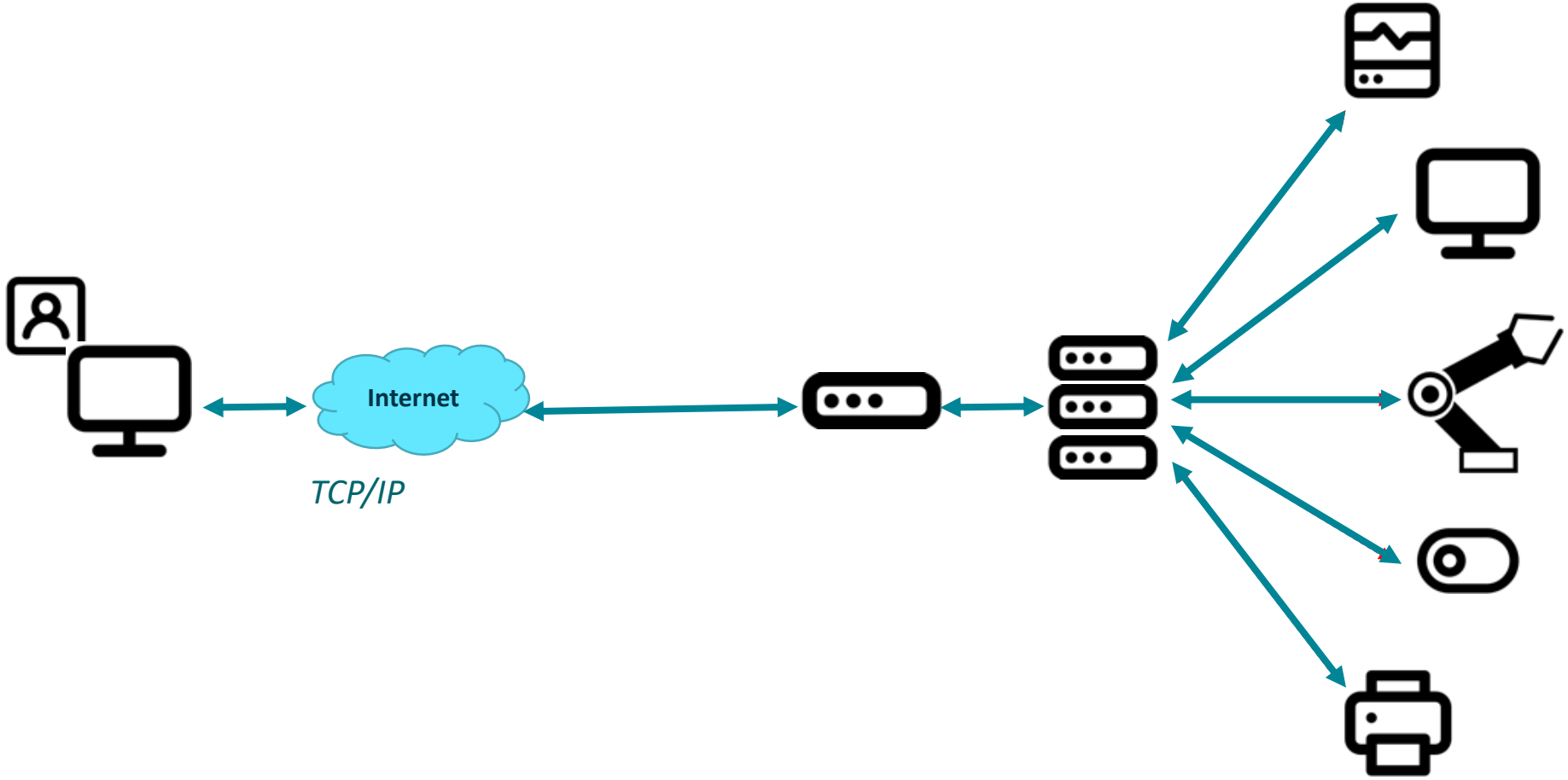
26.02.2019

Security is a critical business issue in IoT

Losing control of your IoT devices is a nightmare

Telefónica
Ideas Locas CDO
ElevenPaths

DDoS attacks (*Distributed Denial of Service*)

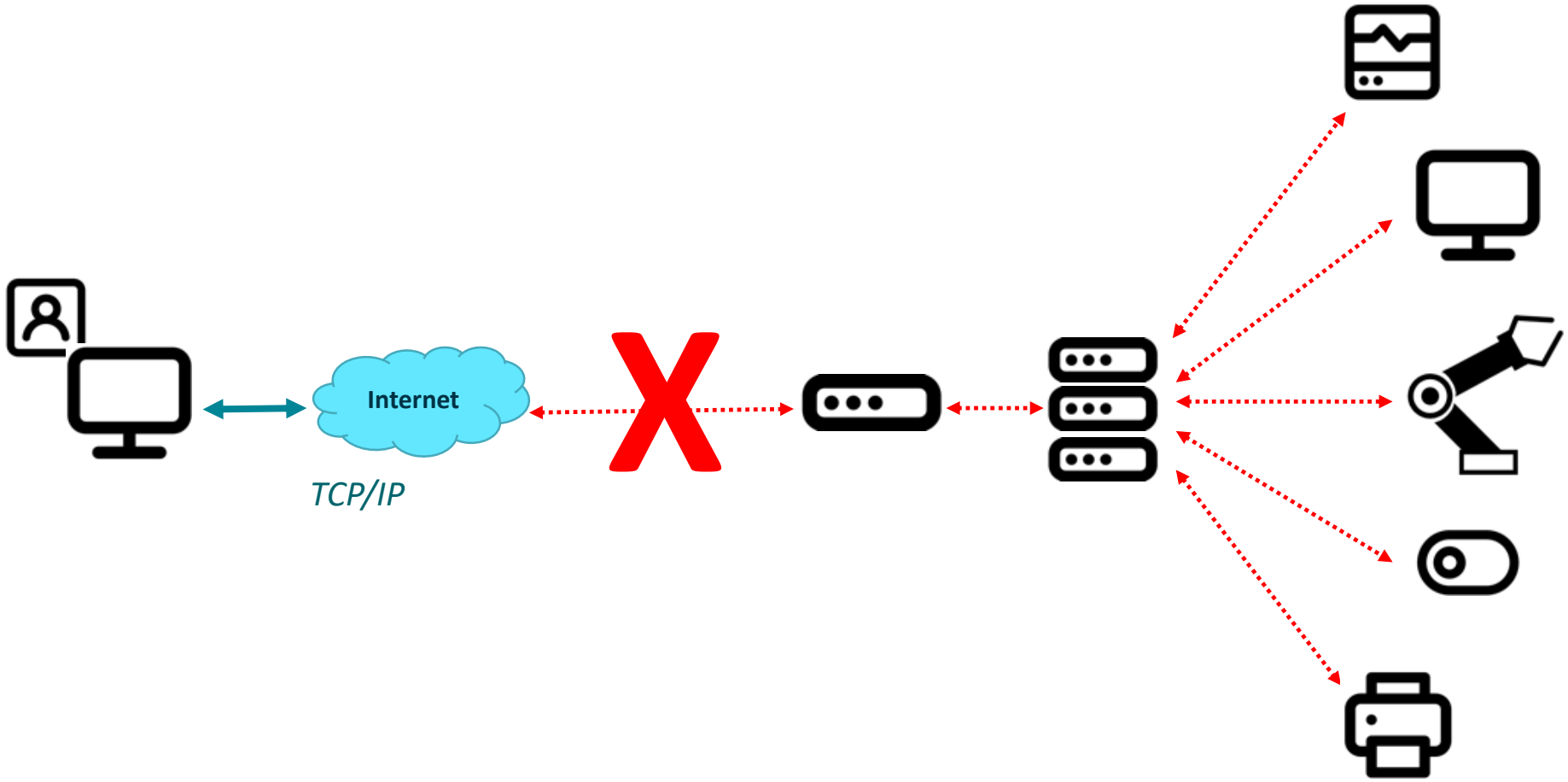


Security is a critical business issue in IoT

Losing control of your IoT devices is a nightmare

Telefónica
Ideas Locas CDO
ElevenPaths

DDoS attacks (*Distributed Denial of Service*)



Take back control of your IoT devices after a *DDoS* attack with *StackSMS*

Telefónica
Ideas Locas CDO
ElevenPaths

What is StackSMS?

*Stack**SMS***

- TCP like communication layer
- It works over GSM network (no Internet or 2G,3G,4G or 5G required)
- Based on SMS architecture
- Secure data integrity and confidentiality (PSK, AES-CTR, etc).
- Open Source SDK available
- Easy to implement using Python, Android and Node.js

Why StackSMS?

- Adds an alternative secure communication channel to your infrastructure (GSM)
- Take back control of a compromised architecture sending any task to any device (bypassing Internet)
- Allows to do almost any task on your system (SDK ready, DIY)

How it Works?

Telefónica
Ideas Locas CDO
ElevenPaths

1

Build your app

Create your own app with the SDK

2

Send the task

Send the task to your infrastructure

3

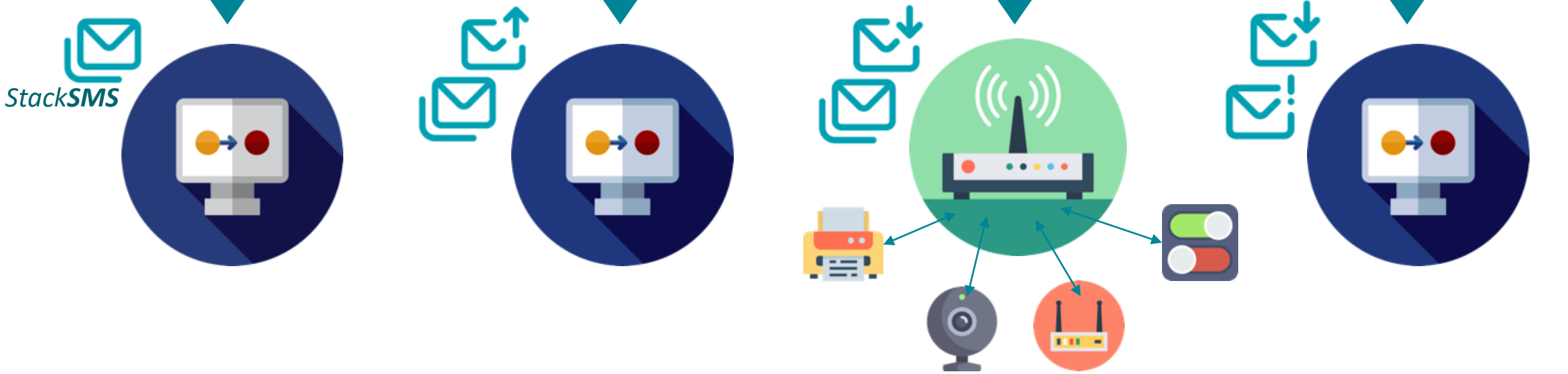
Run the task

Task will be executed in the device assigned by the infrastructure

4

Receive info

StackSMS will send the result of the execution of the task



Telefónica

Ideas Locas CDO

ElevenPaths

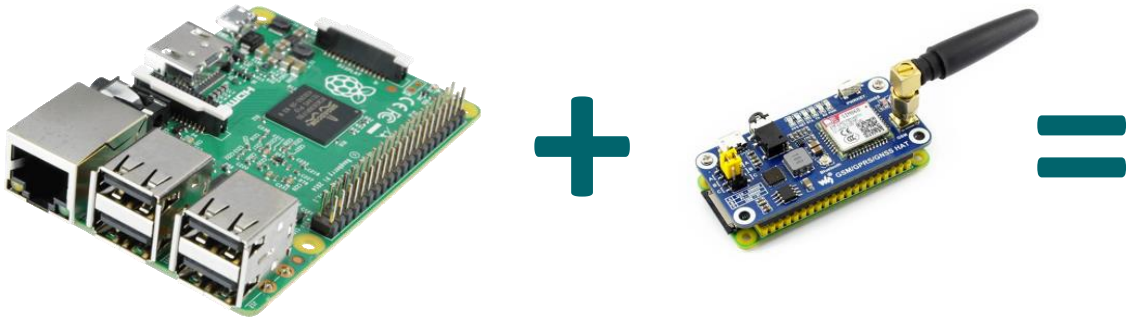
Hack DEMO

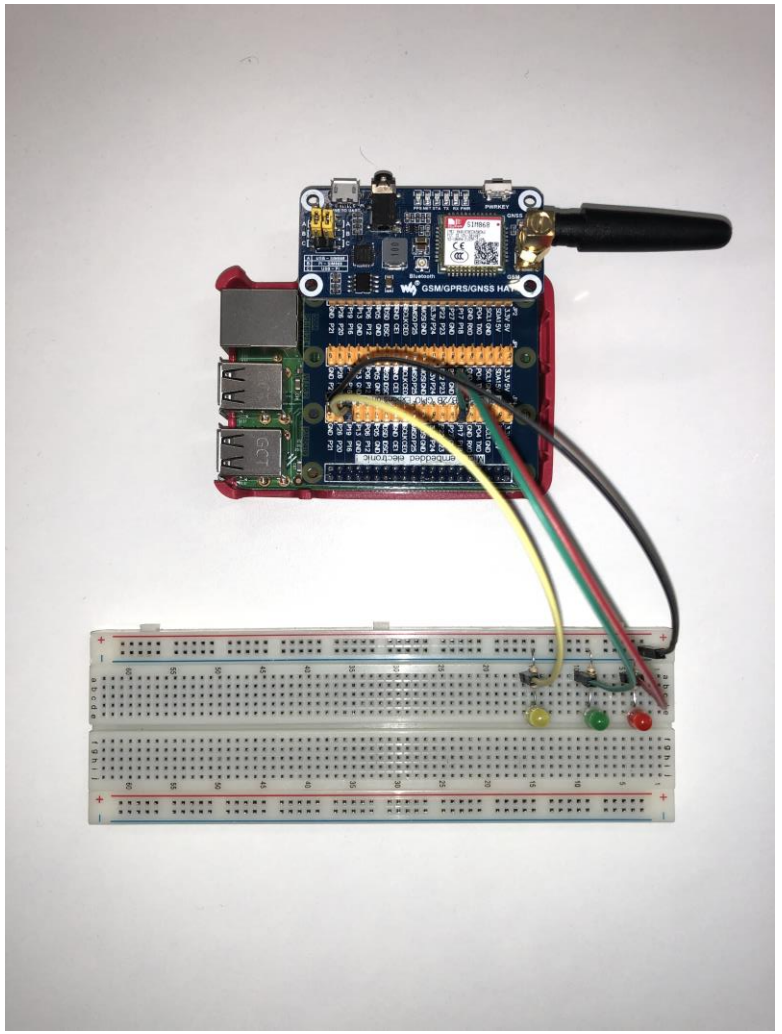
Take back control of your IoT devices after a *DDoS* attack with *StackSMS*

DEMO.
StackSMS with Raspberry Pi

Telefónica
Ideas Locas CDO
ElevenPaths

ID	SYN	ACK	PSH	FIN	CIPHER	15bits
00000000 - 11111111	0 - 1	0 - 1	0 - 1	0 - 1	000 - 111	
KEY	sBEGIN					16bits
00000000 - 11111111	00000000 - 11111111					
Data						N bits
N bits						

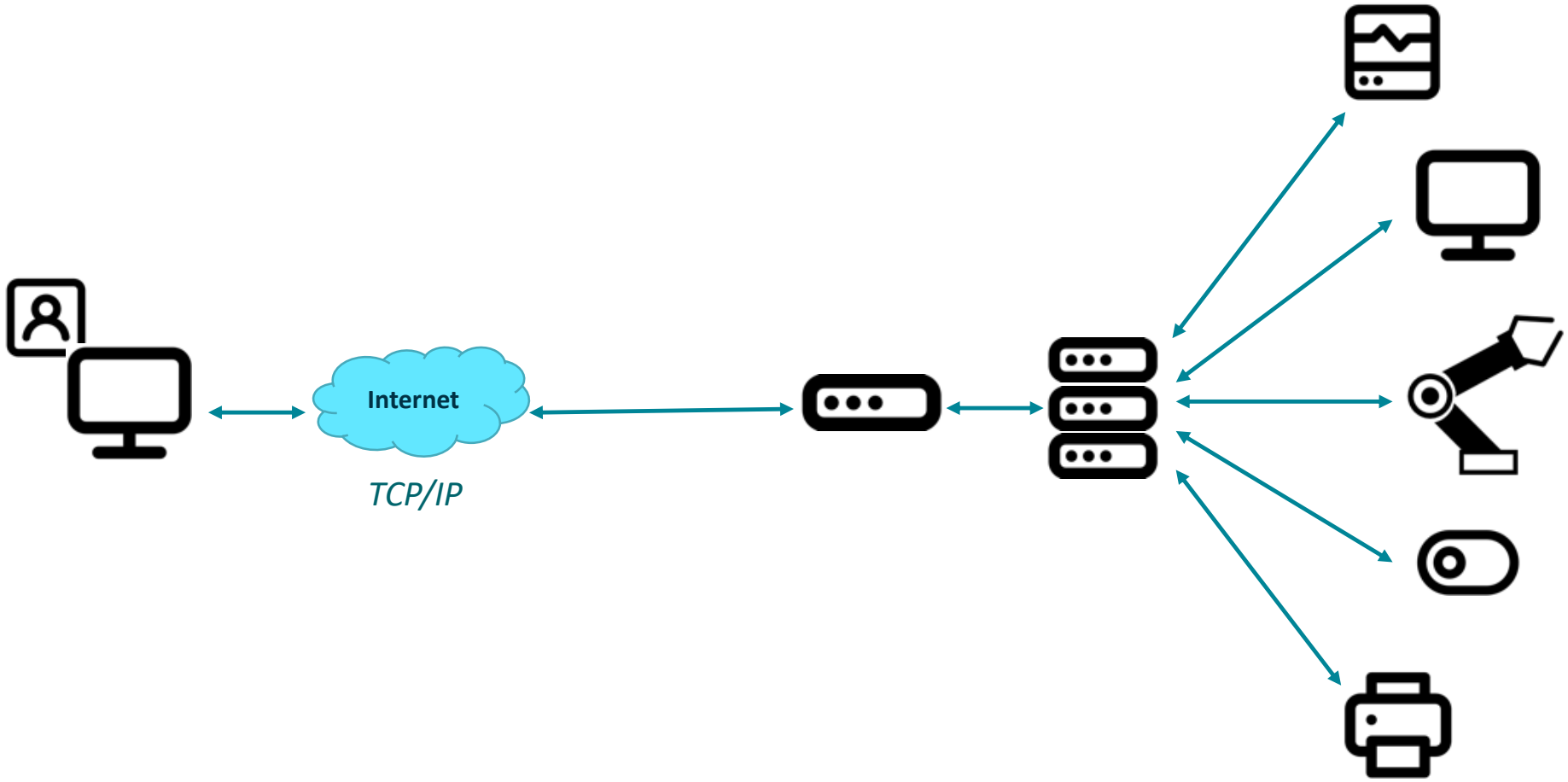




How to take back control of your system after a DDoS attack

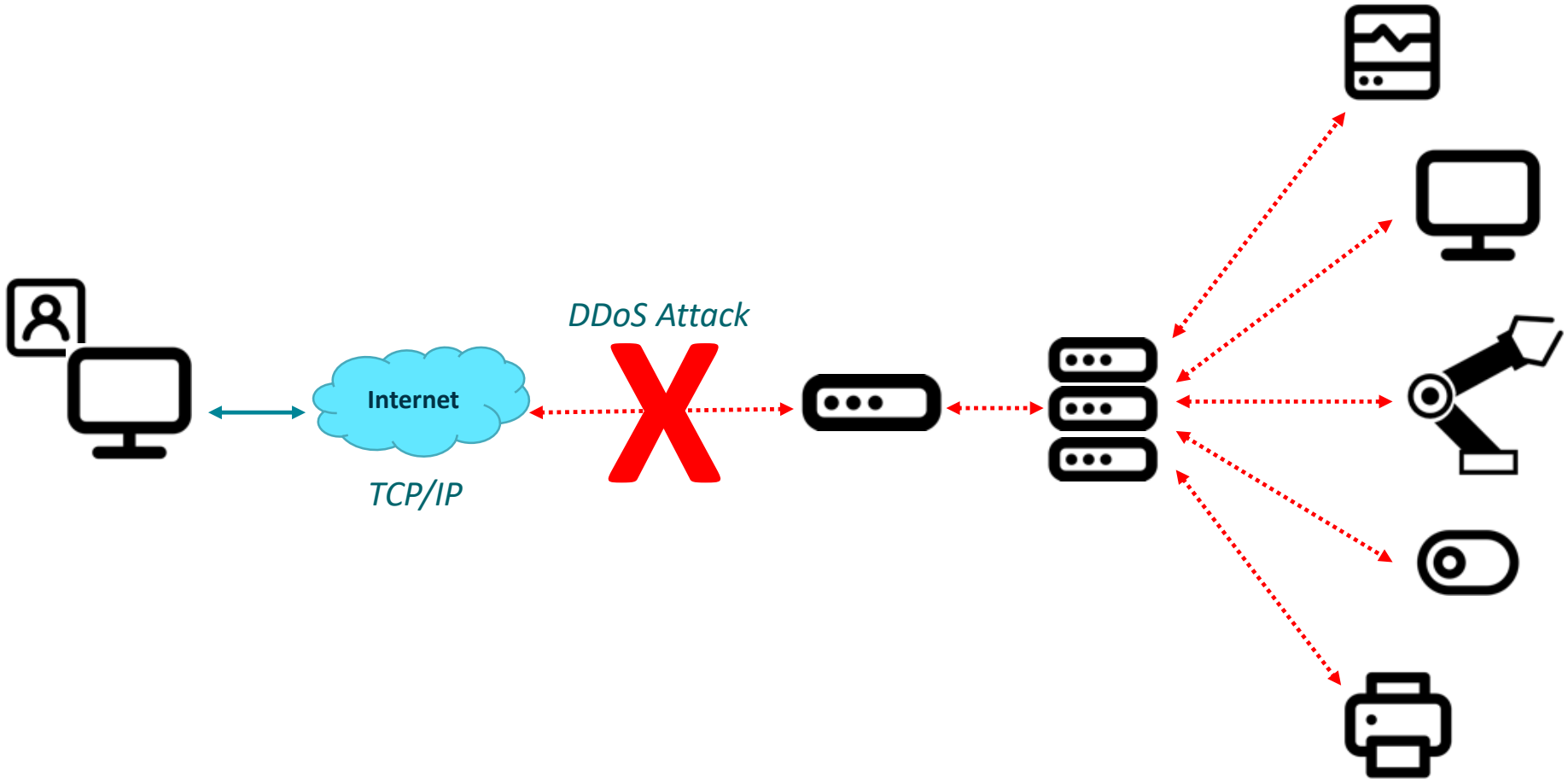
Telefónica
Ideas Locas CDO
ElevenPaths

- ***IoT*** infrastructure



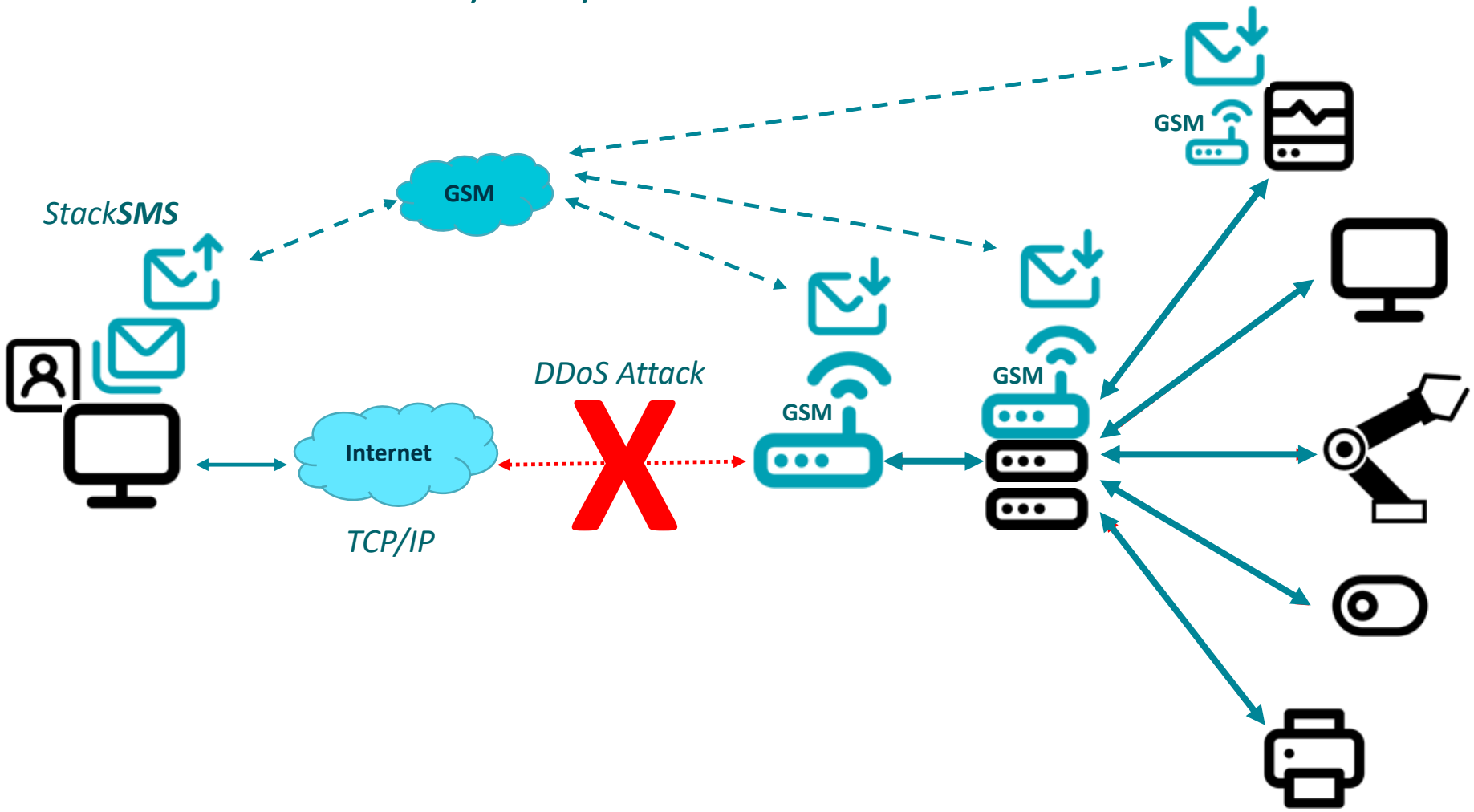
How to take back control of your system after a DDoS attack

- **DDoS attack**. Can't connect to your infrastructure using Internet



How to take back control of your system after a DDoS attack

- Let's take back control of your system with StackSMS



What can you do with StackSMS in a DDoS attack?

Telefónica
Ideas Locas CDO
ElevenPaths

- To reach devices behind your infrastructure a give orders to them
- Access to the router and make actions in order to solve the issue
- Change passwords
- Turn off/on devices
- Send data through the LAN
- Reboot or turn off critical devices
- Send data using a secure channel with GSM protocols (no Internet)

And more …

*Stack**SMS***

Ready to install:

pip install SMS-Stack

Ready to download:

https://github.com/ElevenPaths/SDK-SMS-Stack

Telefónica

Ideas Locas CDO

ElevenPaths

Take back control of your IoT devices with *StackSMS*

Thanks!

https://github.com/ElevenPaths/SDK-SMS-Stack