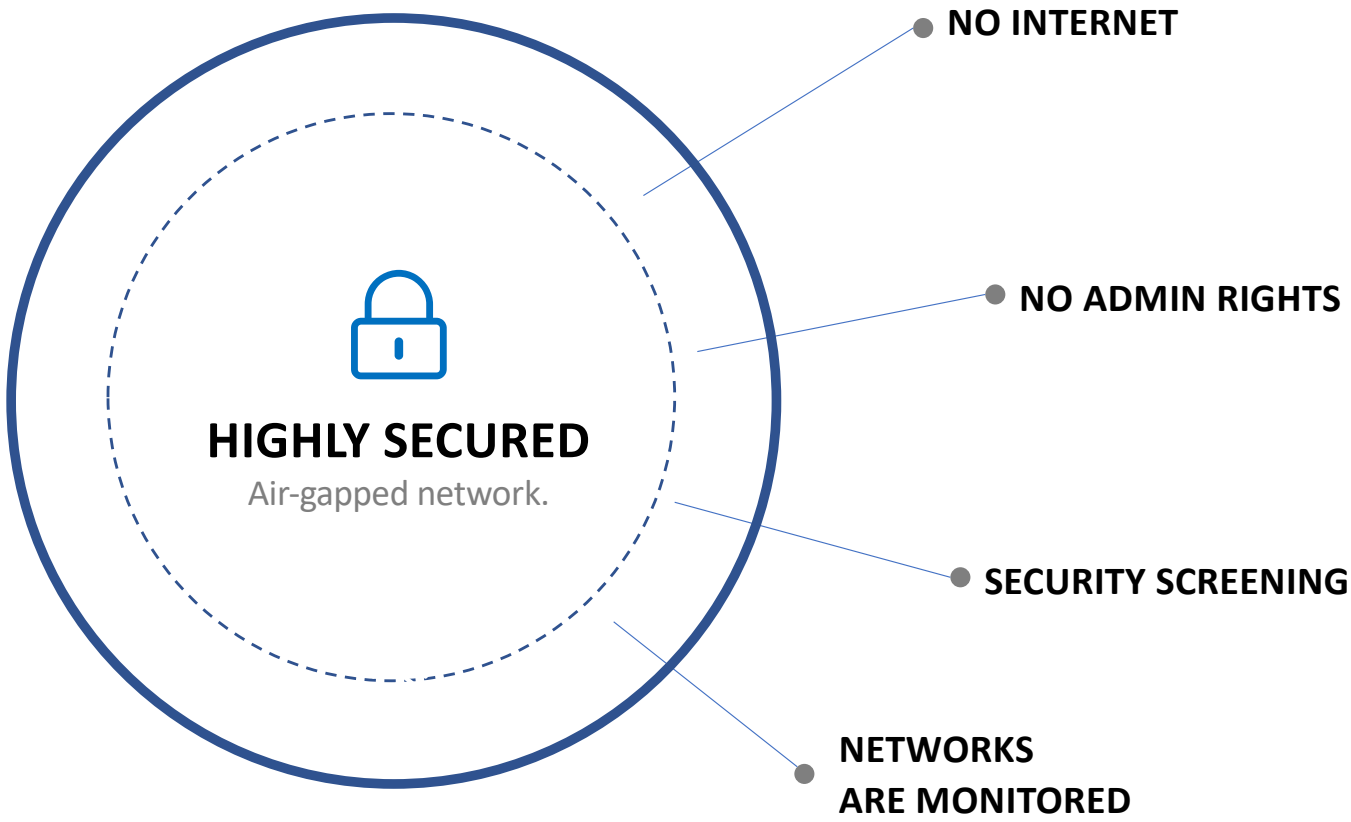
ESC CSAW'18

ONE WEB BROWSER TO RULE THEM ALL

TheMapleCookieArmy
Eléonore Carpentier – INSA CVL
Corentin Thomasset – Grenoble-INP ESISAR – Polytechnique Montréal

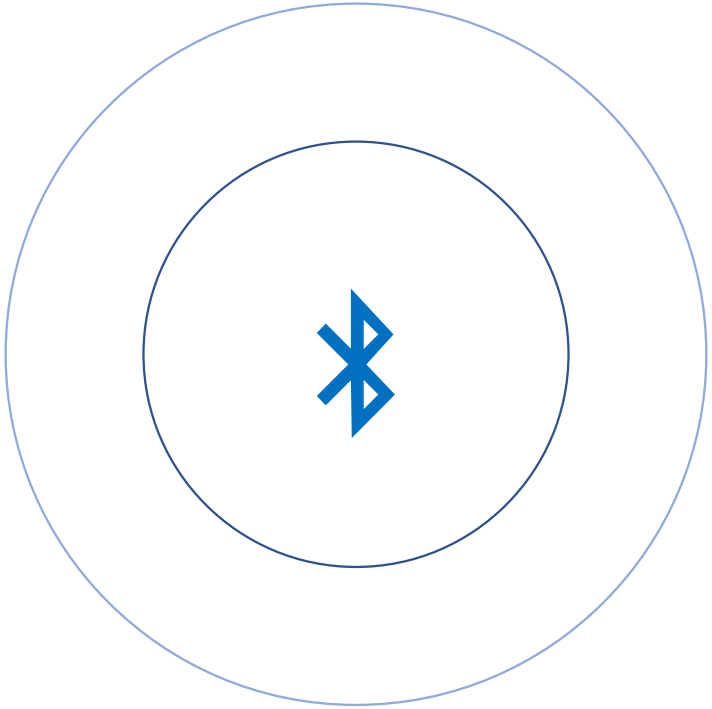
1.

CONTEXT AND ASSUMPTIONS



2.

WIRELESS NETWORKS



HARD TO CONTAIN EMISSION RANGE

Almost impossible to restraint to a given group of users.

BLE UP TO 100m

Varies with the Bluetooth adapter. Laptops and workstations have class 1 adapters (intended range 100m).

CAN BE SNIFFED

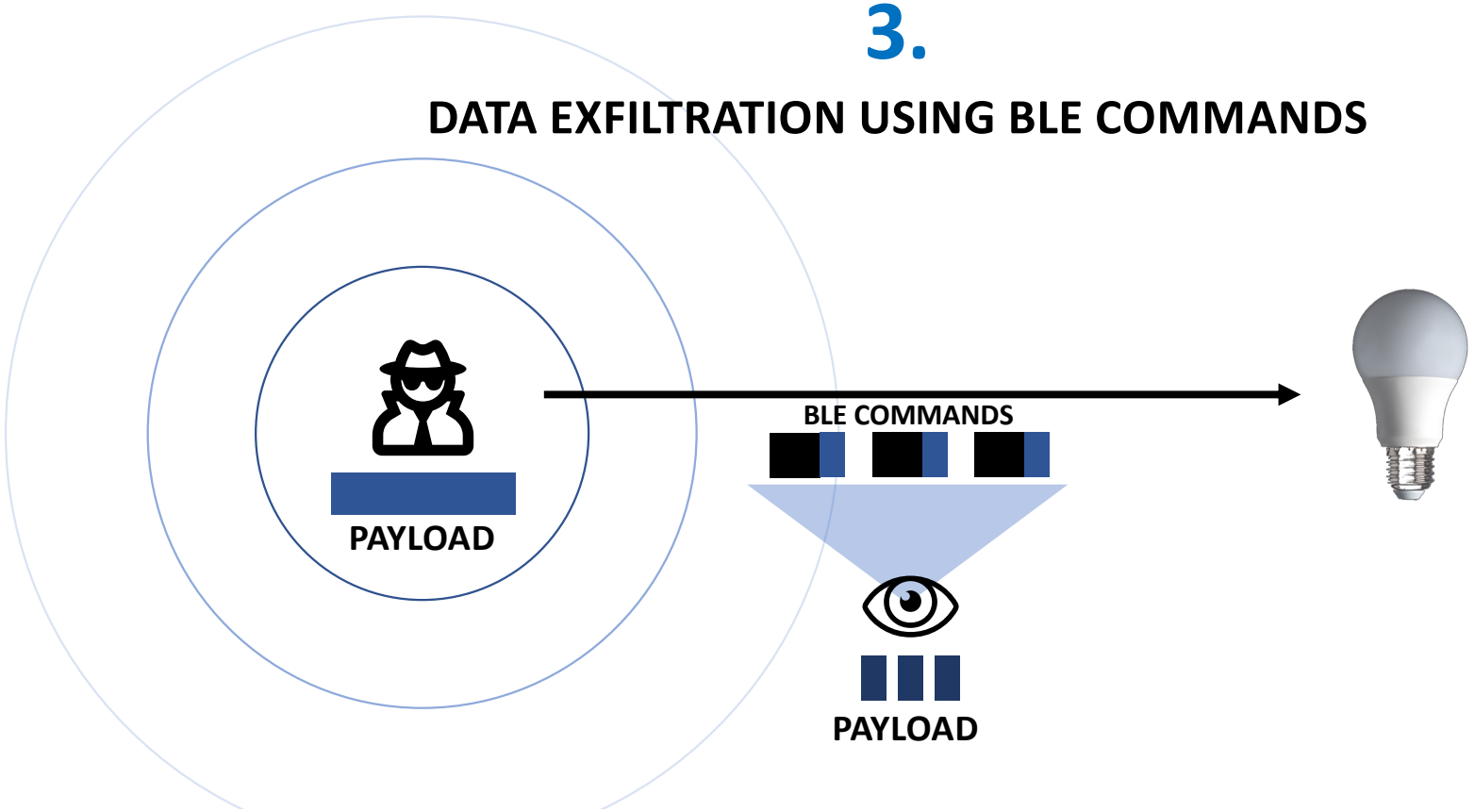
Consider anyone close enough to be able to see unencrypted traffic.

EXTENDED TO 500m

New Bluetooth 5 extend range up to 400m (1km outdoor free field)

3.

DATA EXFILTRATION USING BLE COMMANDS

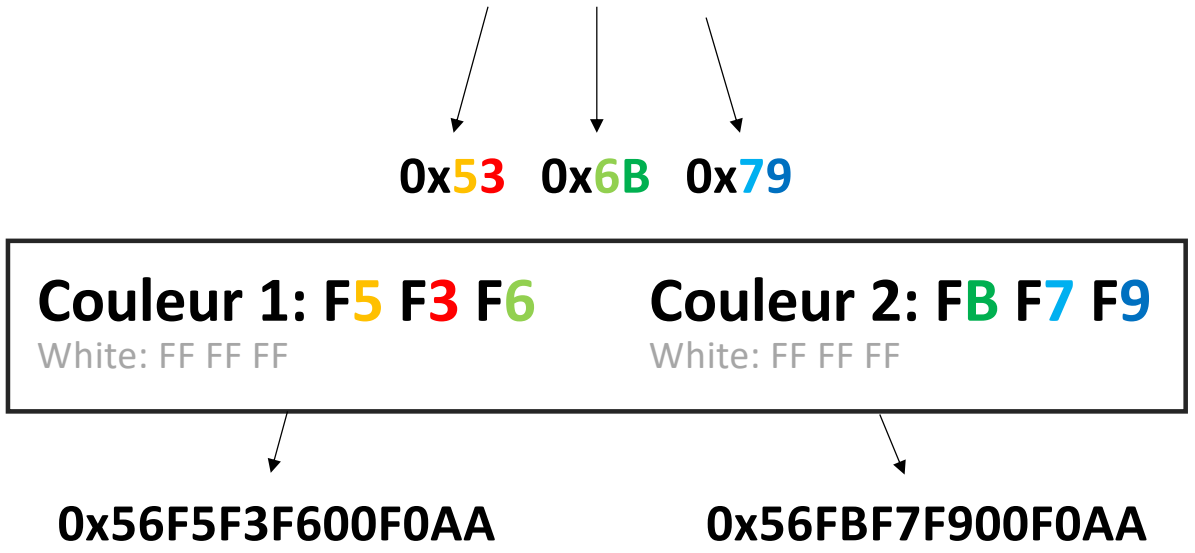


The principle is simple : the attacker sends Bluetooth packets with a hidden data payload to the IoT device and anyone within the emission range can sniff the connection and recover the data as this traffic is unencrypted.

4.

ATTACK DETAILS

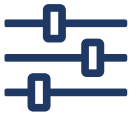
Skyne...



When using the 4 least significant bits of each color channel, the resulting bulb's color change is almost unnoticeable and allows to exfiltrate 12 bits of data per Bluetooth command while remaining unsuspicious on the network level.

4.
ATTACK DETAILS

DELAY



NUMBER OF LSB

ENCRYPTION

To be even more stealthy, the attacker can also delay each command to evade detection and lower the number of bits used to encode data in each color channel. In our final solution we have also added an extra encryption layer to make sure the payload can’t be recovered if commands were intercepted.

5.

IN CONTEXT

How to programmatically send custom BLE commands to the bulb in our scenario ?

SECURITY SCREENING

NO INSTALLATION

NO PERMISSIONS

.EXE SUSPICIOUS

6.

YOUR WEB BROWSER, OUR LORD AND SAVIOR

Web Bluetooth API

~10 Lines Javascript

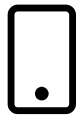
Web Application

7.
IN CONTEXT

No internet
No admin rights
No third party library required.

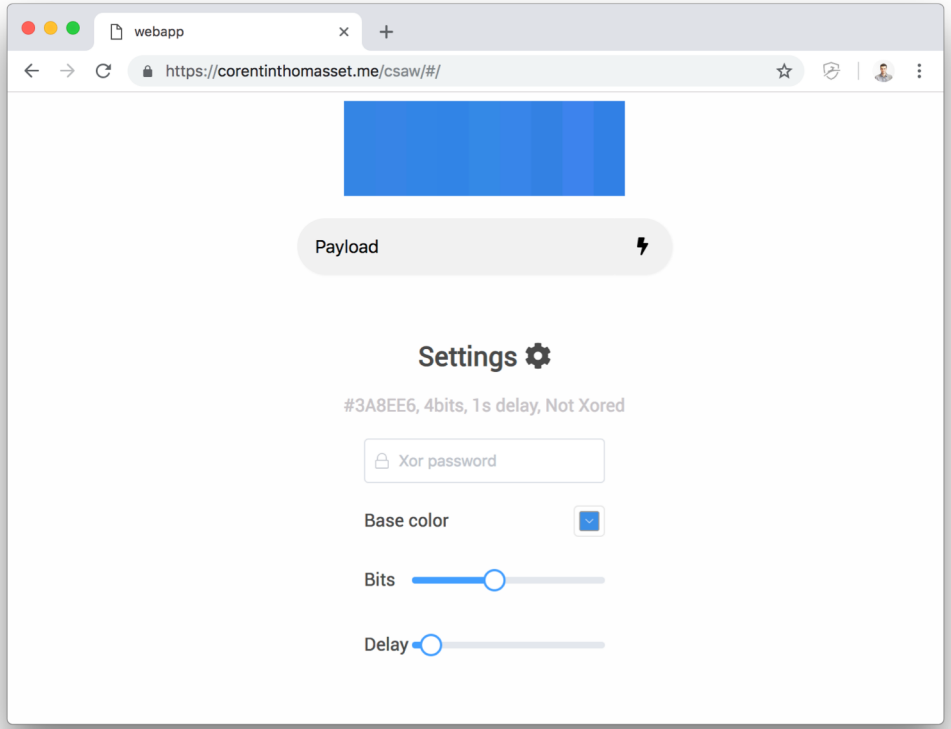
Web browser are present by default on all smartphones.

The app code source can be printer as a QR-Code.



Can be deployed as a fake Magic Blue Control app for smartphones.

8.
PROOFS OF CONCEPT

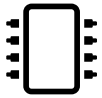


QR-Code with limited functionalities

Smartphone app

Python script to encode & decode

9.
FINAL THOUGHTS



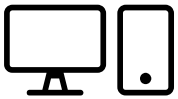
No firmware / hardware modification of the IoT Device.

The script size makes its installation easy even in highly secured environment

Does not require any third party software / library installation and can be ran without any privileges.

Transmission speed is high and can be adjusted to be more

No need of advanced computer science / security knowledge to run the attack.



Cross platform, runs on any device that has a web browser.

Easily applicable to any Bluetooth IoT Device.

Can be deployed as a fake Magic Blue Control app for smartphones.

Thank you

TheMapleCookieArmy
Eléonore Carpentier – INSA CVL
Corentin Thomasset – Grenoble-INP ESISAR – Polytechnique Montréal