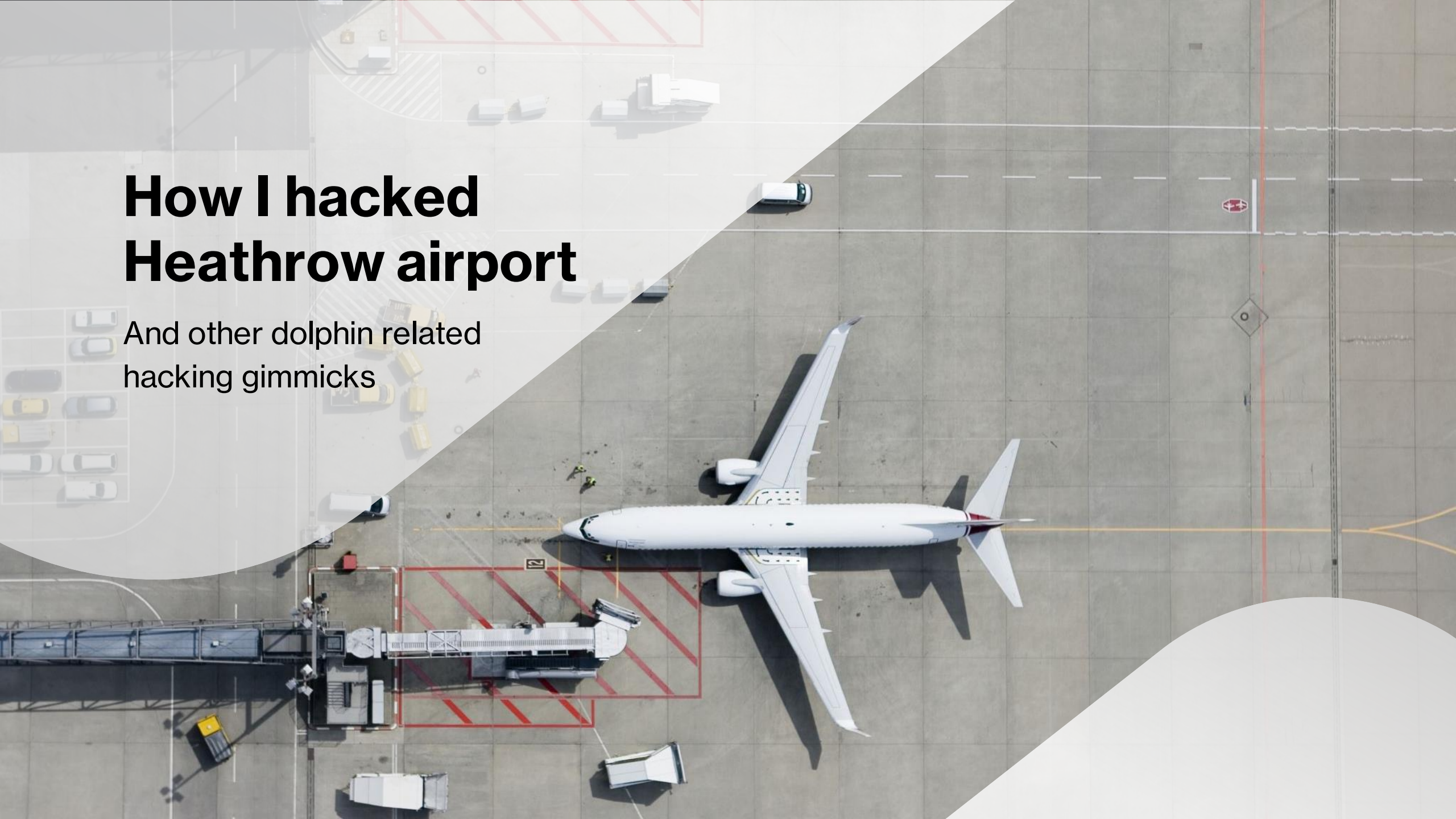
How I hacked Heathrow airport

And other dolphin related hacking gimmicks



Quick intro

-> I go by DE7AULT online, you can call me Morgan

-> Second year student @ Bournemouth University

-> I hack stuff

-> You'll learn how to hack with a tamogotchi

Hacked an airport?
How?

Good question

-> Trip to Helsinki a few weeks ago

-> Had to wait for my gate to open for a few hours

-> Why not poke around and see what Heathrow had to offer:

It turns out all the big screens in the duty free and waiting area of Terminal 5 were all the same brand / make, and all used the same IR codes...

What is IR code?

IR (Infrared) is invisible to humans, data transmission usually happens at wavelengths between 0.74 and 1.4 microns.

An LED will blink with a specific frequency, like morse code, to digitize the IR signal and transmit.

To receive IR signals a photoreceiver is used. It converts IR light into voltage pulses, which are already digital signals.

TV remotes

Your TV remote at home communicates in the same way just mentioned (via IR).

Actually many devices communicate this way, including large screens found in shopping centers and airports.

You just need to have the remote, or do you?

Hacking your TV

IR codes are different per make / model

Manufacturers often share IR codes between different models

If we can figure out the make, we can gain control much quicker

Public libraries of known manufacturers are easily available

Don't usually need specific IR code for specific model

(IE: if we know it's a Samsung TV, any Samsung IR codes will work)

How did I do it?

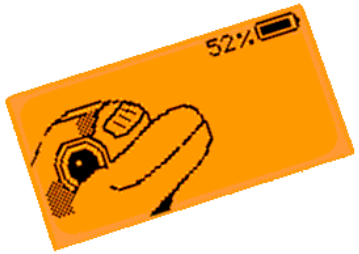
- Discovered make/model of screens used
- Found similar IR stop codes
- Created "wordlist" of known IR codes
- Point and click, screens turned off :)
- Only disabled advertising screens, didn't want to ruin the flight timetables for thousands of people

(Avoiding specifics – still working with Heathrow / Aviation ISAC on remediating the vulnerability)

The Flipper Zero

A self-described portable multitool for pentesters,

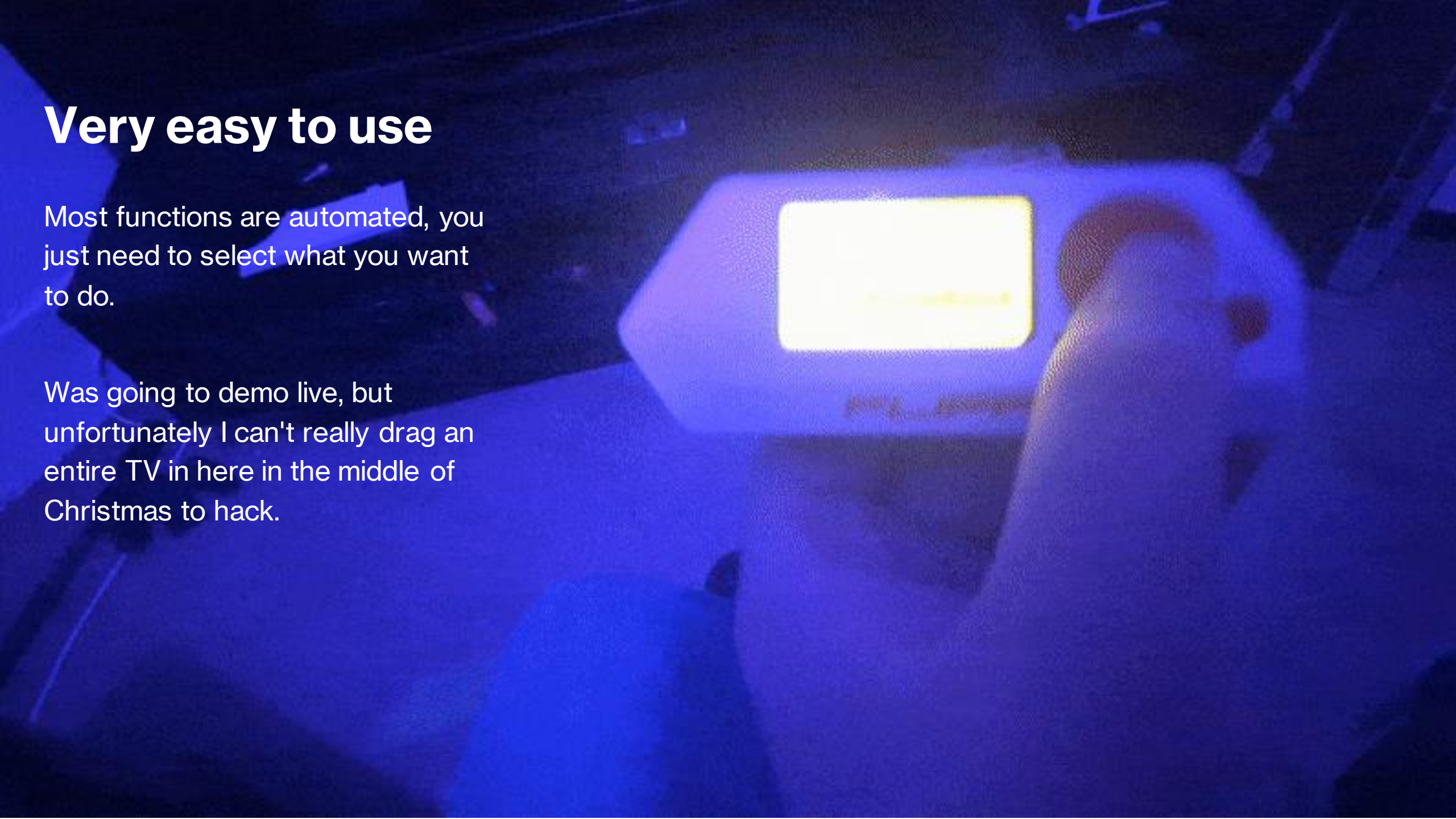
Capable of IR, NFC, RFID, magickey, WIFI, subGHZ, radio hacking and badUSB attacks.



Very easy to use

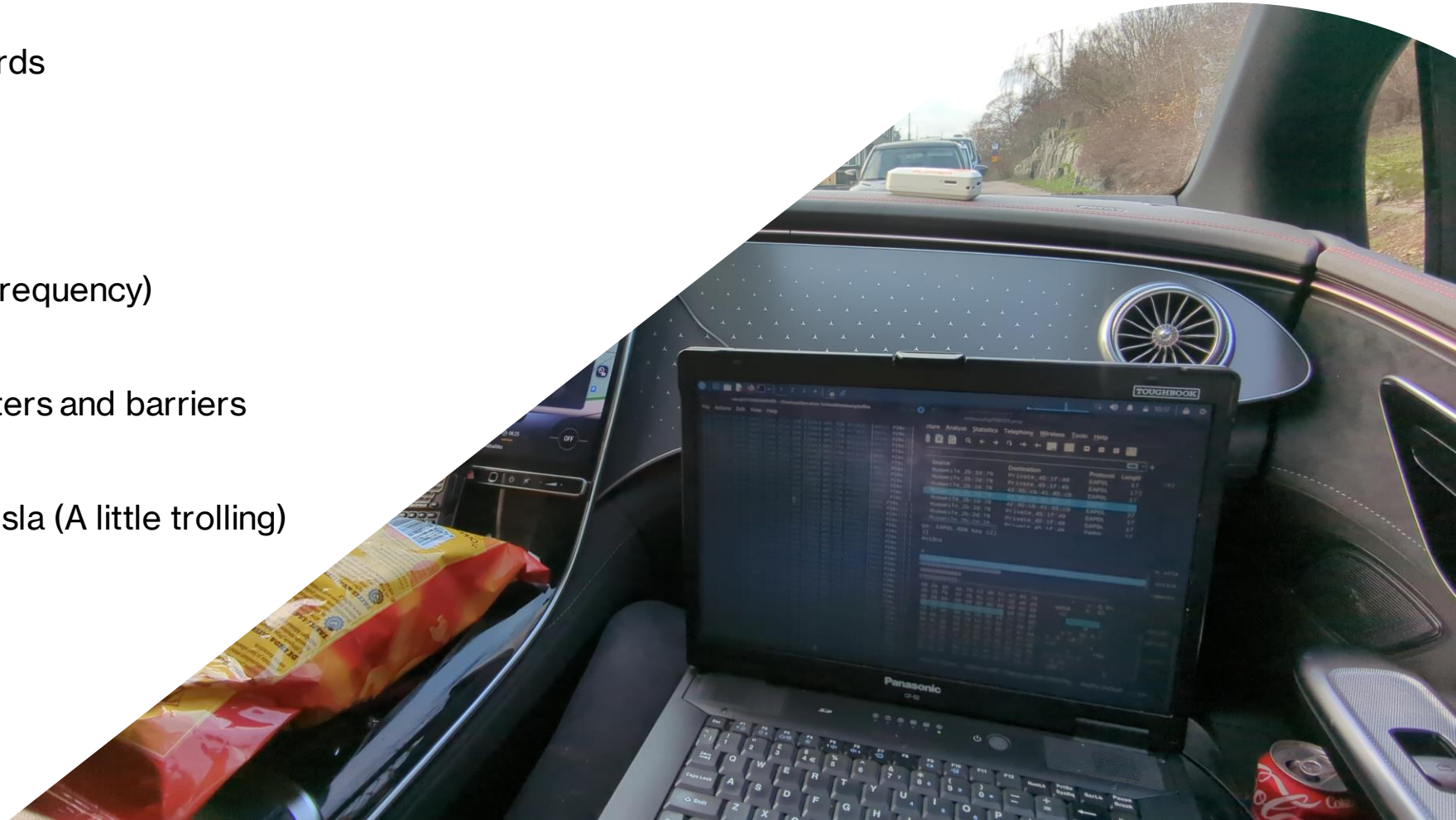
Most functions are automated, you just need to select what you want to do.

Was going to demo live, but unfortunately I can't really drag an entire TV in here in the middle of Christmas to hack.



Other neat tricks

1. Clone NFC access / ID cards
2. Clone RFID / magic keys
3. Spectrum analysis (radio frequency)
4. Bypass pesky parking meters and barriers
5. Open your bosses new Tesla (A little trolling)



Live demo

- I've left some NFC cards around for you to try cloning
- Feel free to read / write to them, experiment with the Flipper
- That's all, if you have any questions, you know where to find me.