




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
- 

13:15 Oslo	EY012	Gate opens 12:50	9
13:15 Calgary	BD3786	Flight closing	32
13:40 Miami	SK3881	Flight closing	25
13:40 New York	BA209	Boarding	29
13:50 Stockholm	AI111	Go to Gate	27
14:00 New York	BD3844	Gate opens 12:50	
14:00 Dubai	CO8245	Gate opens 13:05	
14:00 Izmir	EK002	Gate opens 12:45	
14:05 Copenhagen	YK838	Gate opens 12:45	
14:15 Ottawa	BD3704	Gate opens 13:00	
14:15 Los Angeles	SK3817	Gate opens 13:20	
via: San Francisco	NZ9831	Gate opens 13:10	
14:30 Chicago	AY5781	Gate opens 13:00	
14:30 Boston	SQ2511	Gate opens 13:15	
14:30 Shanghai	CA7022	Gate opens 13:15	
15:00 Vancouver			

15:15 Toronto	QR012	Gate opens 13:45	
15:15 Los Angeles	SK3883	Gate opens 13:35	
15:30 Montreal	AA135	Gate opens 14:10	
15:30 New York	SK3877	Gate opens 14:00	
15:35 Ashgabat	KU101	Gate opens 14:25	
15:40 Denver	T5428	Gate opens 14:15	
via: Chicago	LH9356	Gate opens 14:35	
16:00 Newark		Gate opens 14:25	
16:00 New York	CO8221	Gate opens 16:05	
16:15 Calgary	CO8229	Gate opens 14:45	
16:15 Auckland	SK3878	Gate opens 15:10	
via: Los Angeles	NZ001	Gate opens 14:45	
16:20 Los Angeles	LH9266	Gate opens 15:05	
via: Washington			
16:30 Istanbul	TK1992	Gate opens 15:45	
16:35 New York	AA131	Gate opens 15:20	
16:45 Chicago	AA091		
16:50			



Hacked an airport?
How?

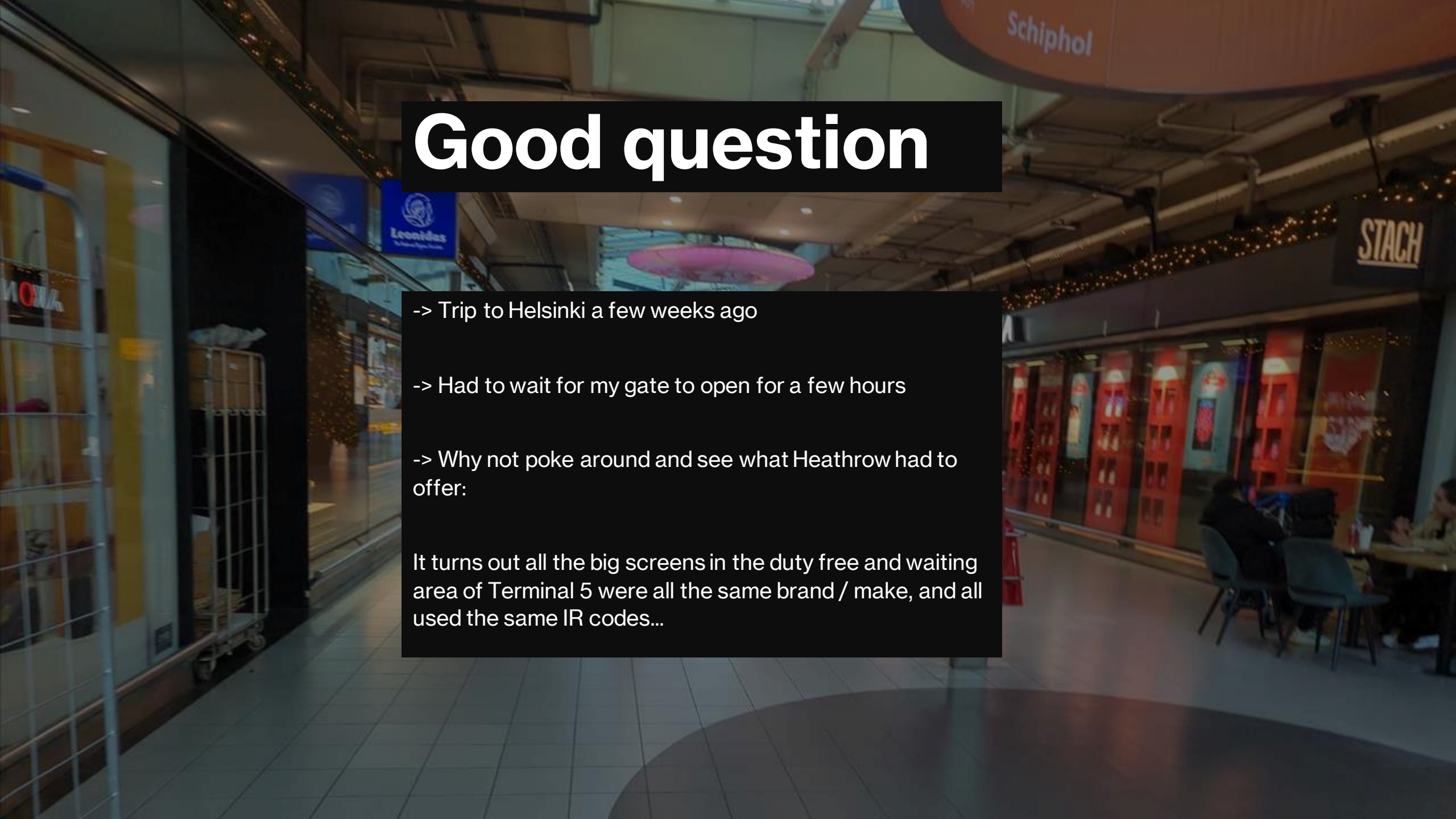
Good question

-> 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

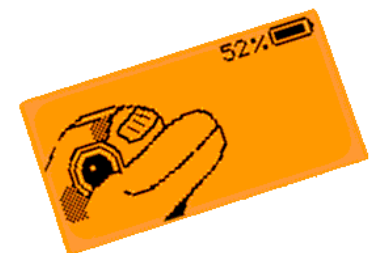
(Avoiding specifics – still working with Heathrow / Aviation ISAC on remediating the vulnerability)



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

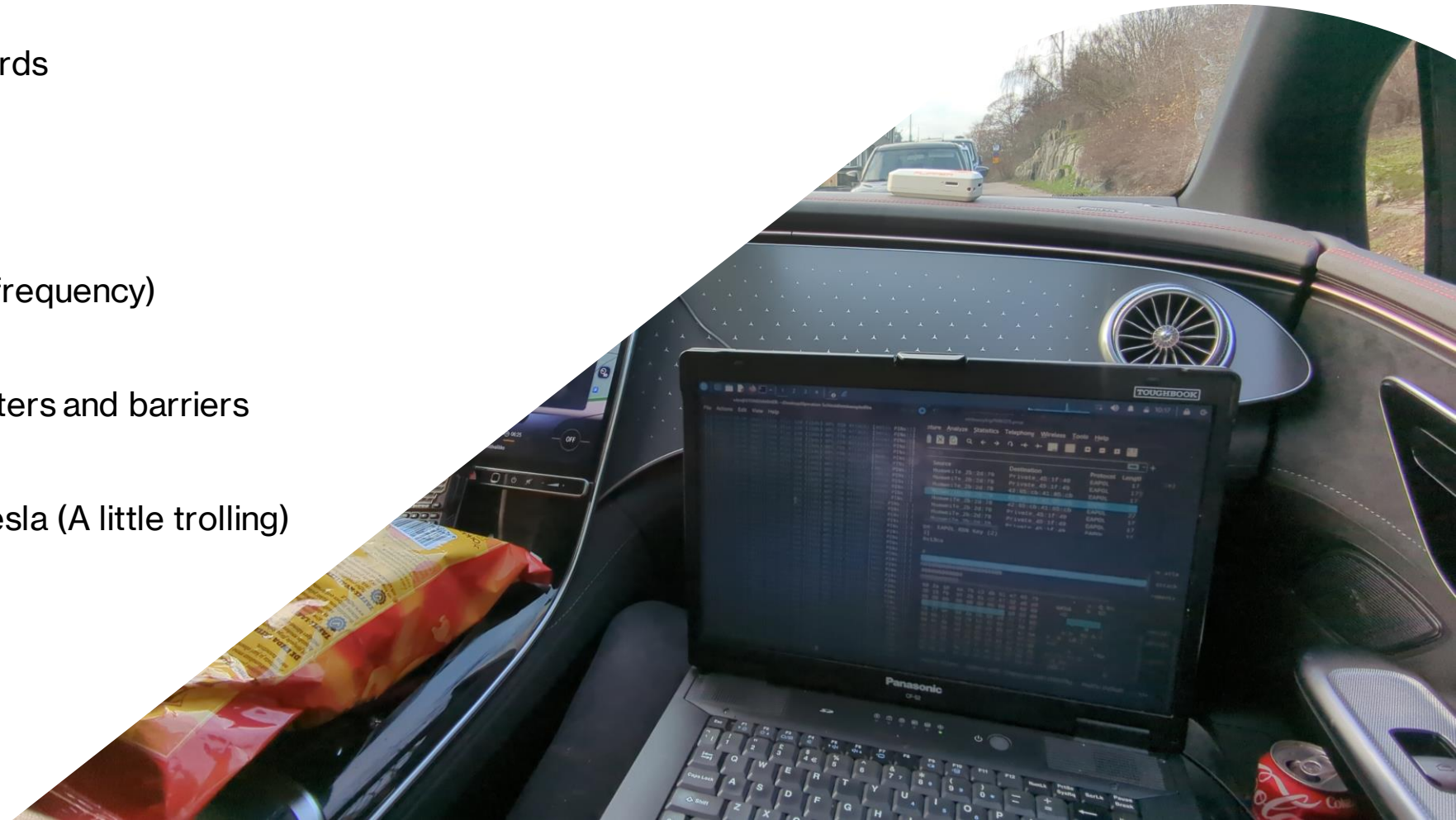
Most functions are automated, you just need to select what you want to do.

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.