WiSpy

With my Raspberry Pi

Disclaimer: This is still in the “Idea” stage

- I’m not a lawyer
  - Please tell me if my idea stray into illegality
- I’ve not started work on this
  - I’m still figuring out how it’ll work
  - And what I’m allowed to do
- I’m likely to be wrong
  - Please correct me

Background

- If I lock up anything nice outside my house, within 3 weeks there will be an “attempt” to steal it
  - Bicycle 3 weeks after moving in: Stolen
  - Replacement 3 weeks after receiving: Attempted Theft
  - Motorcycle 3 weeks after I moved in: Cover stolen
    - Presumably when they were checking to see if they could steal the bike
  - New motorcycle: Woken up by people who were checking the chain on it
- The most frustrating thing is not having information on them

What do I want to know?

- Who are they?
- How often do they check?
  - Will they come back?
- Are they local?

Just Get a Camera

It's *a* solution

- But I rent
  - I can't install proper camera systems
  - I'd be paying for improvements to a building I won't live in forever
- They arrive at night
  - So I need a night camera
- They have hoods and possibly other obscuring clothing
- Camera footage requires high storage costs

What am I thinking?

They probably have their phones on them

- A phone is always on wireless networks
  - Wifi
  - 3G/LTE/4G
- Maybe I could see when those devices come into and out of my property area
  - Maybe I could set up alerts for if they get seen again

Prior Art

Some stuff I already know about

MirrorMe

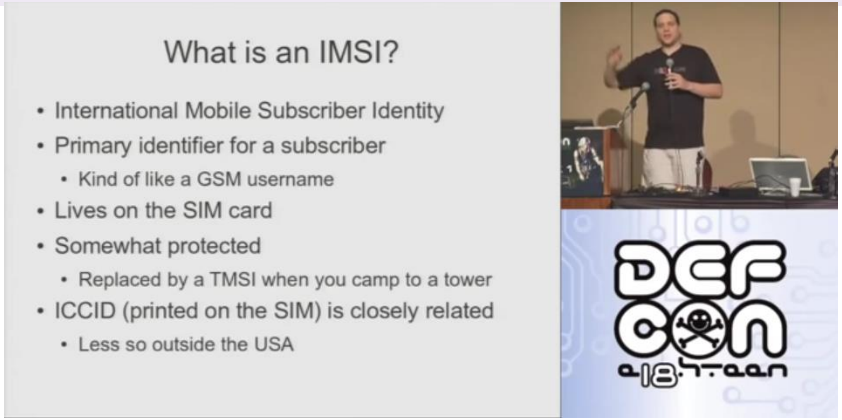
- A RazPi that listens into local wireless access points
- Will attempt to crack and duplicate such networks
  - Kind of like a malicious extender
- If a device connects to the faked Access Point, it's traffic is logged before forwarding.
- Developed by Joe Honour as a PoC project.
  - https://github.com/Guardian-Development/MirrorMe

Wifi Pineapple

- $100
- A full wifi auditing platform
  - Perhaps a bit overkill for this?

“Practical Cellphone Spying” - Chris Paget

- https://www.youtube.com/watch?v=fQSu9cBaojc



What is an IMSI?

- International Mobile Subscriber Identity
- Primary identifier for a subscriber
  - Kind of like a GSM username
- Lives on the SIM card
- Somewhat protected
  - Replaced by a TMSI when you camp to a tower
- ICCID (printed on the SIM) is closely related
  - Less so outside the USA

What’s the Legality

I’m not a lawyer. I’m not a lawyer. I’m not a lawyer. I’m not a lawyer.
I’m not a lawyer. I’m not a lawyer. I’m not a lawyer. I’m not a lawyer.
I’m not a lawyer. I’m not a lawyer. I’m not a lawyer. I’m not a lawyer.
I’m not a lawyer. I’m not a lawyer. I’m not a lawyer. I’m not a lawyer.

General Surveillance

- The Protection of Freedoms Act 2012
  - surveillance camera code of practice (2013)
- Data Protection Act 2018
  - Mainly in force if you record outside your property boundary
  - Don’t publish it
  - People have a right to be forgotten

Anti wire tapping and Jamming

- Obviously wire tapping is illegal
- Can’t spoof existing networks as this may be seen as an attempt at wiretapping
- Jamming Wireless bands would also be illegal

My idea

“We kill people based on meta data.”

WiSpy (That name's probably taken though)

- Monitor a wireless network
- Record devices that appear within range
  - Fingerprint
- Ability to set alerts for certain devices
- Filtering of known devices.

Some avenues and what I need to find out

What does a Wifi Access Point know

- What information, if any, does a WAP see about devices in the area?
  - Ideally without them having to connect
- Are there ways to get a device to announce themselves?
  - Particularly phones

Can I passively pick up phone info?

- I’m not trying to wiretap, I don’t care about encrypted traffic
- Can I hear them post their IMSI or some other identifier?

Help me out

https://gist.github.com/E314c/d6a049dd676de58f8f17475a0c533361

(Shortened as: https://bit.ly/20yx1kB will tweet it later.)