Open Source Intelligence

Do you really know what data you’re leaking ?

Oh Hai!

David Busby
Senior Site Reliability Engineer, DevSecOps @ Quiq
CISSP

@icelus

@oneiroi

Precepts

What this talk is, and what you should take away from the talk

Precepts

Rules of the …

1. Exercise some Wheaton's law (don't be a dick!)
2. Don't use what you learn here to stalk / harass / other abusive behaviour (see rule 1)
3. Unsure? see rule 1.
4. The birds work for the bourgeoisie
5. See rule 1.

https://www.spymuseum.org/exhibition-experiences/about-the-collection/collection-highlights/pigeon-camera/

Precepts

Rules of the …

1. This is not a “how-to” for gathering information on an individual or organization.
2. This is not a “how-to” on how to become a creepy net stalker
    a. Seriously don’t
3. This is a small insight into what information you may not be aware of disclosing in your own life.
4. This talk covers how this information can be misused with real world examples.
5. This talk concludes with how this information can be used for good.

Terminology

1. OSINT - Open Source Intelligence
2. OPSEC - Operational Security
3. PERSEC - Personal Security
4. COMSEC - Communication Security
5. INFOSEC - Information Security

But why?

Sometimes a little data is not always a good thing …

Homicide Offender vs. Victim demographics

View by: # %

Sex | Race | Ethnicity | Age

Offender Sex

Male	4,815
Female	799
Unknown	586

Offenders w/ reported sex 6,200

Download

Victim Sex

Male	3,834
Female	1,353
Unknown	13

Victims w/ reported sex 5,200

Download

But why?

Increase safety through awareness (PERSEC++ && OPSEC++)

Homicides:
77.7% Male offender
12.8% Female offence
73.7% Male victim
26% Female Victim
Sexual Assault
92.5% Male offender
4.2% Female offender
10.7% Male victim
89.71% Female victim

But why?

Protection of human life and wellbeing **should be everyone's first priority**!

Inc, protecting quality of life.
Protection from abuse, fraud, malactors, malevolent behaviours, threats and threat actors.


bUt ThE sTaTs ArE bIaSeD ...

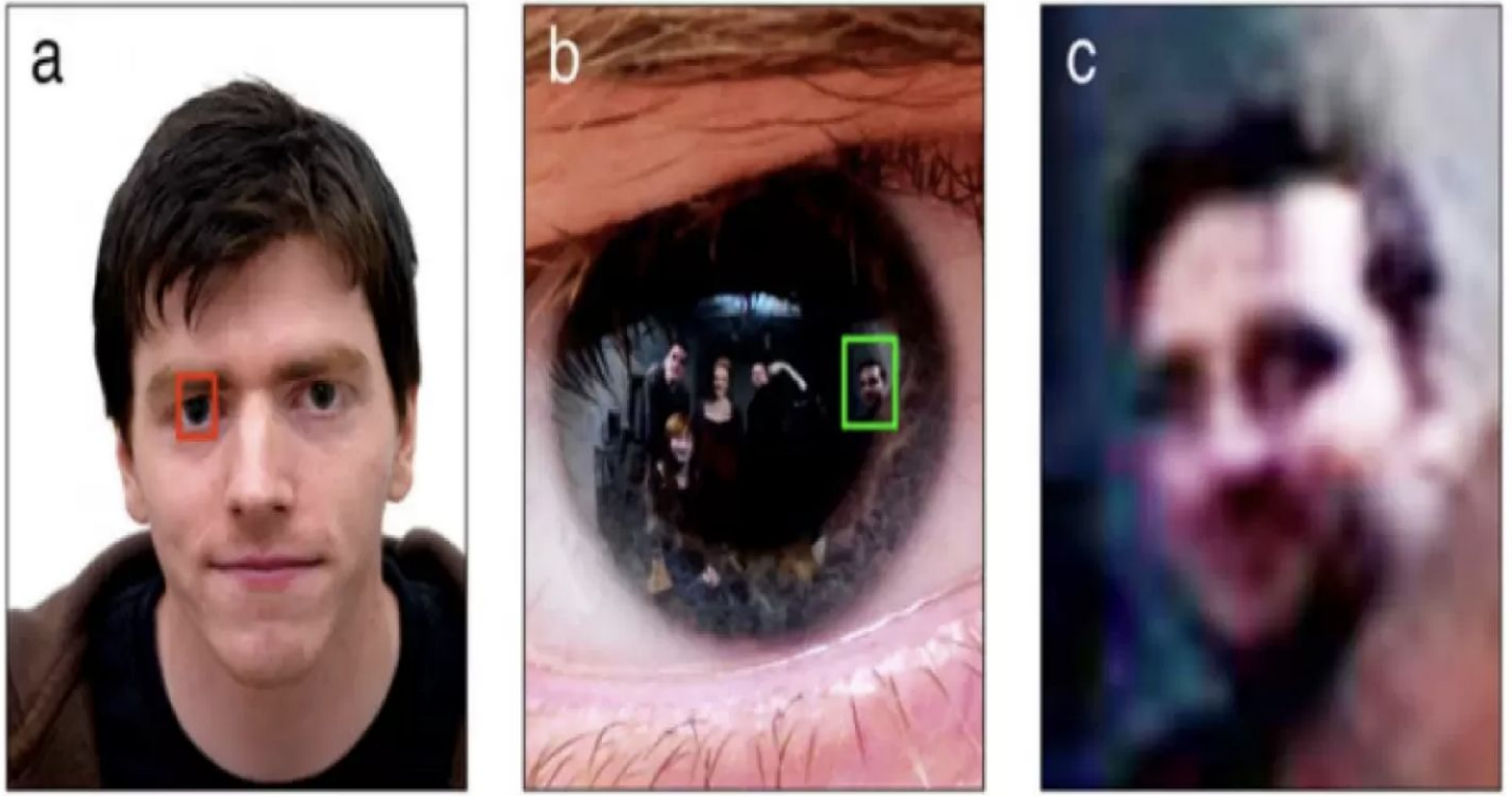
Meanwhile, in the real world

There are examples of where data exposure has lead to very concerning issues …


Stalker used corneal reflection to
locate female singer ...

Data exposure, is not just digital

- BBC article: Stalker ‘found Japanese singer through reflection in her eyes’ (October 2019)
- Corneal reflection allowed identification of a train station.
  - Stalker then used google street view to further confirm angle and approximate distance when the photo was taken.
- Such reflections were a noted concern in a 2013 peer reviewed academic research paper.


a
b
c

It is also digital ...

- Extensible Image Format (EXIF) data is embedded into every single photo you take on your “smart device”.
- Examples:
  - GPS (time, elevation, lat:long, direction facing, etc)
  - Date & time
  - Device type
  - And more

```
exiftool /Volumes/JetDrive/IMG_20160707_192748.jpg | egrep -i 'GPS|Software|Model'
GPS Date Stamp                  : 2016:07:07
GPS Altitude Ref                : Unknown (2)
GPS Longitude Ref               : West
GPS Latitude Ref                : North
GPS Time Stamp                  : 18:20:38
Camera Model Name               : ONEPLUS A3003
Software                        : OnePlus3-user 6.0.1 MMB29M 4 dev-keys
GPS Altitude                    : 0 m Above Sea Level
GPS Date/Time                   : 2016:07:07 18:20:38Z
GPS Latitude                    : 32 deg 58' 3.12" N
GPS Longitude                   : 12 deg 40' 43.88" W
GPS Position                    : 62 deg 18' 7.61" N, 2 deg 40' 43.88" W
```

It’s not limited to images either …

- Let’s look at 802.x and what else you may be leaking without being aware!
- **Bluetooth**
  - Find a bluetooth device with centimeter accuracy written into the bluetooth spec…
    - Bluetooth Received Signal Strength Indication (RSSI)
  - Used in commercial products e.g. Tile, Trackr.
  - Used by marketing agencies to track population density of a given area.

It’s not limited to images either …

- **WiFi**
  - WiFi beacons broadcast (in the clear) every single WiFi AP your device has ever connected to
    - WiFi BSSID’s
  - WiFi data is collected by Gov agencies such as T.F.L.

A little knowledge can be a dangerous thing …

“I’m here to collect your council tax arrears on behalf of $local_council …”

*presents “id”

That ID is _actually_ an O.A.P Bus pass, with red electrical tape.

I swear I’ve seen this somewhere before ….


Leeloo Dallas. Multi-pass.

OSInt _can_ be used for good!

#OSIntforgood

I highly recommend you look at tracelabs (https://www.tracelabs.org/) if you want to learn more.

Trace Labs run “Searchparty” CTF events.

Those search parties, allow participants to submit “flags” to contribute to build an evidence file to help locate real missing person(s).

This can be looking at image artefacts, reflections, unique interesting items in the background, etc.

To simply searching for the $name, $location and the $social_media profile of the missing person.

You submit for example a URL of the $social_media_profile for ~20 points, whilst making observations like, unique identifying features (which may have been missed in the case file), or identifying the individuals, car, cellphone model, etc. From purly visual recognition could net you 100pts or more.

OSInt _can_ be used for good!

#OSIntforgood

You may be asking why?

Practise / skillup, which contributes to real world missing persons cases, you might never have contact with the missing person, nor their family, but you can help them find a missing loved one, from anywhere in the world.

Questions?