The cree.py side of geolocation

Weaponizing your check-in's

Ioannis Kakavas
OWASP AppSec Research EU 2012

Athens, 13/07/2012

Who Am I ?

Ioannis Kakavas

Dipl. Eng. Electrical & Computer Engineer

M.Sc. Information and Communication Systems Security

Cree.py OSINT geolocation aggregator

IT Security Consultant (IAM) at IT Advisor

@ilektrojohn

Why Am I here ?

To scare you.

Why Am I here ?

To scare you. No, REALLY !

Overview

- Location(al) Privacy in a nutshell

- Social Engineering in a nutshell

- Cree.py in a nutshell

- ~~Demo~~ . Lets call it a story ☺

Location(al) Privacy

"Locational privacy (also known as location privacy) is the ability of an individual to move in public space with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use" [1]

Threats :

- {Cell,Smart}phones (Apple 04/2011 ,directional analysis, triangulation etc.)

- GPS navigation systems (TomTom 05/2011)

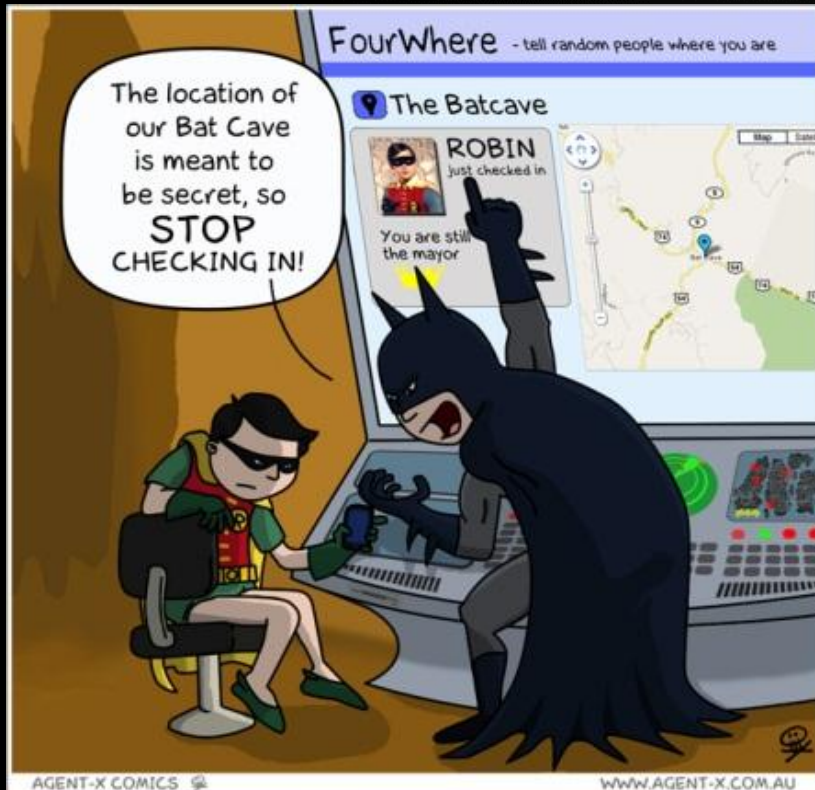- Road tolls

- But the biggest threat is …..

[1] https://www.eff.org/wp/locational-privacy

Location(al) Privacy

OURSELVES !

Location aware social media

Location(al) Privacy

- The locational privacy paradox :

    Victim === Perpetrator

- Exhibitionism

- Need for socializing and belonging

- Simply put .. Human Nature

Social Engineering

- Definition

- Parts
  - Information Gathering
  - Elicitation
  - Pretexting

- Why does it work ?
 - Humans* ARE the weakest link in any given system

*uneducated, unaware humans that is

Cree.py

- When ?
  - Johannes Ullrich, ICS Diary 02/2010
  - Icanstalkyou.com , pleaserobme.com
- Why ?
  - Teach myself python
  - Raise awareness
  - Provide an information gathering tool for Red Teams
- What ?
  - Python scripts, PyGTK, osmgpsmap, pyexiv2
- Where ?
  - Debian based distros, BackTrack 5, Windows >= XP

Cree.py

- How ?
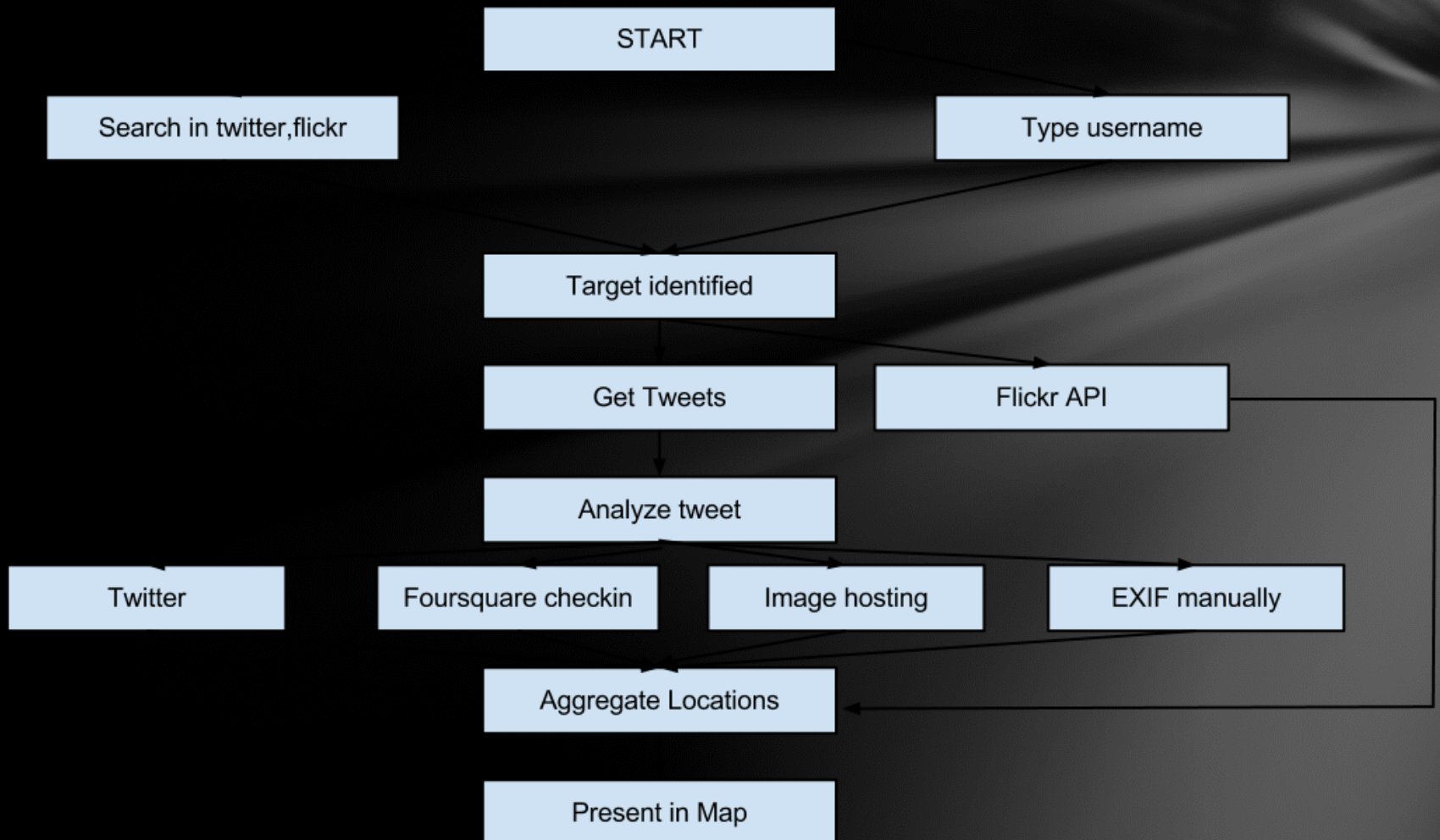
Cree.py

- Yeah, so ?
  - 633,919,264 users on Twitter (last night)
    - ~50% on mobile
    - ?(1-10) % of tweets are geotagged
  - 20,000,000 users on Foursqare
    - ~ 20% check ins shared in twitter
  - 51,000,000 users on Flickr (2011)
    - ? % of geotagged photos
  - 50,000,000 users on instagram (May 2012)
    - All of them on mobile

Cree.py

Who was interested ?

- Couple of VCs / companies offering to go commercial

- NSA,DHS,CIA,ONI and a bunch of 3 letter agencies

- Red teams performing social engineering attacks

- TV, radio, blogs

Who got irritated ?

- Twitter

- Occasional hate mail ("Haters gonna hate")

Cree.py

Who is using it (and cared to tell me) ?

- Penetration testing teams for information gathering

- Private investigators

- Police undergoing OSINT training

Cree.py – A story

Amy Tweetalot
@amytweetalot
Social butterfly. Twitter and instagram fanatic :) Keen on meeting new people,
Stockholm

Edit your profile

3,538 TWEETS
353 FOLLOWING
444 FOLLOWERS

Tom Shilder
@tomstalkme
CTO at MySuperWOW . Young and ambitious. My tweets are my own. Social media fanatic
Stockholm

Edit your profile

5,582 TWEETS
963 FOLLOWING
2,168 FOLLOWERS

Disclaimer: above users are fictional, but based on real twitter users. Personal data altered.

Cree.py – A story

Hands ON

Cree.py – What's next ?

- Roadmap:
  - Q3/2012 v0.3 (code cleanup & optimization, fix modularity, robustness)
  - Q1/2013 v0.4 requested features implementation
    - Support for more services/frameworks (picassa, google+ etc.)
    - GTK - > QT (Apple fanboys hold on!)
    - Search by location
    - Retrieved data analysis and report generation
  - v0.5 …..

Cree.py – Get involved !

I just met you , and this is crazy, but here is my github :

https://github.com/ilektrojohn/creepy

So, FORK me maybe ???

The end !

Thanks for listening !

QUESTIONS ?

FEEDBACK!

@ilektrojohn

https://ilektrojohn.github.com/creepy

jkakavas@gmail.com