echo)) wi-fi ((location

luiz eduardo

agenda

- intro/ motivation
- the idea
- system architecture
- possible models
- phase zero
- phase zero.one
- what's next
- what else is out there?

intro / motivation

- playing with something old
  - microsoft location finder
- playing with something new
  - apple, skyhook, etc
- not really knowing if and how people are tracking me
- ... technology is cool

wtf is echo location?

- a common method of obtaining information about a remote object is to bounce a *wave* off of it

the idea

- understand how the existing stuff works
- create a wi-fi-based tracking system (without reinventing the wheel)
- use existing technology to the max

the idea (cont)

- track people
  - friends
    - maybe a dynamic twitter/ dodgeball thingy
  - enemies
  - employees
- devices
  - wi-fi enabled or not (phones, laptops, videogames, etc)
- or ... just for fun

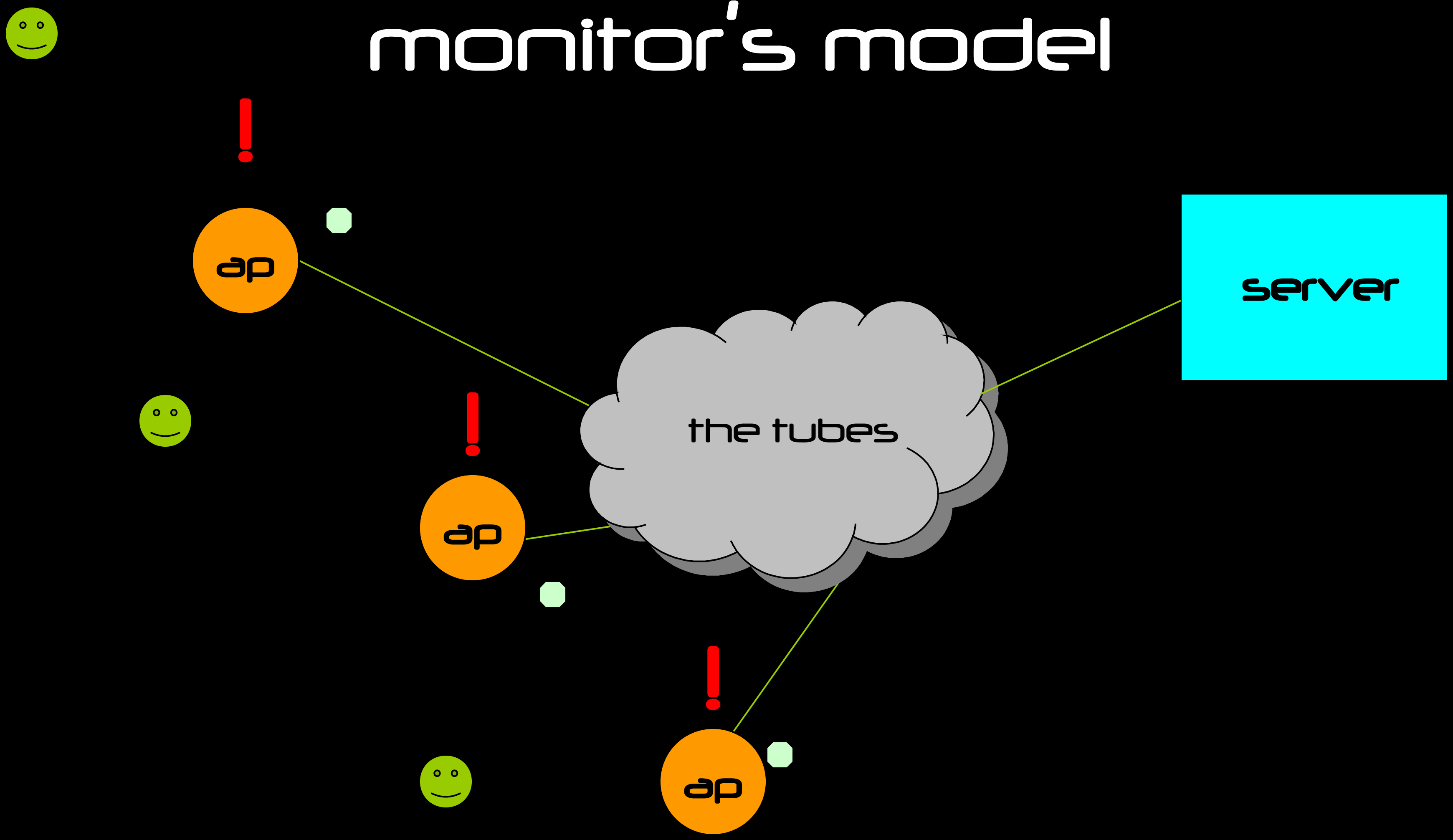
system architecture

- monitors
- clients
- “location” server
- notification server

concerns / challenges

- make something that works (duh!)
- ... and is legal
- kiss / lazy approach
- easy of “use” (or install) on clients/ devices

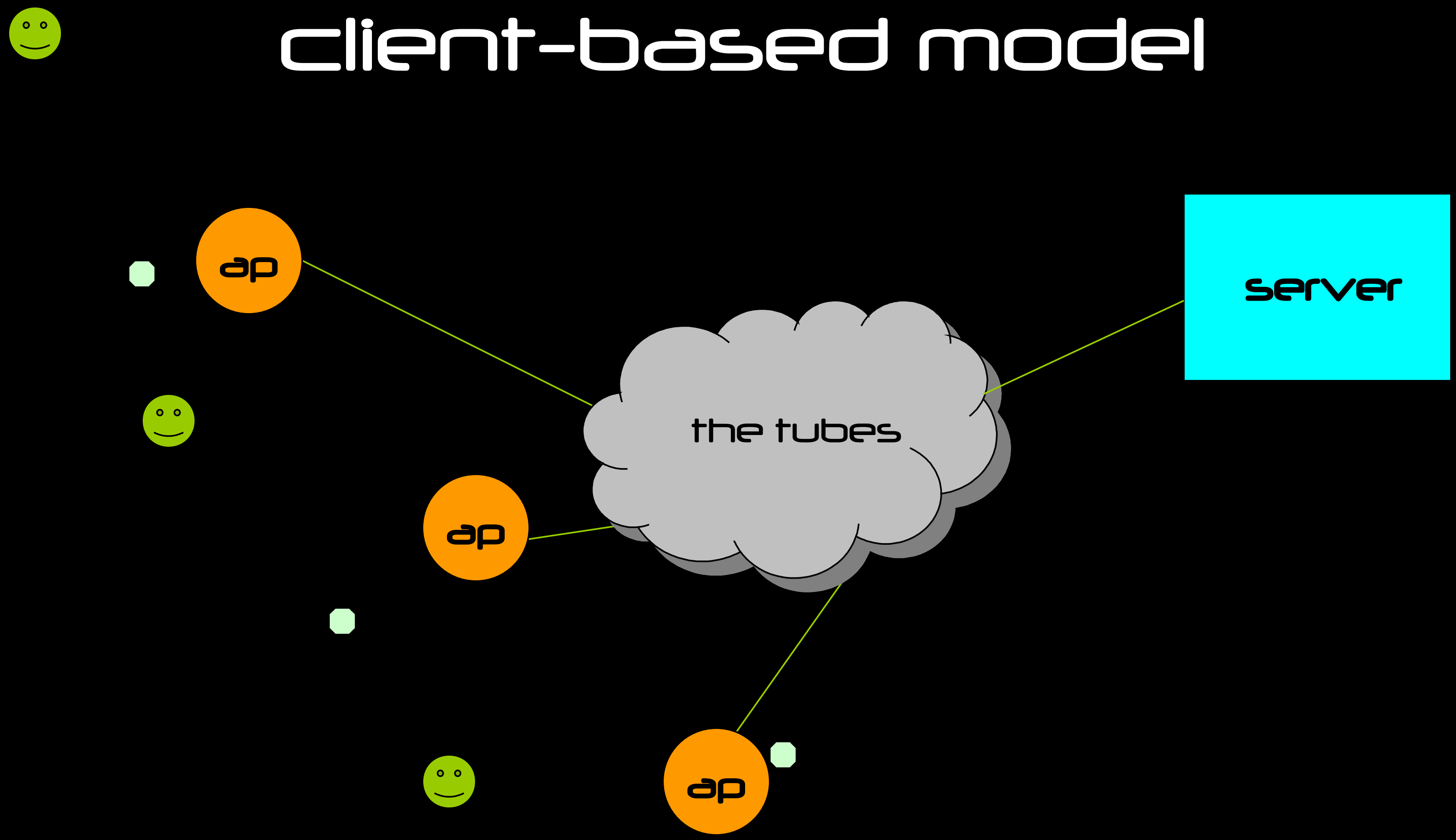
monitor's model



monitors approach

- open-wrt, dd-wrt, etc
- community wireless-way
- monitors report to the server when a client is seen
  - by mac address? ☹
  - secure way for the monitor to talk to the server?

client-based model



client-based approach

- device runs "special" sw to talk to server
- ideally to be used on any open wireless network (!?! how about metrowifi nets?
- ideally to be used on any hot spot?
- protocol to talk to server
  - vpn client on demand
    - not hotspot friendly
    - each client has a different username
  - something dns-like with some unused bits flipped?

client-based model (cont.)

- too many possible platforms
- use of a hardware based wi-fi device:
  - older sd cards with wi-fi
  - eye-fi like cards

bonus: impossible model

- kyocera/d-link-like evdo box
  - pros: will be always connected
  - cons: how to know where it is?
- or, why not simply use the existing cellular data network (charges?)

phase zero

phase zero

- mix of both approaches
- server: vpn concentrator
- parse logs using splunk
- vpn client on demand
  - or be lazy: native vpn clients on older wi-fi only blackberry
- monitors need to be open system access-points ☹

phase zero f'-ups

phase zero.one
(aka: post-toorcon)

- no actual coding done
- but got some action
- logged data
- netgeo and alikes

phase zero.one f'-ups

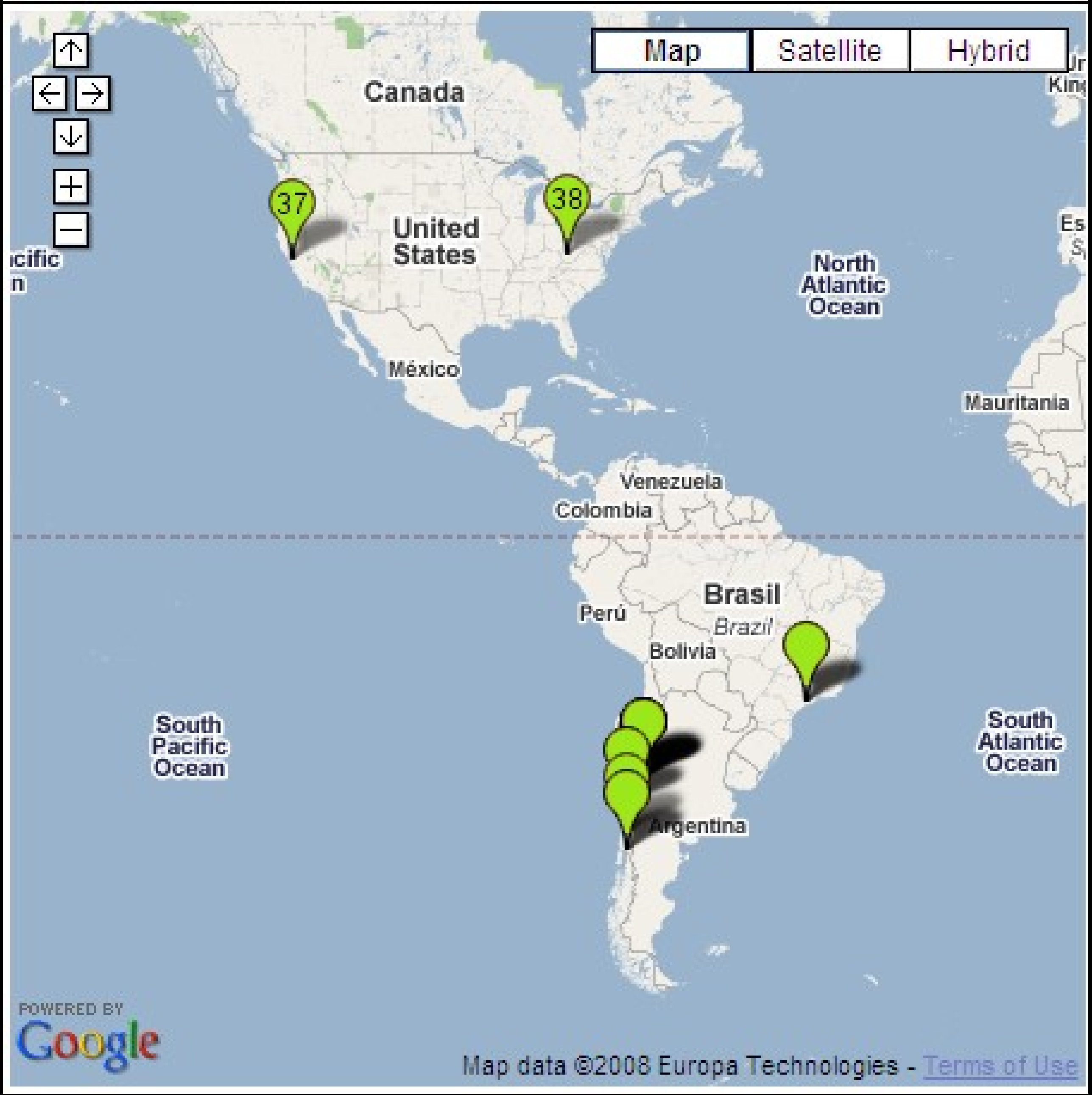
- burned pcmcia slot on my dell

sample data

```
Apr 28 11:32:52   200.72.180.244
Apr 28 11:56:55   200.72.180.244
Apr 28 18:08:15   200.72.180.244
Apr 29 16:31:09   200.126.75.226
Apr 29 18:10:05   200.72.180.244
Apr 30 07:00:49   200.72.180.244
Apr 30 09:36:21   216.155.76.130
Apr 30 09:53:29   216.155.76.130
Apr 30 10:50:18   200.126.67.142
Apr 30 11:11:45   200.126.67.142
Apr 30 19:05:34   200.72.180.244
May 1 08:36:39    200.72.180.244
May 1 13:45:47    200.113.44.15
May 1 14:13:13    200.113.44.15
May 6 16:27:39    74.95.200.14
May 8 17:23:28    208.54.95.67
May 9 08:43:07    189.78.132.176
May 11 14:23:48   189.78.164.106
```

more info

Hostname	Country Name	City	Latitude	Longitude	ISP
200.72.180.244	Chile	Santiago	-33.45	-70.6667	ENTEL CHILE S.A.
200.72.180.244	Chile	Santiago	-33.45	-70.6667	ENTEL CHILE S.A.
200.72.180.244	Chile	Santiago	-33.45	-70.6667	ENTEL CHILE S.A.
200.126.75.226	Chile	Valdivia	-39.8	-73.2333	Telefonica del Sur S.A.
200.72.180.244	Chile	Santiago	-33.45	-70.6667	ENTEL CHILE S.A.
200.72.180.244	Chile	Santiago	-33.45	-70.6667	ENTEL CHILE S.A.
216.155.76.130	Chile	Calbuco	-41.7668	-73.1333	Telefonica del Sur S.A.
216.155.76.130	Chile	Calbuco	-41.7668	-73.1333	Telefonica del Sur S.A.
200.126.67.142	Chile	Concepción	-36.8333	-73.05	Telefonica del Sur S.A.
200.126.67.142	Chile	Concepción	-36.8333	-73.05	Telefonica del Sur S.A.
200.72.180.244	Chile	Santiago	-33.45	-70.6667	ENTEL CHILE S.A.
200.72.180.244	Chile	Santiago	-33.45	-70.6667	ENTEL CHILE S.A.
200.113.44.15	Chile	Santiago	-33.45	-70.6667	Telefonica Empresas
200.113.44.15	Chile	Santiago	-33.45	-70.6667	Telefonica Empresas
74.95.200.14	United States	Alameda	37.7534	-122.2604	Comcast Business Communications
208.54.95.67	United States	Hurricane	38.4043	-81.9702	T-MOBILE USA
189.78.132.176	Brazil	São Paulo	-23.5333	-46.6167	NET Serviços de Comunicação S.A.
189.78.164.106	Brazil	São Paulo	-23.5333	-46.6167	NET Serviços de Comunicação S.A.


Map
Satellite
Hybrid
Canada
United States
37
38
North Atlantic Ocean
México
Mauritania
Venezuela
Colombia
Brasil
Brazil
Perú
Bolivia
South Pacific Ocean
South Atlantic Ocean
Argentina
POWERED BY Google
Map data ©2008 Europa Technologies - Terms of Use

what's next then?

?

who else is out there?

how about security?

- anonymicity

packet capture fiesta

ideas?

le (at) ruckuswireless.com

luiz.eduardo (at) gmail.com

thanks

- Noid, Evil and layerone crew