



Cracking the poor and the rich

Discovering the relationship between physical and network security

Damian Finol
Informatics Engineer

[Author]

- Damian Finol
- Venezuelan
- Engineer in Informatics
- Currently doing a Masters in Computer Science with focus on Distributed systems and paralellism
- Working as an Information Security Specialist for a venezuelan Bank
- Teaching Databases, Operating Systems and Data Security at Universidad Nueva Esparta
- Totalfarker

[Project in a nutshell]

- Started as Wi-Fi mapping of Caracas, Venezuela
- Seeks to understand if the difference in wealth affects network security
- The future?, electronic fences over wireless?

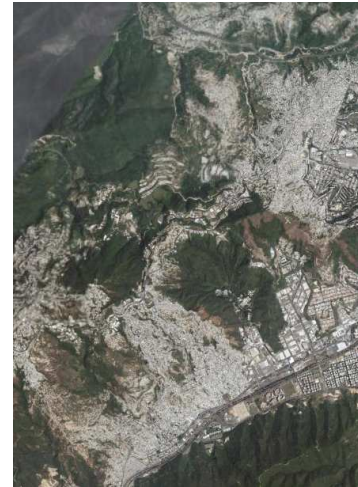
Venezuela



- Located in South America
- Has a GDI of 0.826
- Over 53% of the population lives under extreme poverty
- 20% of the population has access to the Internet.
- 86% of Venezuelans have a mobile phone (2nd in Latin America)
- 45%+ access internet from their homes, 27% of them get it from Wi-Fi Cafés.
- 67% of Internet users come from the D and E status (Poorest users)
- Most of the poor live in slums located in the extreme east (Petare) and extreme west (Catia, 23 de Enero, etc)

[Slums]

- Two big Slums in Caracas, One located to the west (left) The other to the east (right)
- Internet connections available using 3G modems, EVDO / EDGE Cell networks and WIMAX.
- Low physical security: houses (ranchos) are built using mud, adobes and zinc ceilings



[Wealthy neighborhoods]

- Mostly in the Eastern and south eastern side of the city
- Patches of high density high rise buildings (Mostly in the East) and houses / mansions in the South East.
- Internet connections are mostly DSL and Cable
- Wi-Fi Cafés almost inexistent
- Buildings are built with concrete (unlike American's card box constructions)
- Strong physical security: Electric fences, watch guards, dogs, motion detection sensors, bulletproof windows and cars, cameras, gated communities.



[Wi-Fi Cafés and Internet use]

- Slum version of Boingo
- SSID Has owner's Cell number
- Phone cards are used to purchase wi-fi key
- Key is reissued Sunday evening
- Requires strong security: WPA/WPA2
- Internet use is mostly recreational (Messenger), Crime (Identity theft, investigating kidnap victims, blackmail) or illegal informal economy (piracy of movies, music, software)



[Tools of the trade]

- Acer Aspire One with Atheros chipset



- Backtrack 4 beta + Kismet



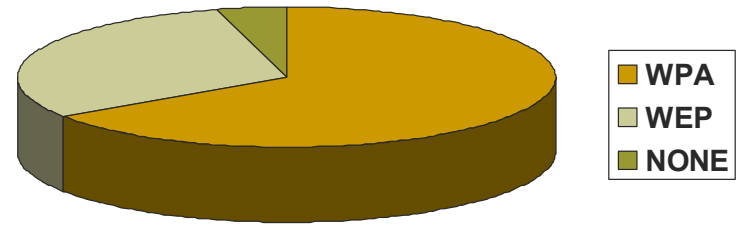
- Volkswagen FOX 2008 and driving like crazy!



[Wi-Fi raw in the Slums]

- Sample of 400 random Wireless networks in Catia (Big slum – Western Caracas)
 - 262 using WPA / WPA2
 - 121 using WEP
 - 17 not using encryption (unsecured)

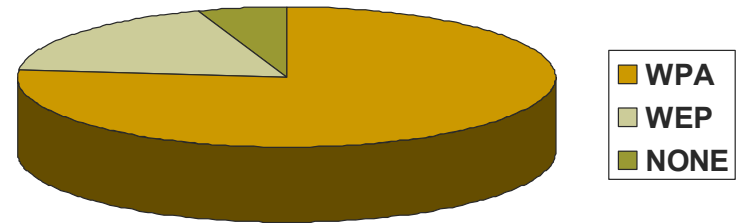
- 43 Wi-Fi Cafés.



[Wi-Fi raw in the Slums]

- Sample of 400 random Wireless networks in Petare (Biggest slum – Eastern Caracas)
 - 307 using WPA / WPA2
 - 72 using WEP
 - 21 not using encryption (unsecured)

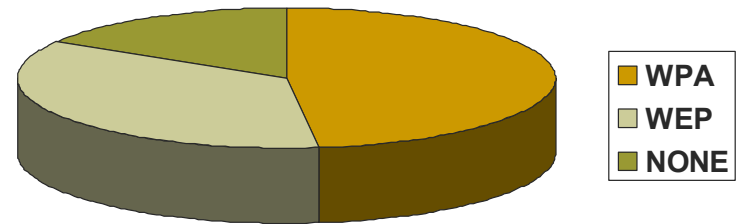
- 82 Wi-Fi Cafés.



[Wi-Fi raw in the rich areas]

- Sample of 400 random Wireless networks in Chacao (Eastern Caracas)
 - 192 using WPA / WPA2
 - 142 using WEP
 - 66 not using encryption (unsecured)

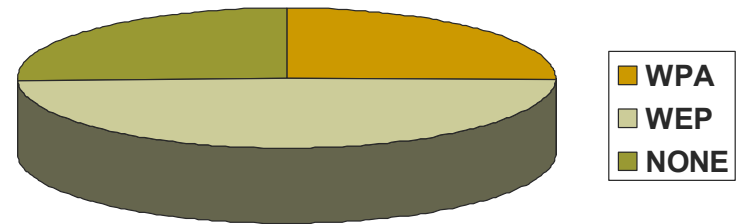
- 11 Wi-Fi Cafés.



[Wi-Fi raw in the rich areas]

- Sample of 400 random Wireless networks in Prados del Este / Hatillo (South Eastern Caracas)
 - 101 using WPA / WPA2
 - 197 using WEP
 - 102 not using encryption (unsecured)!

- 3 Wi-Fi Cafés.



[Notes on results - Slums]

The results taken from the samples in the slums tend to show that people living in the slums hold great value for their internet and their network security. Internet after all is a commodity, one that doesn't come cheap for them, hence the need to use stronger security mechanisms to prevent theft of it.

Special note should be taken of Wi-Fi Cafés, which offer unlimited Internet over wireless for a set period of time and due to the nature of their business, they must provide a high level of security in their network to protect against theft and incurring in losses. This in turn drives conscience of security on the people who use the service.

Finally, one should look at how low physical security in the slums affects the population, Caracas is by far the most dangerous city in the world ranked No 1 murder capital with over 130 killings for every 100k residents, followed by Cape Town with 62 per 100k (almost half). Ranchos (Slum houses) don't offer much protection from theft, vandalism, stray bullets. Yet people in the slums activate advanced encryption techniques to protect against Internet service theft.

[Notes on results - Wealthy]

Results from wealthy areas aren't exactly astonishing and predicted by the hypothesis, Internet is highly available on wealthy areas from different sources, 3G, WiMAX, EDGE/EVDO, DSL, Cable, Satellite, calls for a high demand of legal internet service, one that isn't shared and allows full bandwidth speed.

Special note on the difference between High Rise buildings and houses, the first one, specially in the Chacao area there exists a very high concentration of Wireless networks, whereas in residential (almost suburban) house complexes there is low concentration. This comes from population density and signal dissipation (Over yards and several walls). The 400 sample had to be taken from both slums and rich areas because of the low amount of wireless networks available in the South Eastern side (house complexes)

Finally, the wealthy areas have strong physical security, like gated communities, electric fences, guards, dogs, cameras and motion detection sensors. Yet, they don't use advanced encryption techniques, settling for 'router defaults' (Indeed, a large number of default SSID's where seen) or a high number of unsecured networks.

[Wrap up]

- Questions? Comments?
- E-mail: damian.finol@gmail.com