CERIAS

the center for education and research in information assurance and security

Wireless Security Analysis

Prof. Anthony Smith, Sarath Geethakumar, Utsav Mittal, Ryan Poyar

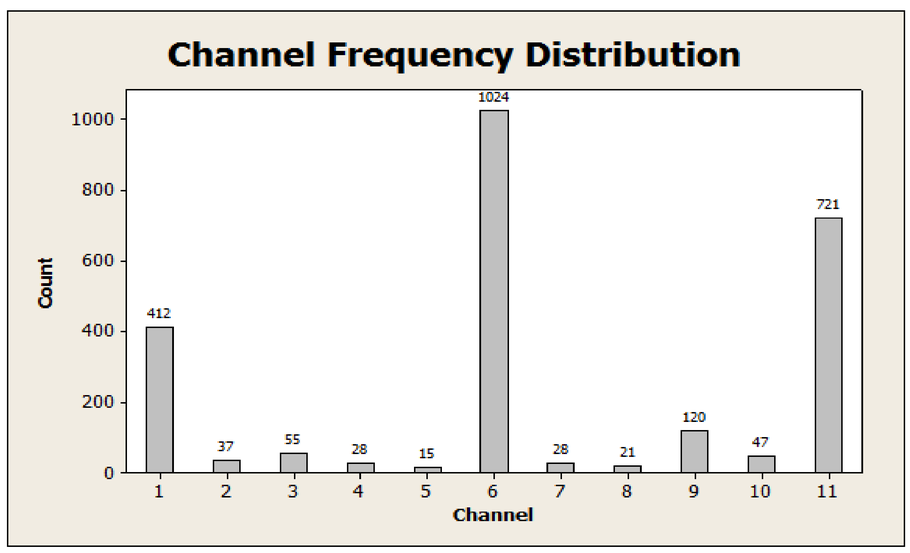
Area Under Study : Lafayette/ West Lafayette
Total Wireless Access Points Detected = 2508
50% of networks are either WEP or OPEN – COMPLETELY INSECURE

Wireless Security Options:
Open – No password required for connection
WEP (Wired Equivalent Privacy) - Basic encryption is used. **Completely broken.**
WPA (Wi-Fi Protected Access) - Advanced encryption is used. Possible vulnerabilities within the authentication phase (TKIP)
WPA2 (Wi-Fi Protected Access 2) - Currently the best option to secure a network. Fixes a few of the minor issues in the original WPA.

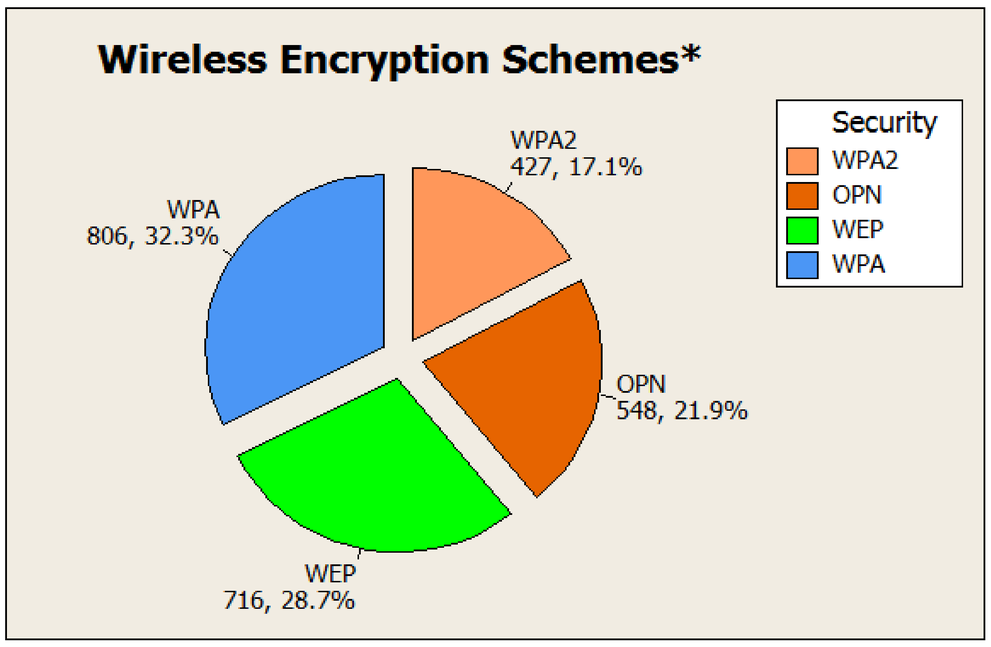
WEP Security Statistic:
- 716 out of 2508 Access Points use WEP (28.7%)
- WEP is not considered secure anymore
- 50% of networks are either WEP or OPEN.
- Easy targets for WARDRIVERS and attackers.
- Time taken to crack WEP – 4 min 11 seconds
- Tools used : airodump-ng, aireplay-ng
- **Not advisable to use anymore.**

WPA Security Statistic:
- 806 out of 2508 Access Points use WPA (32.3%)
- Safer than using WEP or leaving access point OPEN.
- Breakable if passphrase is dictionary word – Dictionary Attack
- Breakable if SSID is common SSID – Rainbow Table Attack
- Tools used – airodump-ng , airbase-ng, aireplay-ng

Ways to secure WPA-PSK:
- Avoid dictionary words as passphrase
- Avoid common SSID as network name or SSID.
- Avoid using default channels. Most common channels – 6 &11
- Disable SSID broadcast .
- Use MAC Access Control List along with wpa-psk



Lafayette Wireless Security Statistics:



TOP 6 SSID'S IN LAFAYETTE

SSID	COUNT
LINKSYS	143
NETGEAR	40
BELKIN54G	29
DLINK	15
WIRELESS	7
TSUNAMI	3

Attacks on Wireless Networks:
WEP Crack (basic) - wait for packets to capture
WEP Crack (replay attack) - replay a single packet many times to generate a lot of packets
Korek-ChopChop WEP Crack - doesn't require clients to be associated
WPA Crack - Capture a handshake (association). Do an offline dictionary attack or Rainbow Tables. (only works with weak passwords)

DOS:
Deauth Attack - Continuous sending of a fake de-association request to a client(s)
Frequency Jamming - Continuous transmitting of data on a specific frequency (causing constant collisions) - higher power jamming helps

Channel Frequency Distribution:
- 86% of AP's use default channels 1,6 or 11
- 41% of AP's on Channel 6
- Causes interference amongst AP's on same channel.
- Jamming a channel affects all AP's on that channel.
- Easy for attackers to target.
- Jamming Channel 6 renders 41% networks useless.

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center

CERIAS

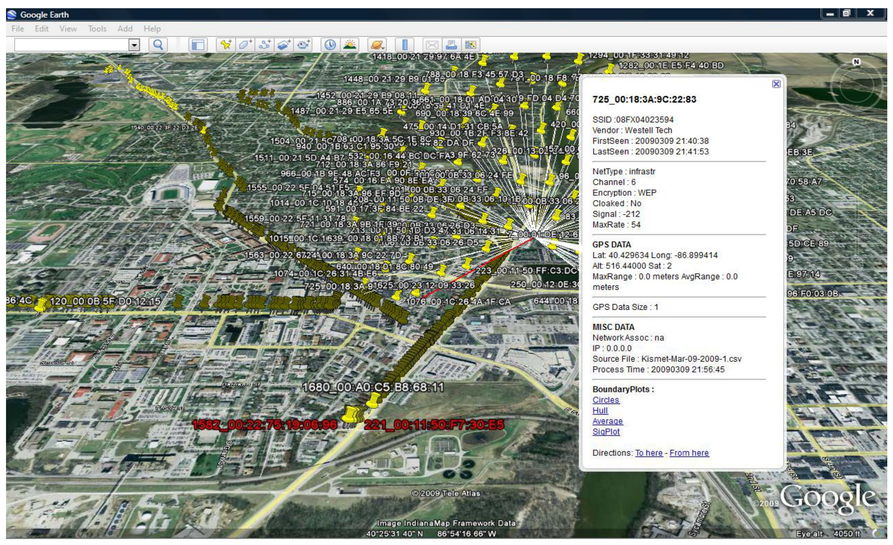
the center for education and research in information assurance and security

West Lafayette – WI-FI Snapshot

Prof. Anthony Smith, Utsav Mittal, Ryan Poyar

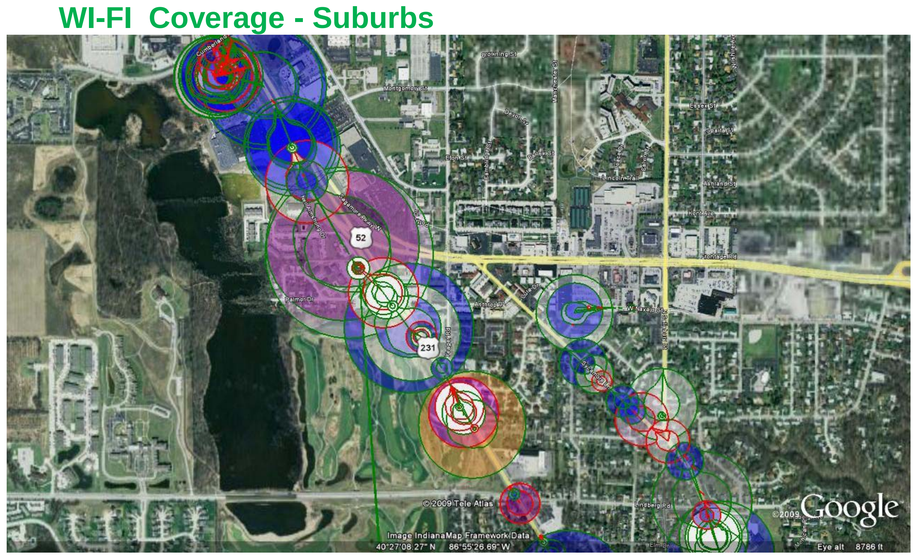
- **Data collected using GPS and wireless laptop.**
- **Approx. 1700 wireless AP's in the sample**
- **Data projected using Google Earth.**

Access Point Details

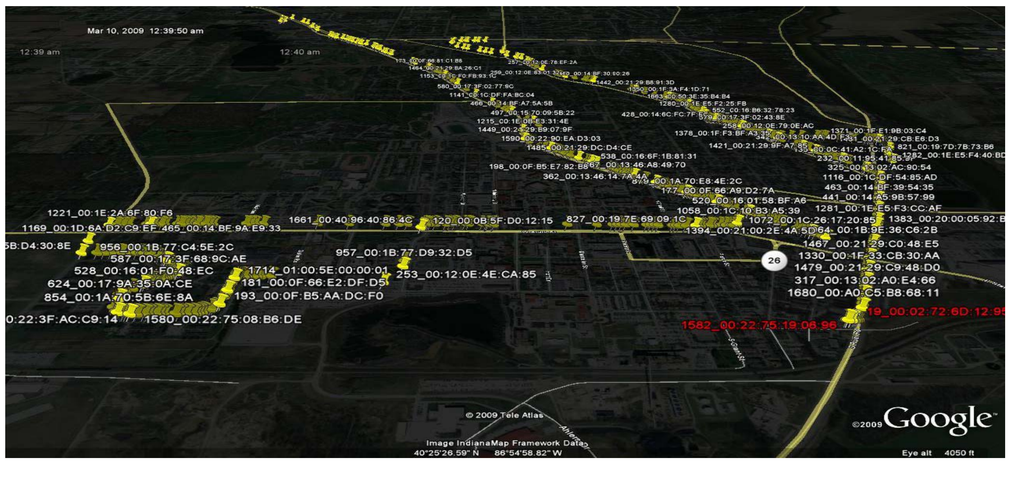


Street View

WI-FI Coverage - Suburbs

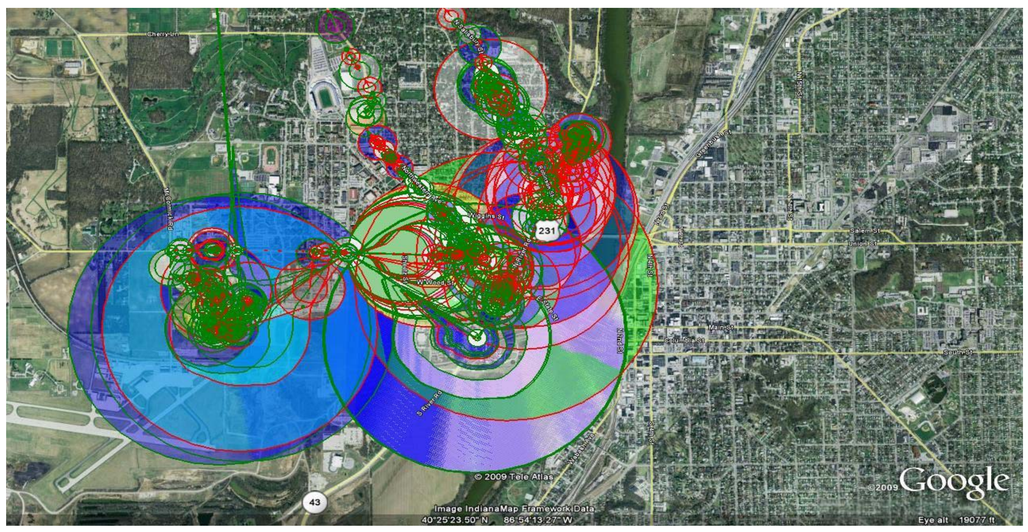


Wireless Access points across West Lafayette



WI-FI Overview – Night View

Downtown West Lafayette



PURDUE UNIVERSITY

CERIAS®

Discovery Park e-Enterprise Center