

Wardriving Project

Group #1: Emmanuel Cardenas, Natalia Cardona, Steele Choate

Tim Fielder

UTPB

November 19, 2024

Group Members

We were group #1, consisting of:

- Emmanuel Cardenas: Driver
- Steele Choate: Analyst
- Natalia Cardona: Programmer

UTPB

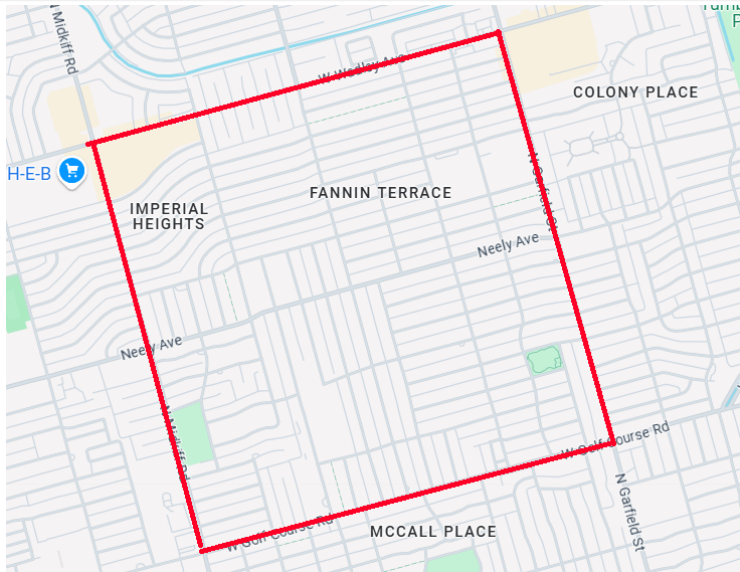
Geographic Location

Our group covered the area bounded by:

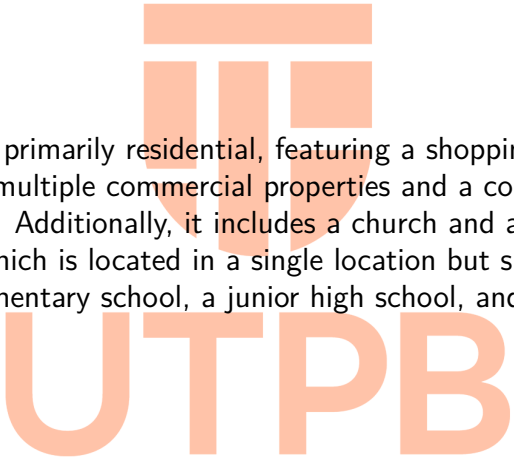
- W Wadley to W Golf Course
- N Midkiff to N Garfield

UTPB

Map of Area



Description of Area



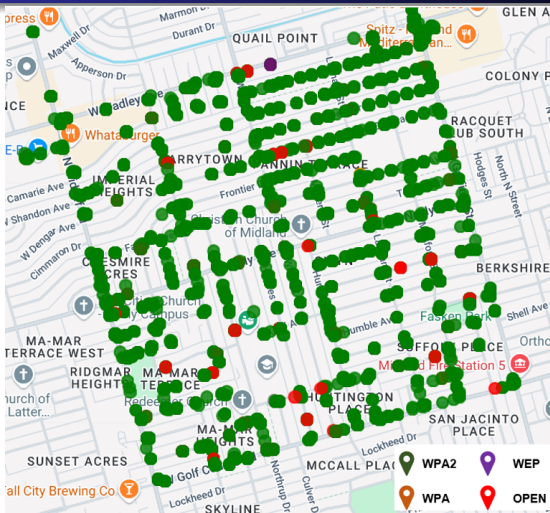
The area is primarily residential, featuring a shopping center plaza with multiple commercial properties and a couple of restaurants. Additionally, it includes a church and a school complex, which is located in a single location but subdivided into an elementary school, a junior high school, and a high school.

Data

We found 3770 total access points, falling into the following broad categories:

- Open: 147
- WEP: 2
- WPA: 2
- WPA2: 3606
- WPA3/WPA2 EAP Only: 13

Map of APs



HTML Map Link

Open APs

Of the open APs we found, these appear to have no security at all:

Security Type	Open
---------------	------

Count of SSID	
[ESS]	147
[ESS][WPS]	9
Grand Total	156

Map of Open APs



WEP APs

These APs are operating in WEP mode only:

Security Type	WEP	
---------------	-----	--

Count of SSID	
[WEP][ESS]	2
Evans	1
rfcl13ntA	1
Grand Total	2

Map of WEP APs



WEP APs


These APs provide WEP as a backwards compatibility option:

- None were found in the area.

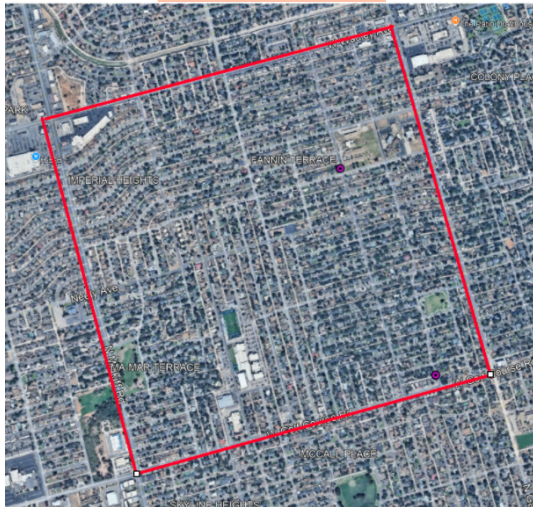
UTPB

WPA APs

These APs are operating in WPA mode only:

Security Type	WPA	
Count of SSID		
[WPA-PSK-TKIP][ESS]	2	
DOWNHOME	1	
House_Ext	1	
Grand Total	2	

Map of WPA APs



WPA2 APs

These APs provide WPA as a backwards compatibility option:

Count of SSID	
WPA2	3606
Grand Total	3606

Map of WPA2 APs



Relevant Findings

- Unsecured Systems with Strong Signals:
Open networks ([ESS]) or those using WEP with strong signals can be exploited for monitoring or proxy attacks.
- Backward Compatibility Risks:
Mixed protocols like [WPA2-PSK-CCMP+TKIP] weaken security by supporting outdated components.
- WPS as a Weak Link:
Networks with [WPS] enabled are prone to brute-force attacks on the PIN, compromising strong encryption.
- Signal Strength as an Indicator:
High-signal networks with weak security attract exploitation attempts.

What can someone do with this information?

- Reconnaissance for Exploitation
 - Target weak protocols (WEP, WPA).
 - Brute-force PSKs or crack encryption
- Exploitation of [ESS][WPS]
 - Attack WPS PIN to extract PSKs.
- Targeting Open/No Security Networks
 - Sniff unencrypted data.
 - Perform MITM attacks.
- Mapping Network Vulnerabilities
 - Identify weak settings in mixed configurations.
 - Exploit backward compatibility modes.
- Social Engineering
 - Leverage network info for phishing or deception.

Questions



UTPB