# “Free” Wifi: Breaking in to WEP encrypted networks

CIS4360 Project

Matthew Tschiggfrie and Kevin Huynh

## Goal:

Access a WEP password protected wifi network

## Method:

Exploit WEP vulnerabilities to implement an attack based on Initialization Vectors to obtain key

# WEP

- Packets encrypted using RC4 stream cipher
- Two part 128 bit key:
  - 24 bit Initialization Vector
  - 104 bit root key
- IV is pseudorandomized for each packet
- Root Key is shared across the network
- Programs available online can get in WEP networks in under 3 mins

# Brute Force

- 64-bit WEP key
  - 40-bit key + 24 bit initialization vector
  - 2^40 = 1,099,511,627,776 possible keys
- 128-bit WEP key
  - 104-bit key + 24 bit initialization vector
  - 2^104 = 20,282,409,603,651,670,423,947,251,286,016 possible keys
- Let's say we can try 50,000 keys a second
  - 254 days for 64-bit
  - 10^19 years for 128-bit
- Obviously not going to work

# Using Known Duplicates of IVs

- Need multiple packets with duplicate IVs
- 50% that an IV will repeat after 5,000 packets
    - Collect patiently or inject packets for responses
- Take XOR of 2 encrypted packets with same IV
    - perform statistical analysis on this to get the key
- Log into the network with this key
- Takes between 50 seconds and 20 minutes

# Progress/Split Work/What Next

- Researched what we need to do
    - now how do we do it?
- We are responsible for reading and researching on our own
- Going to get together for work
- Figure out how to read/inject packets from a network

# References

http://eprint.iacr.org/2007/120.pdf

https://www.isoc.org/isoc/conferences/ndss/02/papers/stubbl.pdf

http://www.opus1.com/www/whitepapers/whatswrongwithwep.pdf

http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html