‘Wardriving’:

A wireless data poaching

- T.J. Maxx Data Theft Case

T.J. Maxx data theft: Background

- TJX: The parent company of T.J. Maxx, Marshalls and other retailers.
- 45 million credit and debit card users information stolen and sold.

What’s so special.....

- Large data/card information stolen
- Time

Wireless Wardriving

- Driving one’s car around with laptop and antenna to detect wireless access points and see how they’re configured.
- A map can be made of the different access points(when GPS is added).
- Wireless poachers can attack targets from miles away with the help of telescope antenna. (up to 45 miles/ 72 km)

Reason..

- **Store secured using Wired Equivalent Privacy(WEP)**
  - Were using outdated protocol
  - Allowed small amounts of data to leak from data packets flowing across the wireless network.
- **WEP deficiency**
  - Gives up its encryption key when attacked.
  - In standard WEP
    - Every device uses the same key

Wardriving protection

- Use latest wireless security technologies
  - WPA
    - Backward compatible
  - WPA2
    - Stronger authentication
    - A new schedule for rotating encryption keys
  - VPN
  - SSL/TLS

Takeaway…….

- Implement proper security infrastructure
- Keep up with new technologies
- Always be prepared