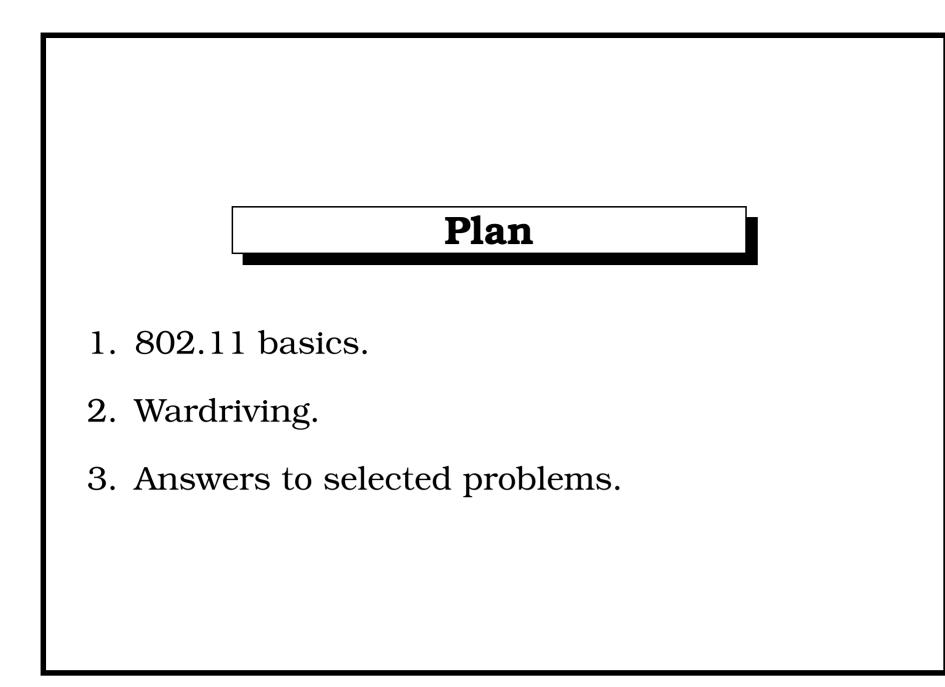
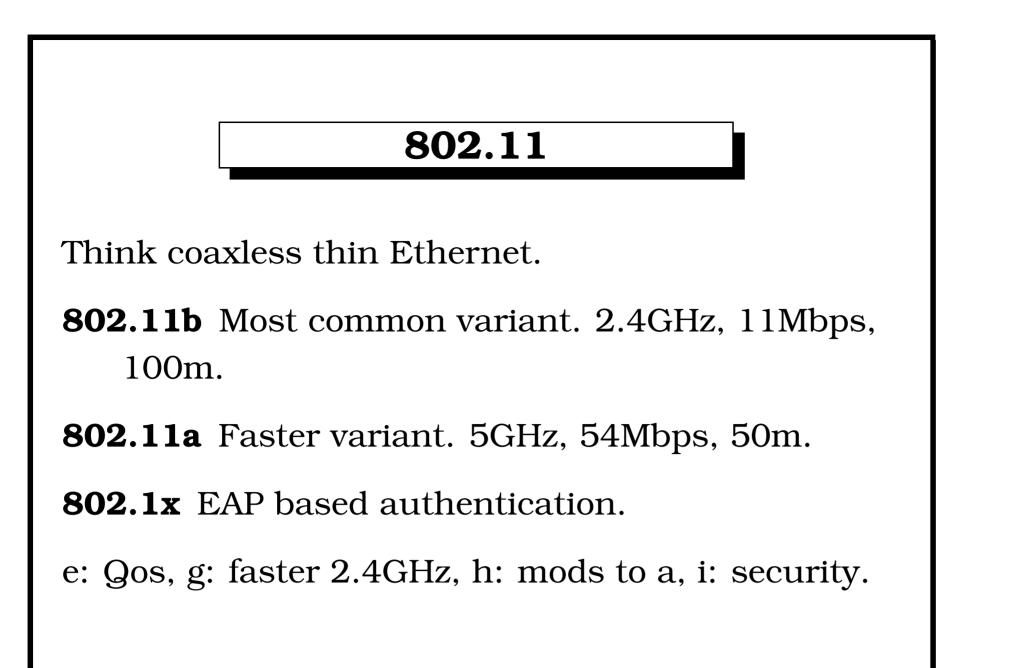
802.11b and the Joy of WarCycling in Dublin

David Malone

12 November 2002





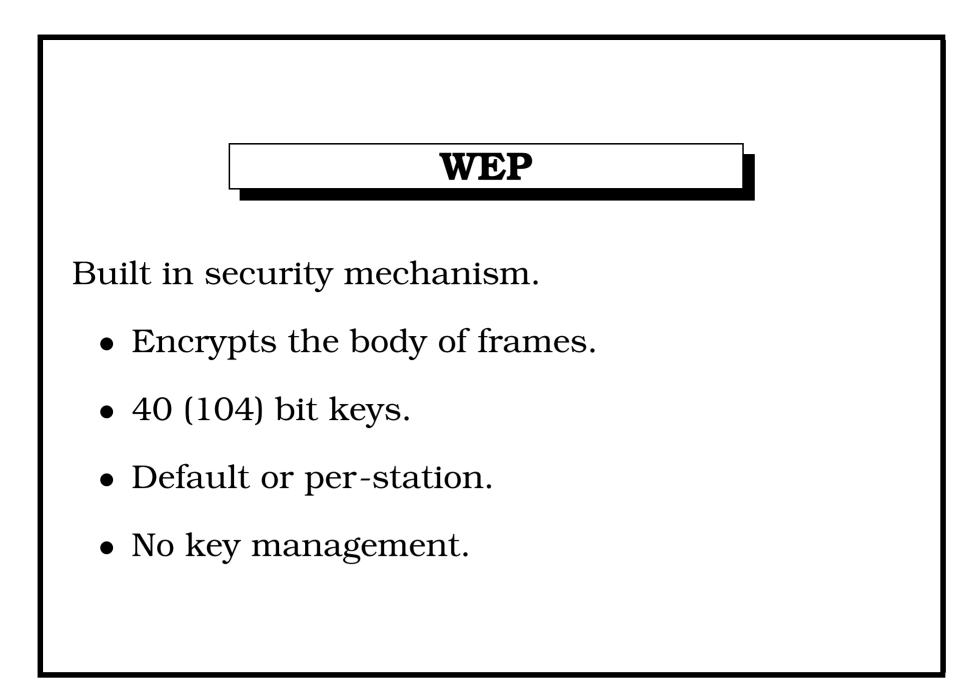
802.11b Concepts

Channel Frequency for communication (1–14).

BSSID Group of communicating individuals (MAC).

SSID Network name (20 chars).

mode Infrastructure/ad-hoc (IBSS).

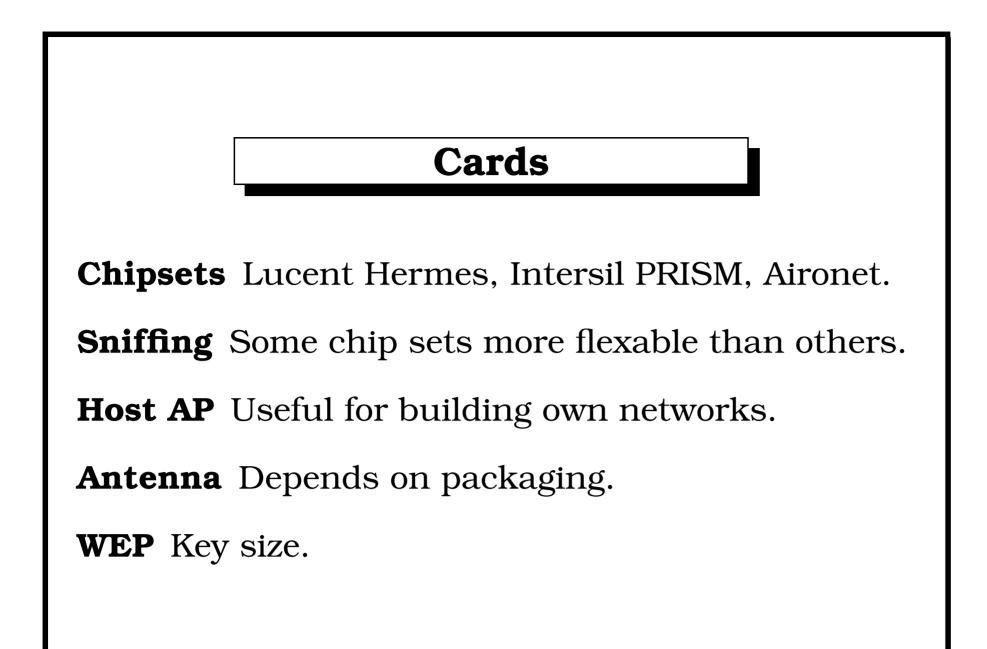


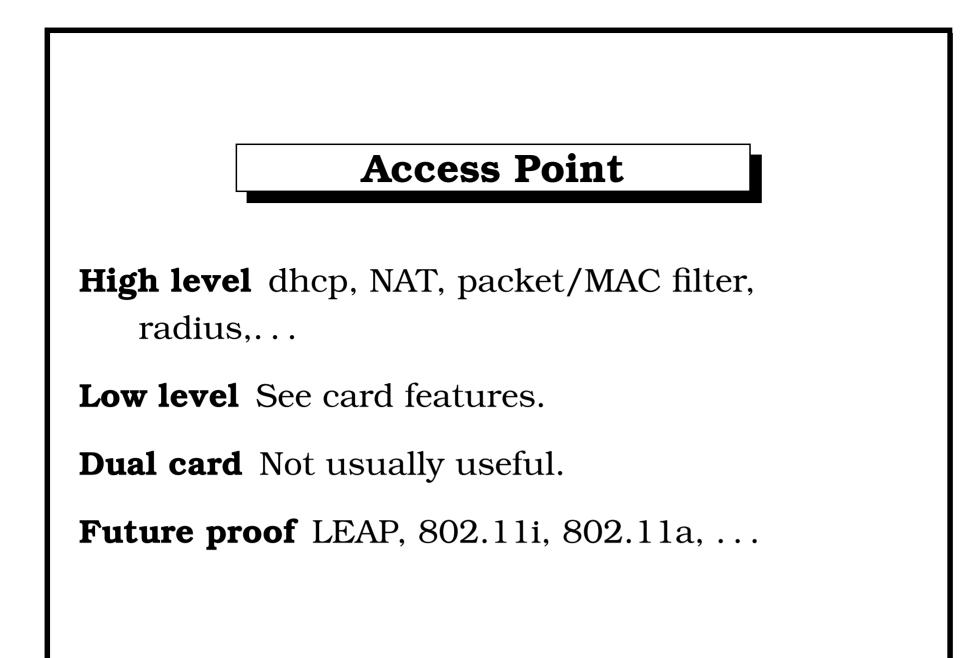
WEP Problems

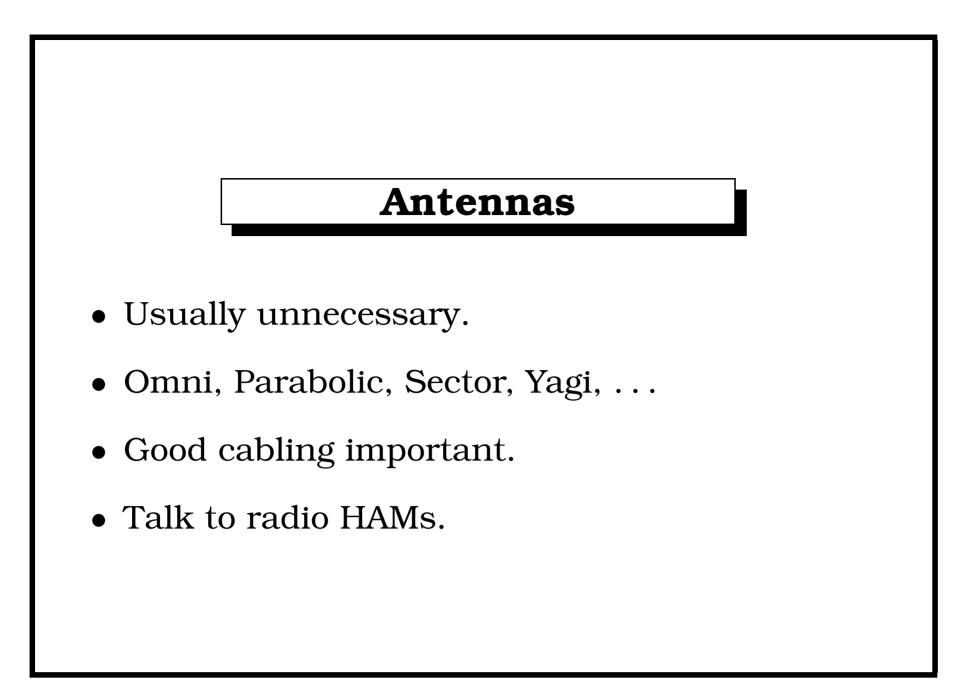
Has been shown to be flawed.

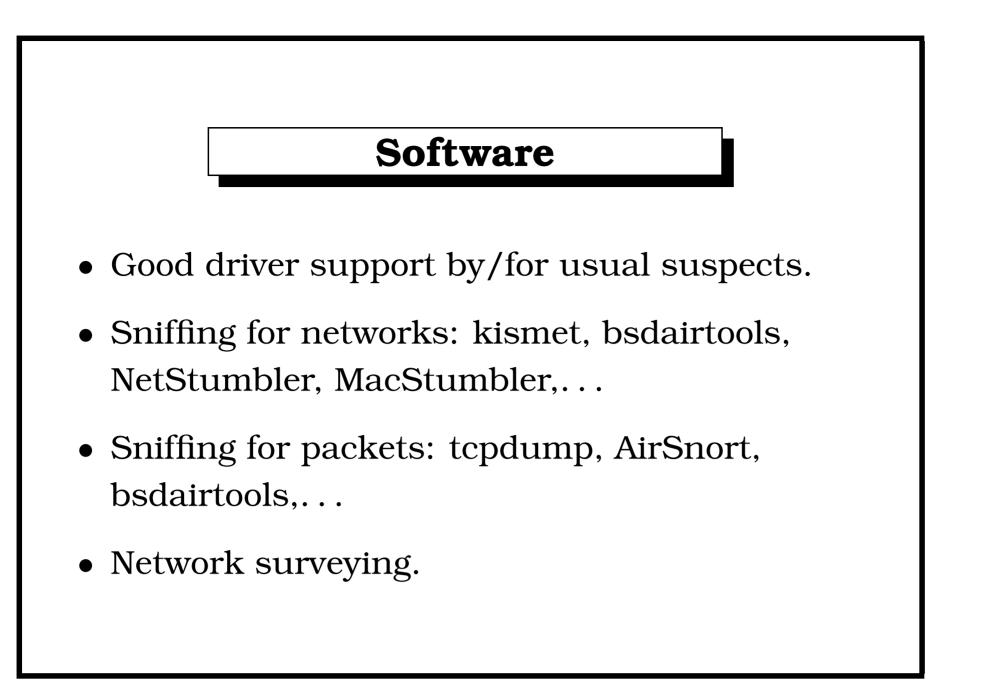
- Key is usually constant.
- First byte is 0xAA.
- Initial Vector is observable.

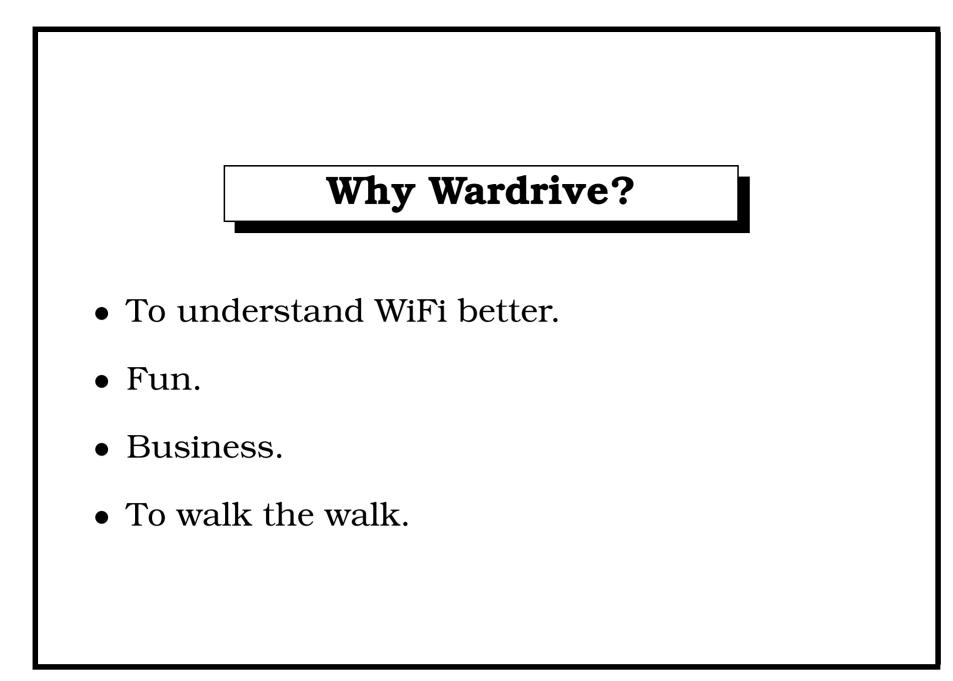
Some IVs provide information about key.











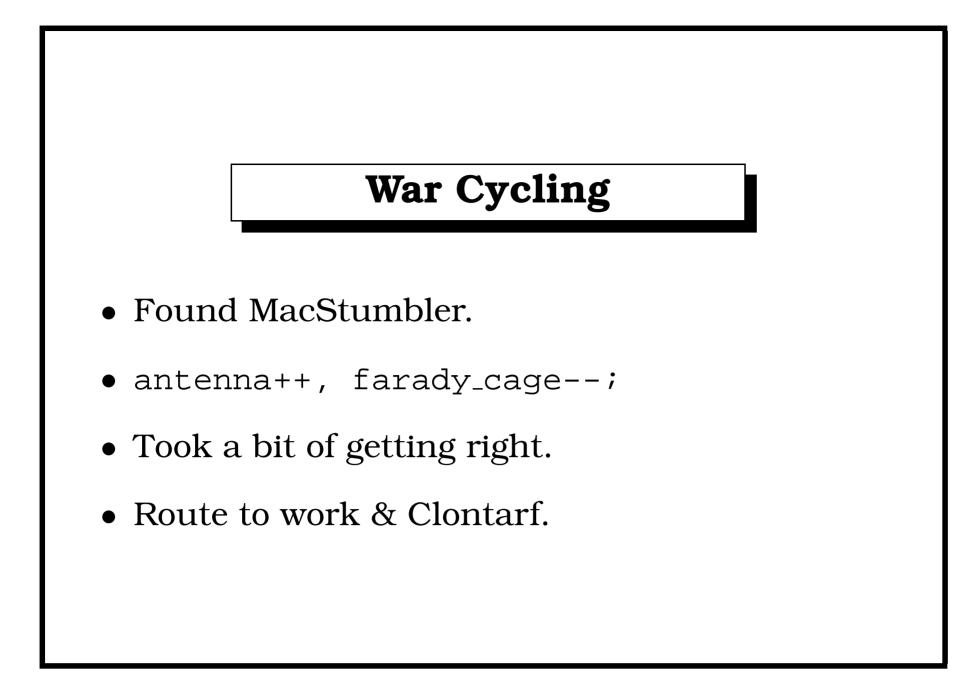


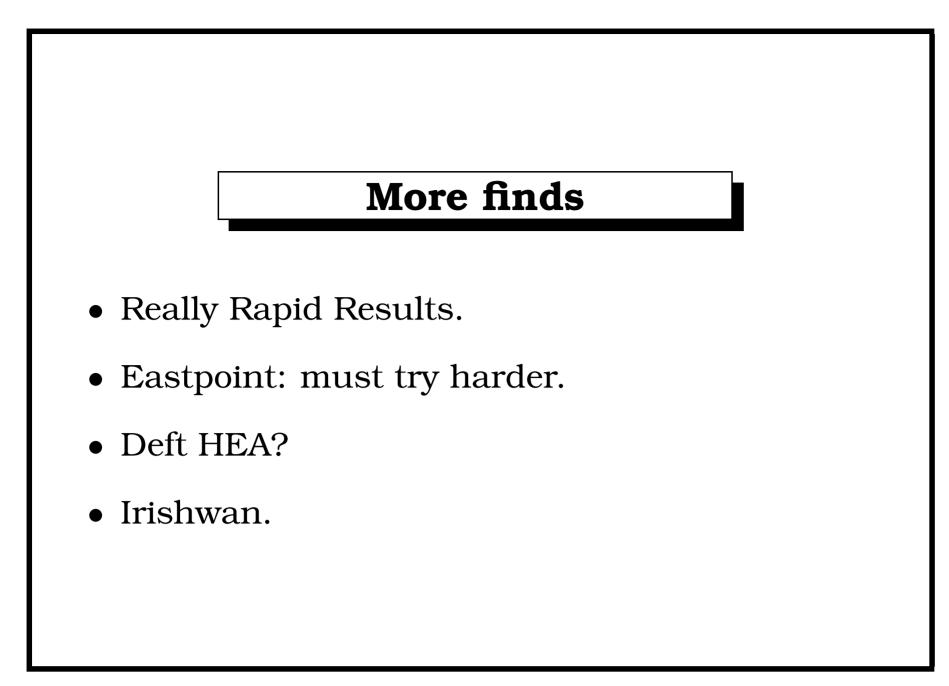
- Expand to around town.
- Industrial Estates.
- Missing pieces.

Interesting Finds

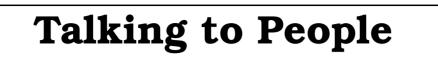
- IFSC and friends.
- Big network in the docs.
- Public service use?
- Industrial estate spotting.





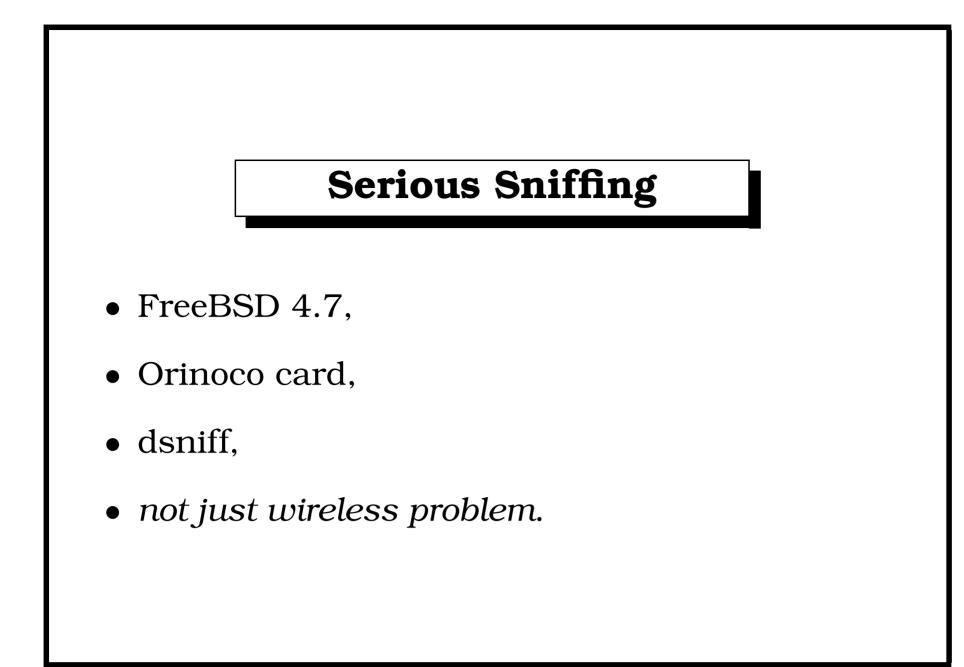






- Legal advice.
- Help with mapping.
- 'Guys in a car. . . '
- Feedback.

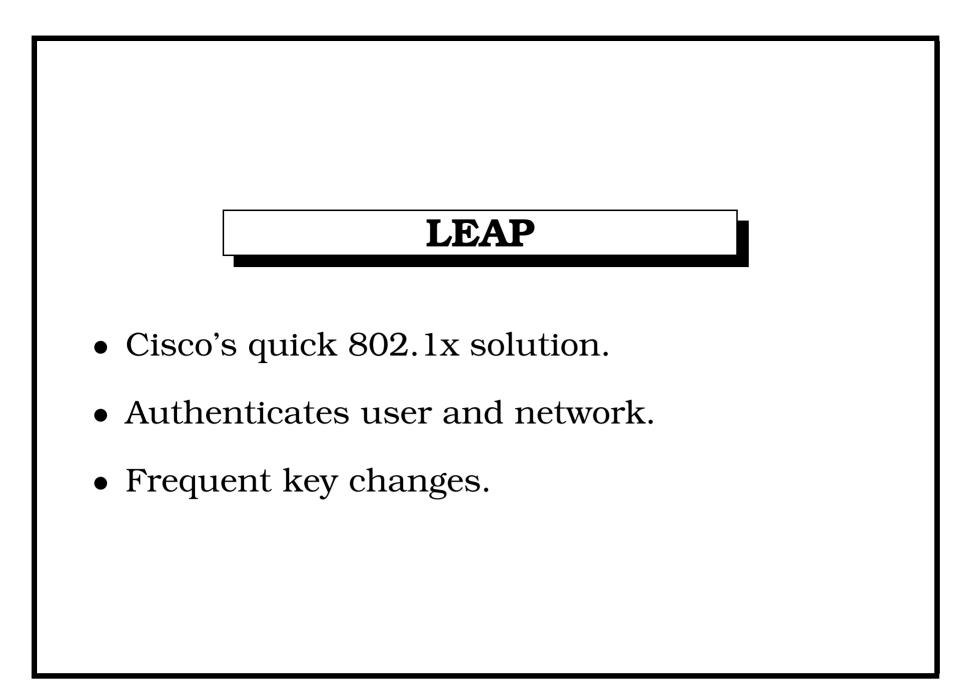




Dirty Wireless

- Put wireless on own network/VLAN.
- Do normal ingress/egress filtering.
- Application level security.
- Doesn't protect wireless network.





IPsec/VPNEncryption to local gateway.

- Authenticate with local gateway.
- WEP shouldn't be a factor.