Security in 802.11 Wireless Networks

David Wagner

University of California, Berkeley

The Setting

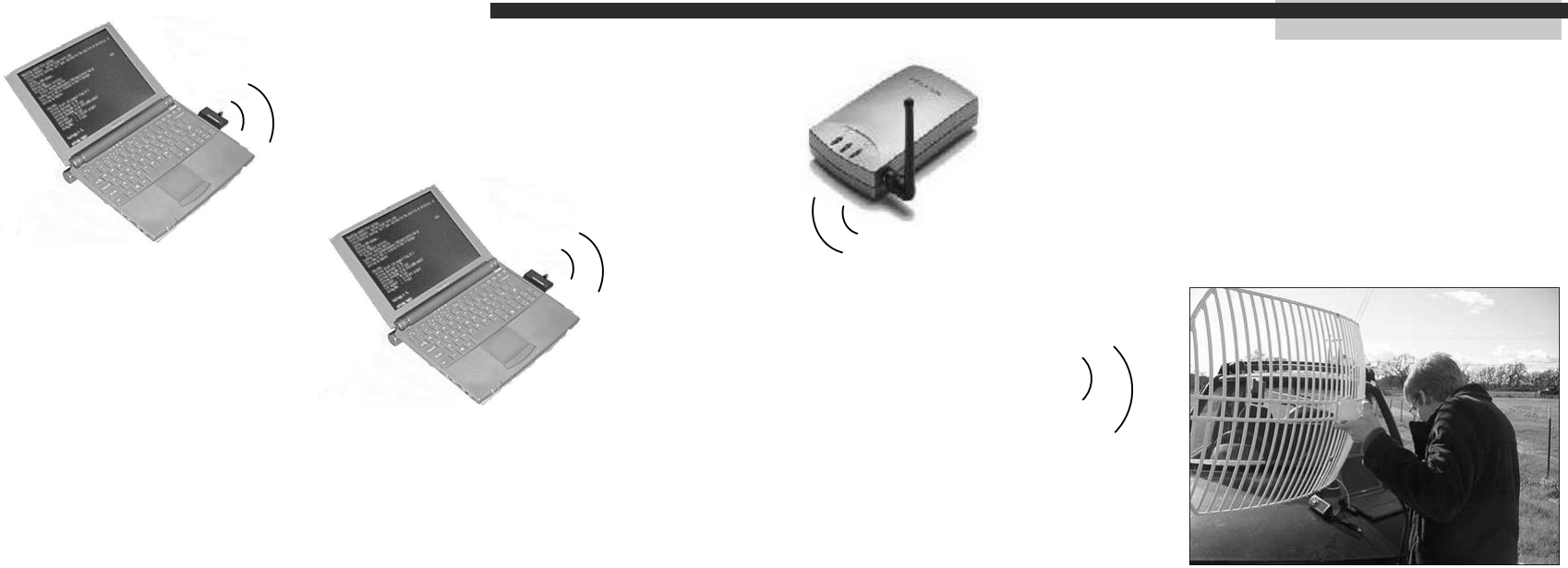
An example of a 802.11 wireless network

(current installed base: ~ 15 million users)

The Problem: ***Security***!

- Wireless networking is just radio communications
  - Hence anyone with a radio can eavesdrop, inject traffic

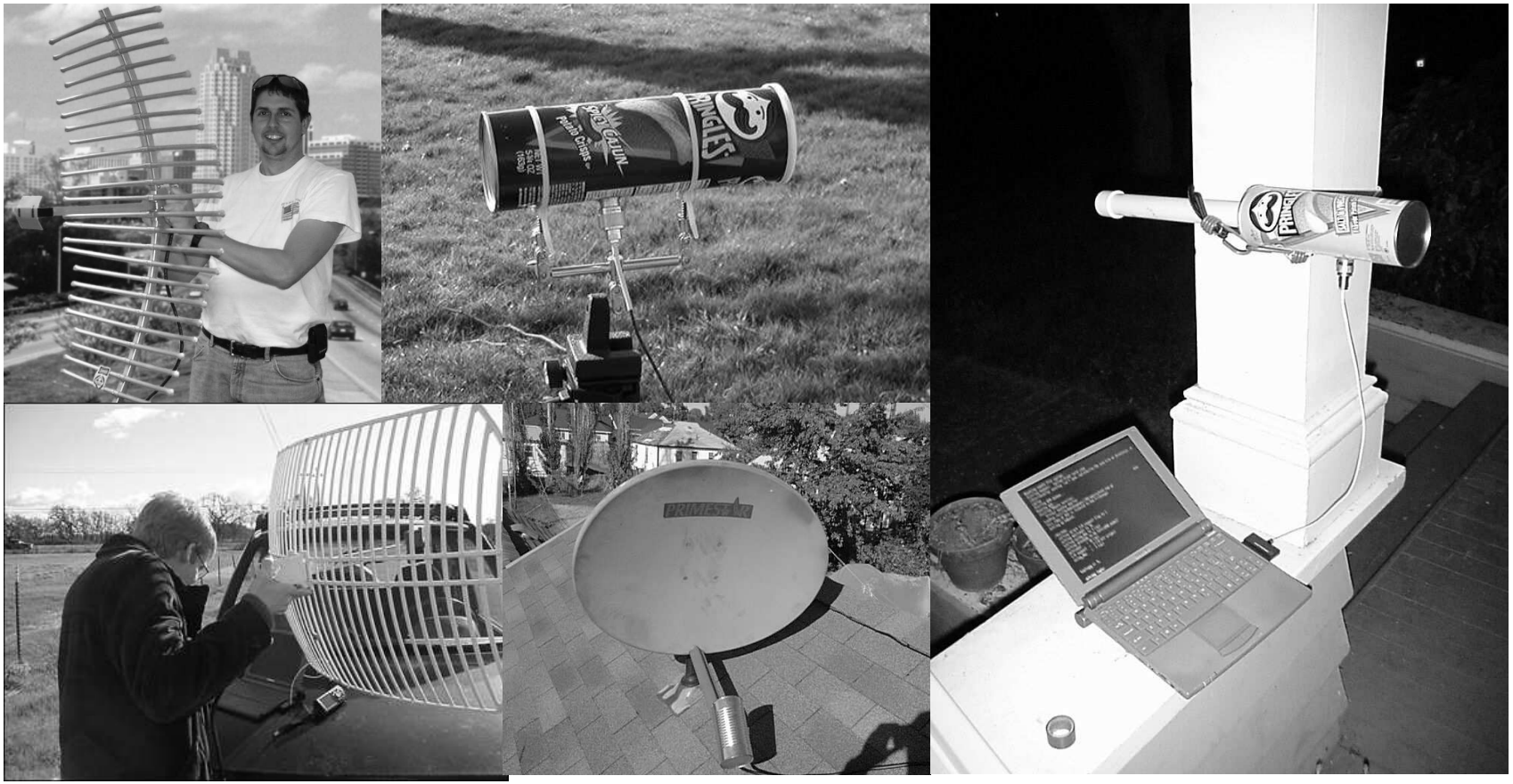
The Problem: ***Security***!



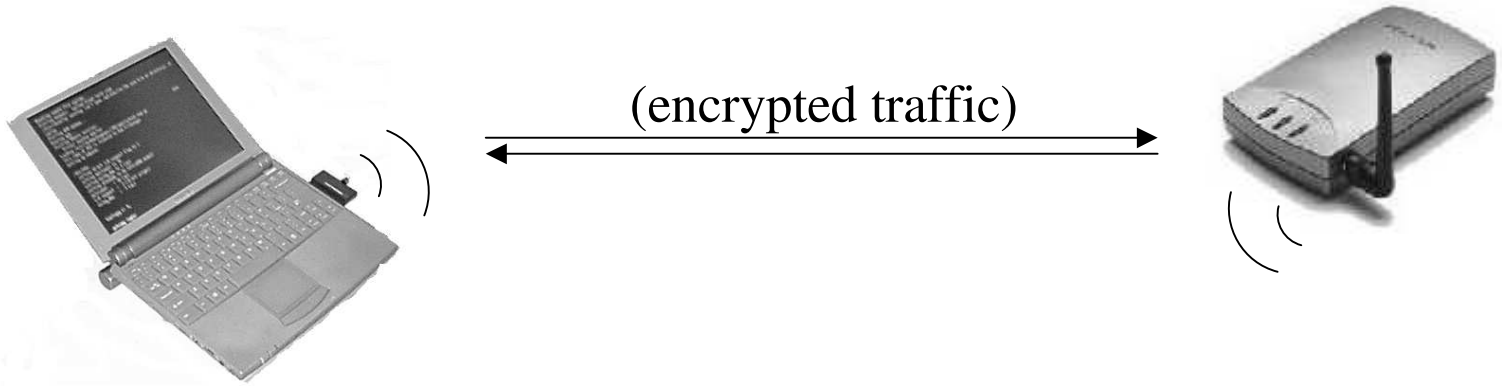
- Wireless networking is just radio communications
  - Hence anyone with a radio can eavesdrop, inject traffic

The Security Risk: RF Leakage

Toys for Hackers



WEP



- The industry's solution: WEP (Wired Equivalent Privacy)
  - Encrypt all data traffic, using a globally shared RC4 key
  - Detect spoofed packets with a CRC checksum

Problems with 802.11/WEP

- WEP is cryptographically insecure
  - Can learn key by observing a few million packets (RC4 was used improperly) [FMS]
  - CRC checksum is insecure [BGW]
- WEP is often not used
  - High administrative costs (WEP punts on key mgmt)
  - WEP is turned off by default

Summary

- 802.11 networks: insecure in theory & in practice
  - 802.11 encryption is readily breakable, and 50-70% of networks never even turn on encryption
  - Hackers are exploiting these weaknesses in the field, from distances of a mile or more