

# Airsnarf

*Why 802.11b Hotspots Ain't So Hot.*

# Coming up...

- Disclaimer
- Example hotspot setup & weakness
- Rogue APs
- Demo of Airsnarf
- Defense strategies

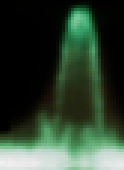
# Disclaimer

- This presentation and example software are intended to demonstrate the inherent security flaws in publicly accessible wireless architectures and promote the use of safer authentication mechanisms for public 802.11b hotspots. Viewers and readers are responsible for their own actions and strongly encouraged to behave themselves.

# Example HotSpot Setup

- Visit hotspot provider website and create login
- Visit hotspot with wireless device
- Power on, associate, get IP, DNS, etc.
- Open web browser and get redirected
- Login, backend authentication & billing, welcome to the Internet

Is this secure?



Access Point



SSID: "goodguy"

Stronger or Closer  
Access Point

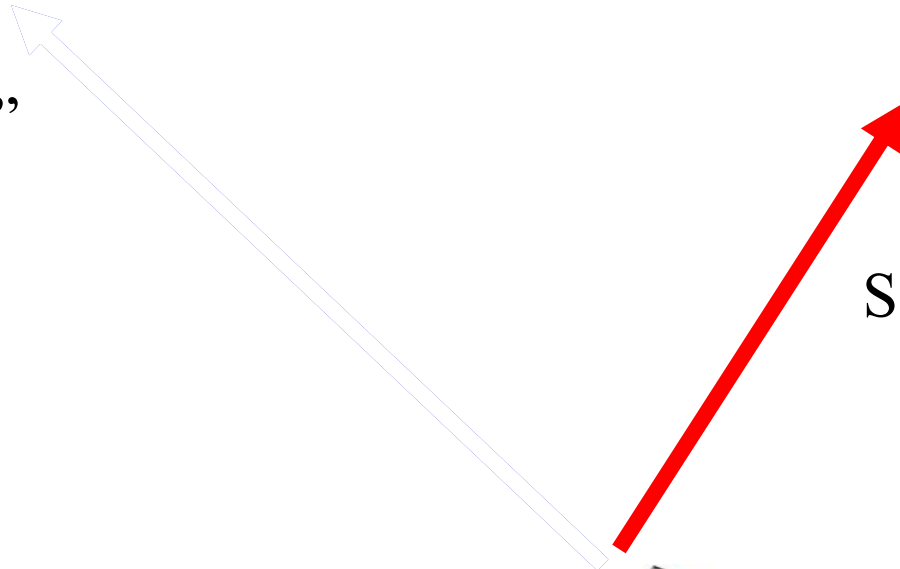


SSID: "badguy"



Wi-Fi Card

SSID: "badguy"



# Rogue APs?

- Rogue AP = an unauthorized access point
- Traditional
  - corporate back-doors
  - corporate espionage
- Hotspots
  - DoS
  - theft of user credentials
  - AP “cloning”

# Hotspot Rogue AP Mechanics

- “Create a competing hotspot.”
- AP can be actual AP or HostAP
- Create or modify captive portal behind AP
- Redirect users to “splash” page
- DoS or theft of user credentials
- Bold attacker will visit ground zero.
- Not-so-bold will drive-by with an amp.



# Airsnarf

- Nothing special
- Simplifies HostAP, httpd, dhcpd, Net::DNS, and iptables setup
- Simple example rogue AP
- Demonstration



# Defense Strategies

- Local AP awareness
- Customer education
- One-time authentication mechanisms
  
- Don't charge for hotspot access?

# Links

- **Airsnarf** - <http://airsnarf.shmoo.com>
- **HostAP** - <http://hostap.epitest.fi/>
- **Red Hat Kernel w/ HostAP** - [http://www.cat.pdx.edu/~baera/redhat\\_hostap/](http://www.cat.pdx.edu/~baera/redhat_hostap/)
- **Looking for hotspots?** - <http://www.hotspotlist.com/>
- **Other “wireless portal software”** - <http://www.personaltelco.net/index.cgi/PortalSoftware>

# Questions?