Have you updated your wireless card drivers lately?
Ryan Riley
rileyrd@cs.purdue.edu

Goals
1. Survey current work on **implementation flaws** in 802.11 cards
2. **Find and test a flaw** in the driver of my Broadcom wireless networking card
3. Write a **point and click** interface for exploiting that flaw

Current Work
- Insecure **operating system** features
  - Revealing the user’s list of trusted networks
  - Silently connecting to trusted networks
  - Not disabling the card when not in use
- **Firmware/Driver flaws**
  - Driver level **buffer overflows**
  - Assuming a well-behaved environment
  - Poor handling of error conditions

Attack Vectors

Broadcom Flaw
- Buffer overflow using network name
- **Case of specification vs. mechanism**
  - Specification allows 32 characters
  - Mechanism allows 255 characters
- A 200 character name can overflow a buffer in the driver
- **Attacks**: Crash, total machine hijack.

Click to Crash
- Created an **easy to use GUI** for Linux designed to make exploiting these flaws easier.
- **Passive Features**:
  - Displays clients in range
  - Displays preferred access points for those clients
- **Active Features**:
  - Send target malformed packets
  - Attempts exploiting 7 known flaws
  - Can cause machine crash

Screenshot

Scary Facts
- These flaws are **remotely exploitable**
- The attacker only needs to be in **radio range**
- **Total machine compromise** is very possible
- 7 flaws were released in November 2006
- Broadcom/Dell patch took **38 days** to be released
- Patch released: 12/19/2006

Conclusions
- Wireless card implementations can have flaws leading to a total machine compromise
- Security professionals and hackers are just beginning to look for them
- **Have you updated your wireless card drivers lately?**