

War Driving by Remote Control

Securing Wireless Assets and Auditing for Rogue Devices

Introduction

- 7 years as a Windows and UNIX sysadmin
- Nearly a graduate of CLU, B.S. in C.S
- Curious about how most everything works.
 - Which can be both an asset and a liability!

What's this about?

- An Introduction to Wireless Security
- Building a war driving RC car using Linksys routers!

Wireless Networking

- Benefits
 - Convenient
 - Mobility
 - Don't have to drag wires all over my house
- Risks
 - It's a radio and anyone can listen to the signal!
 - Security came after the fact

Wireless Security

- None
- MAC Address Filtering
- WEP - (Wired Equivalency Privacy)
- WPA/WPA2 - (Wi-Fi Protected Access)
- WPA w/ Radius, VPN, etc

How Is Wireless Abused?

- Freeloading - Stealing Bandwidth
- Sniffing/Eavesdropping
- Stepping stone into corporate network
 - TJ Maxx - 45.6 million credit cards stolen
 - <http://www.securityfocus.com/news/11455>
- Man-In-The-Middle Attack
 - “Radisson” access point near hotel

State of Security

- Poor configuration

- War drive results
 - 199 Total Access Points
 - 67 with no security
 - 85 with WEP
 - 45 with WPA/TKIP/AES

- WEP is broken

- 104 bit with only 40-80K packets, with 50-95% reliability. All done in under 60 seconds
- <http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/>

Excuses for Poor Security

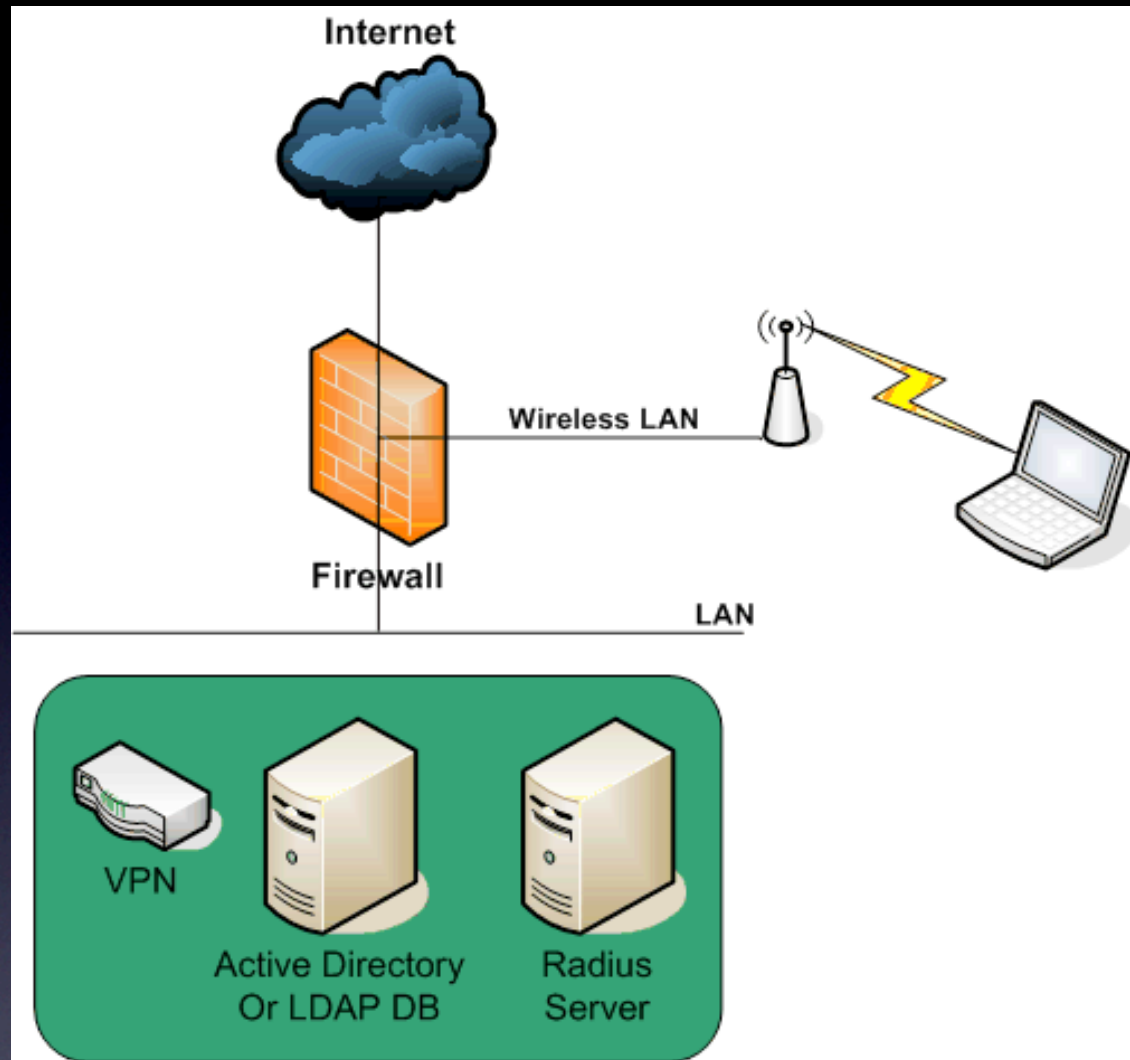
- “I’m just a small business, why would anyone hack me?”
- “I don’t have anything important on my computer, so I’m not worried.”
- “It doesn’t bother me if they use my bandwidth.”

It's important if...

- You bank or pay bills online.
- If you don't want someone attacking someone else using your IP address.
- You'd rather not have someone watching everything you do online.
- If you would rather not have someone downloading child porn using your IP.
- You need low ping times cause you're playing online video games! ;-)

Defense

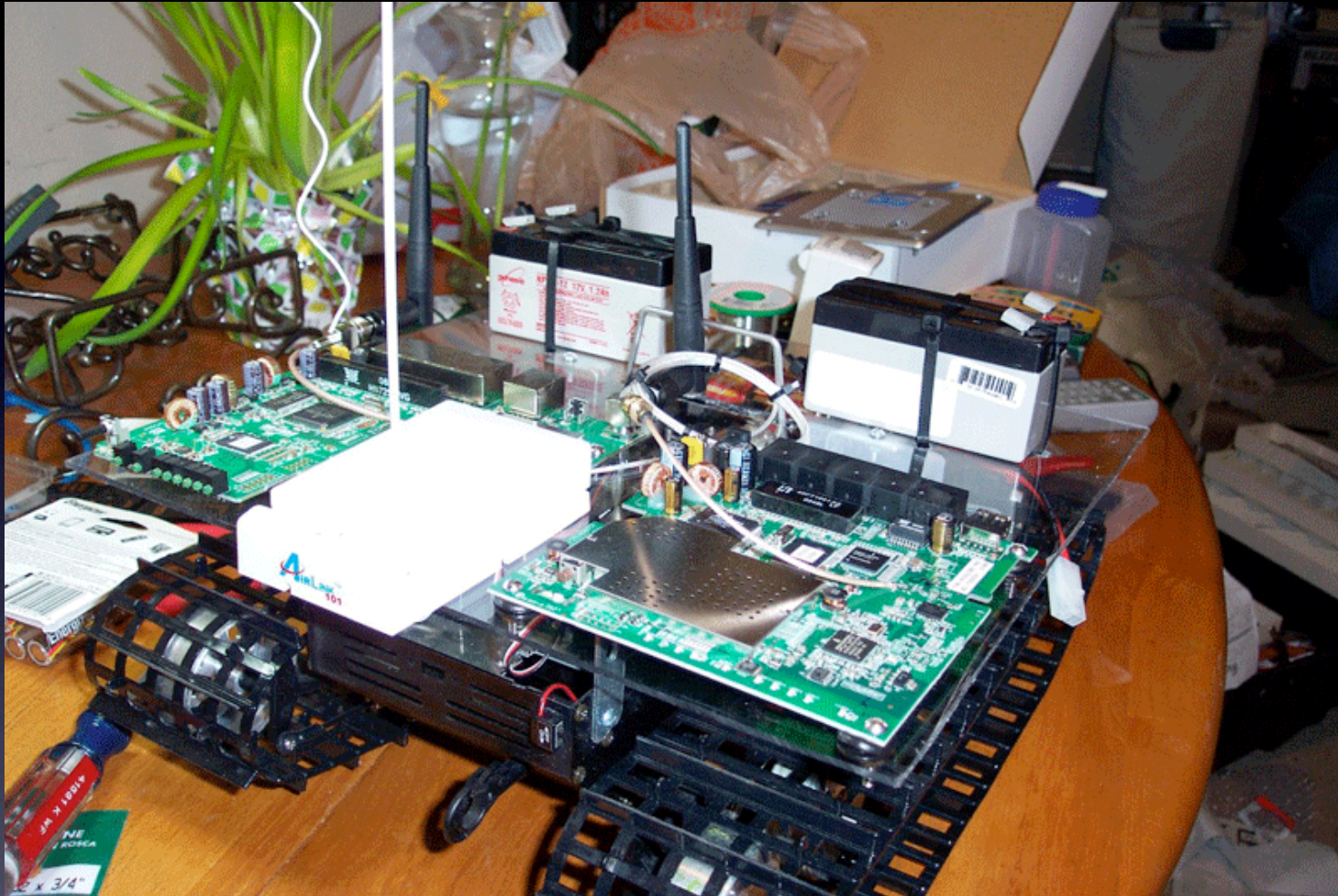
- Monitoring
 - IDS
 - Kismet - Create a mesh of kismet drones to find wireless devices coming into an area.
- Auditing
- Defense in Depth



Defense in Depth?

Other Wireless Tech

- RFID
- Bluetooth
 - Car Whisperer
- Alarm systems?????
- Share common problems in limiting access



Jäger

Where the idea came from

- BoeBot
 - Bluetooth
- Robot Guard Dog - never could find the dog
 - Wireless Sniffing Robot by Schmoo Group
- Purpose

The Schmoo Group's Robot



Functionality

- Wireless detection and sniffing
- GPS
- Activity Remotely Viewable
- Speed

Parts

- Remote Control Car
- Linksys Routers
- GPS Module and Antenna
- Improved Wireless Antenna
 - Stock Linksys antennas run @ 1 - 1.5 dBi
 - New antenna runs @ 10 dBi

Software

- OpenWRT
- Kismet
- GPSD
- a bit of scripting

Problems

- Battery Power
- Hardware Failure
- Developing New Skills
 - Soldering
 - Electrical
- Hardware Limitations

Problems

- Driver Support
 - Broadcom driver support
- How do you assemble this into a working device?

Results

- Removed GPS
 - Parts arrived late
- Limited range of RC controller
- Detection works well
- Data recorded being saved for later analysis

Future Ideas

- Add GPS
- Control of vehicle from router
 - GPIO connectors on routers
- Better batteries
- Directional antenna
- Automatic notification of access points
- ????

Questions

- jason@sysadmins.info
- IRC on freenode.net in #pauldotcom
 - ask for Tadaka