Securing Your Wireless Network

Geof Goodrum
Washington Area Computer User Group

September 18, 2004

A Word from Our Sponsor ...

- Visit the Washington Area Computer User Group booth for more information
- Copies of slides and handout are on our web site
  - http://www.wacug.org/
- My Background
  - User Group member since 1985
  - 10 years experience as Unix/Linux System Admin
  - 5 years experience Network Admin
  - SANS Institute training: Security Essentials
  - 2 years running home wireless network
  - It's not paranoia – they are out to get us!

Overview

- Choosing wireless network equipment
- Why should I secure my network?
- How can I keep intruders out?
- How do I keep my data safe?
- What's coming
- Summary

Choosing Equipment

- Wi-Fi Alliance Certification
  - ensures interoperability
  - “enhanced” product modes not certified
- WPA or WPA2 support
- 802.11b or 802.11g?
- Wireless enabled routers vs. Access Points (APs)

Why Should I Secure My Network?

- Protect your data
- Block Spammers
- ISP Terms of Use Policy
  - unintentional community networks
- Other illegal activity

How Can I Keep Intruders Out?

- Change default passwords
- Update your network's firmware
  - Check for updates every few months
- Use Filters
  - Use Media Access Control (MAC) address filtering
  - Deny by default, Allow by exception
- Disable unneeded features
  - Simple Network Management Protocol (SNMP)
  - Demilitarized Zone (DMZ)
  - Service Set Identifier (SSID) broadcast
  - WAN ping

How Can I Keep Intruders Out?

- Carefully position Wireless Access Point
- Software firewall, antivirus/spyware scanners are still needed
- Use an external service to test your firewall
  - ShieldsUp! http://www.grc.com/
  - Issues with port 113 (AUTH/IDENT)

How Do I Keep My Data Safe?

- Use Data Encryption
  - Wired Equivalent Privacy (WEP)
    - Cracked - “unsafe at any key length”
    - Change key periodically
  - Wi-Fi Protected Access (WPA)
    - Current standard – fairly secure
    - Should be enabled by default since January
  - WPA2
    - Just adopted - uses Advanced Encryption Standard (AES)
  - End-to-End Secure Protocols
    - Virtual Private Network (VPN)
    - Secure Socket Layer (SSL)
- Never connect an AP to a hub
  - broadcasts to the world

What's Coming?

- WPA2 products about to hit the street
- WiMAX to make long-range broadband networks available starting in 2005
- Easier setup of Wi-Fi Certified products
- Wi-Fi Multimedia (WMM) certification and 802.11e Quality of Service standard
- 802.11n wireless standard for 108 Mbps
- Free/low-cost community networks?

Odds and Ends

- Send firewall logs to Dshield.org
- Subscribe to security mailing lists and newsfeeds
  - http://www.us-cert.gov/channels/
  - http://www.securityfocus.com/archive
- Slower wireless networks (< 20Mbps) are susceptible to denial of service (DOS) jamming

In Summary

- Update firmware
- Change passwords/keys
- Use WPA or WPA2
- Disable unneeded services
- Use a software firewall, spyware and antivirus scanner
- Monitor logs
- Confirm your network security
- Join your local User Group!