Wireless Security for Home Users

Cliff Skolnick, co-founder BAWUG

Overview

- Reasons to Secure a Home WLAN
- Security Policy Development
- Security Model Implementation
- Insecurity Demonstration
- Using Open Networks Safely

Reasons to Secure a Home WLAN

- A computer on a home network often stores personal information.
- An attacker on the local network has a higher chance of gaining access.
- Theft of services can be used for illegal activity
- An intruder can spy on your network.

Secure the Network and Secure the Host

- Create a policy
- Secure the network
- Secure the hosts

Create a Home Security Policy

- What will be on the network?
- What will be shared on the network?
- Who do you want to be able to access the network?
- Who will need access to what?

Home Security Models

- Network Based Security Model
  - Required: Encryption, Firewall, Host Virus Scanner
  - Optional: NAT, Network Virus Scanner, IDS
- Host Based Security Model
  - Required: Host Firewall, Host Virus Scanner

Picking a Model

- How many machines need to be secured?
- Do you need to share files or printers between machines?
- Will guests or neighbors need access?

Securing a Host

- Install anti-virus programs
- Use secure protocols
- Personal firewalls
- Shut down services

Securing the Network

- Required
  - Firewall
  - NAT
  - Encrypt wireless
- Optional for advanced users
  - Network virus filters
  - IDSs

Securing the WLAN

- To keep honest people honest
  - Closed (no SSID Broadcast)
  - MAC filtering
  - WEP
- Real security
  - WPA
  - VPN

Securing the WLAN

- WEP vs. WPA (PSK)
  - Shared Secret
  - Rotating Keys

Insecurity Demo

- What do you have to lose?

Using a Laptop on the Road

- Public access spots are hostile
- Protection is required
- Encryption is helpful
- Keep protection up to date

Hostile Environments

- Any open net! Even your own!
- Hotel networks
- Conferences
- Coffee shops
- Friend's networks

Preparing for Battle

- Anti-Virus program (up to date defs)
- Shut off unneeded services
- Personal firewall
- SECURE YOUR PASSWORDS!
  - E-mail, web, telnet, anything unencrypted

Securing Traffic

- VPN
- E-mail
  - Inbound e-mail
  - Outbound e-mail
- Secure surfing

Resources

- Misc Resources

  http://www.toaster.net/wireless/

- Rob Flickenger on ssh Tunnels

  http://www.oreillynet.com/pub/a/wireless/2001/02/23/wep.html

- Open AP Best Practices (in-progress)

  http://www.thirdbreak.org/best_practices/openap.html

Questions?

www.bawug.org

cliff@steam.com