Attacking 802.11 Networks

Joshua Wright
Joshua.Wright@jwu.edu

LightReading LIVE!
October 1, 2003

Attention

The material presented here reflects the personal experience and opinions of the author, and not of behalf of my employer.

Introduction

- Wireless LAN Attack Techniques
  - From the attacker's perspective
- How WLANs are compromised
- As many demonstrations as we can fit into 45 minutes
- Question and Answer

What an attacker is looking for

- Free Internet Access
- Unauthorized Information Disclosure
- Denial of Service targets
- Bypassing Perimeter Defense Systems
- Just to make administrators look stupid

Attacker – Free Internet Access

- Attacker is looking for access to the ‘net
  - Anonymity – they don’t want to get get caught
  - Could be benign – access to google.com, email access, chat
  - Could be against AUP – access to adult content, child pornography, launching attacks against other victim networks
- Minimum steps will thwart this attack
  - Lower-fruit is likely just around the corner

Attacker - Unauthorized Information Disclosure

- “What is interesting about THIS network?”
  - Workstation configuration
  - Network device configuration and software version information (CDP)
  - Business-critical data? Confidential customer records?
- Some information disclosure will lead to escalated privilege for an attacker
  - Especially common for IPSec WLAN security implementations

Attacker – Denial of Service

- Significant threat to all 802.11 networks
  - Often exploiting weaknesses in the 802.11 specification and flawed driver software
  - Deficiency is in client software and drivers
  - Ranges from mild inconvenience to sustained attack crippling client devices
  - No easy fixes
- Attackers are difficult to locate
  - Is the attack from common mischief, a disgruntled employee or corporate espionage?

Attacker – Bypassing Perimeter Defenses

- "Crunchy on the outside, soft and chewy on the inside" – Mentos Network Design
  - Common to many organizations with few security resources to manage client devices
  - Attacker uses stepping-stone attacks
- Wireless network operate without boundaries
  - Network perimeter is exposed throughout the enterprise
  - Where are you exposed?

Attacker – Just to make administrators look stupid

- Increasingly common “attack”
  - “Well-intentioned” people demonstrating flaws in production wireless networks
  - “I wanted to show how much information is at risk” or “… how easy it is to break-in”
- Results in bad publicity and further exposure for a business
  - The press makes the flaws in your network public information

How an attacker exploits a wireless network

- Reconnaissance/Information Gathering
- Network Probing
- Vulnerability Testing/Attacking
- Information Retrieval

Recon/Information Gathering

- WLAN Discovery Tools
  - – Tools report discovered wireless networks
  - – Use passive or active analysis to discover type of AP’s, type of clients and protocols in use
- Public Information Sources
  - – Results of WLAN discovery posted for public analysis
  - – http://www.wigle.net/
- Wardriving
  - – Traditionally performed from a car in the parking lot, street, etc.
  - – Can be done anonymously from your lobby, offices with handheld devices

Network Probing

- Discovering network SSIDs
  - – Cloaked SSIDs are NOT passwords!
  - – Implemented in the “essid_jack” tool
- Enumerating AP Information
  - – SNMP attacks, banner grabbing
  - – Probing AP’s with undocumented protocols
- Passive Analysis
  - – Determine what protocols are in use

Vulnerability Testing/Attacking

- How attackers exploit target systems
  - Exploiting IPSec-secured WLANs
  - Flaws in MAC-based authentication
  - Flaws in Cisco LEAP
  - Exploiting PEAP+WEP

Exploiting IPSec secured WLANs

- Common Security Configuration for protecting WLANs
  - Any traffic from WLAN must authenticate to VPN server before reaching internal network
- Attacking the IPSec Server
  - Exploiting flaws in IPSec implementation/IKE aggressive mode + pre-shared keys
  - Exploiting implementation bugs in VPN server software (IKE Crack, BUGTRAQ announcements)

Exploiting IPSec secured WLANs

- Layer 2 connectivity is often unrestricted
  - Permits any attacker to connect to other wireless clients
  - Attacker exploits vulnerable clients, connecting to corporate network through VPN
- Impact
  - An attacker is still unable to decrypt captured information since IPSec encryption is strong
  - Attacker can exploit vulnerable clients, and escalate privileges through existing connections

Flaws in MAC-based authentication

- Controlling access based on source MAC
  - Static lists on APs
  - Dynamic MAC access with captive web portals (hot-spot access)
- Authentication is solely based on MAC
  - Trivial to impersonate a valid user
  - All traffic on the network is from legitimate MACs

Flaws in MAC-based authentication

- Attack Scenario
  - Attacker identified a victim they want to impersonate
  - Connects to network with own MAC
  - Launches DoS against victim (BSoD)
  - Impersonates MAC+IP of victim
  - Gains unrestricted access
- Impact
  - Attacker can bypass security controls
  - Unrestricted access to internal hosts

Flaws in Cisco LEAP

- Weak authentication process
  - Username is sent in clear-text
  - Leaks information about user password
- Attacker can force user to reauthenticate
  - No waiting for victim to authenticate to the network
  - One packet forces reauthentication
  - No visible sign of attack to victim

Flaws in Cisco LEAP

- Attacker utilizes dictionary attack
  - Collect authentication credentials, off-line attack against weak passwords
- Impact
  - Account username and password disclosure
  - Unauthorized network access
  - Potential for privilege escalation – shared usernames/passwords among multiple systems

Flaws in PEAP+WEP

- Protected EAP – Microsoft/RSA/Cisco IETF draft
  - Uses TLS tunnel for encryption of weak authentication (MS-CHAPv2)
  - TLS provides mutual authentication
    - Protects against MitM, rogue APs
- Most implementations still use WEP
  - Flaws too numerous to enumerate
  - Latest attacks permit network access even with dynamic WEP keying (WEP Wedgie)
- TLS tunnel relies on trust of CAs
  - Most implementations include a standard list of CAs
  - Administrators add local CAs to avoid paying Verisign for digital certificates

PEAP Attack Scenario

- Attacker sets up Win2K CA Server on the Internet
- Attacker spams an organization
  - Uses a harvested list of addresses from google.com
  - HTML-formatted email exploits IE vulnerability to add their CA to each client
- Attacker launches MitM attack against a victim workstation
- Victim attempts to authenticate AP and establish a TLS tunnel
  - Checks list of CAs, attacker uses valid certificate from rogue CA server

Flaws in PEAP+WEP

- Impact
  - Attacker can establish MitM position
    - Lots of opportunity for attack
  - Password harvesting
    - Attacker impersonates valid internal resources
    - Collects passwords from “rogue” applications
  - Attack Escalation
    - DNS poisoning, session-piggybacking, SQL injection, etc.

What to do?

- Deploy WLANs with caution
  - Use careful site-surveys
  - Make use of planning tools to identify coverage areas
- Deploy WPA-I
  - Work with vendors on a clear upgrade path to AES
- Use WLAN IDS Systems

  Train intrusion analysts on WLAN analysis
  - The best tools will not help an untrained person recognize and assess threats
  - SANS, e-fense, Foundstone training

Summary

- A determined attacker has a lot of opportunity to attack 802.11 networks
- Mitigating threats will improve defensive posture
- Deploy a defense-in-depth position
- Monitor networks with automated and manual assessment
- Design incident response plans
  - What is the impact to your organization?

Questions?

Thank You!

Joshua Wright

Joshua.Wright@jwu.edu