# Wireless Security Tools

Shambhu Upadhyaya
Wireless Network Security
CSE 566 (Lecture 7)



## Popular Attack Tools

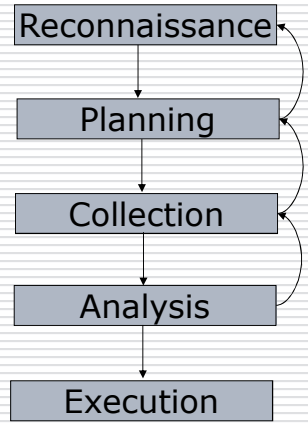
- Tools
  - NetStumbler
  - Kismet
  - Airsnort
  - Airjack
- These tools may not work against WPA or RSN
- Purpose is to "know the enemy"

# Attacker Goals

- One of the main issues to understand is the goal of the attacker
  - Snooping for gaining information
  - Disruption of service (DoS)
  - Network traffic modification
  - Masquerading
- Some may do availability attack (DoS)
- Some may do confidentiality attack (identity theft)



# Attack Process



# Reconnaissance

- Finding the victim
  - Actively searching till an easy target is identified
    - Looking at publicly available databases or maps of access points
  - Targeted attack
    - Finding a specific target requires tools such as war driving
- Tools
  - NetStumbler
  - Kismet



# Simpler Reconnaissance

- Hand held devices with notifications to connect to wireless Internet
  - iPhone, BlackBerry
- "**Security expert converts popular music/movie player and browsing device into a penetration testing, hacking tool**"
  - http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=219100135
- Can be used for ARP spoofing, Sniffing (using popular tools like NMAP)

## NetStumbler

- One of the most popular war driving software
- Works only under MS Windows
- Intuitive UI
- Easy to install and operate
- Ability to connect with several types of GPS receivers
- Also available as MiniStumbler, which can run on Pocket PCs



## NetStumbler

- It displays most of the needed info. in one screen broken into two panes
- Left pane provides shortcuts for displaying the networks
- Right pane displays all the networks
- See Figure 16.2 of Edney's book

## Kismet

- Passive tool for war driving
- Runs under Linux and OpenBSD
- Includes all the functionality of NetStumbler along with basic traffic analysis functionality
- Can display strings of characters it sees in the traffic on unprotected networks
- Good for finding passwords, etc.



## Kismet

- Saves the info it collects in series of text files
- These files contains list of all information about a network, raw packet dumps, and captured WEP traffic
- Use may violate *State and/or federal laws* by intercepting communications

# Kismet

- The main window of Kismet is shown in Figure 16.4 of Edney and Arbaugh



# Planning

- For a Open Network
  - Using Kismet one can capture the network traffic which can be analyzed using tools like Wireshark (http://www.wireshark.org/)
  - Using such tools one can determine the MAC addresses of valid clients
- For Protected Networks
  - First WEP keys have to be cracked
    - Dwepdump
    - Dwepcrack

## Collection

- It is simple to collect enough packets using dwepdump to recover a WEP key
- The most difficult part is determining the size of the key (40 bits or 104 bits)
- Good to start with the assumption of 40 bits



## Collection

- Collect enough packets using Dwepdump
- Purpose is to recover a WEP key
- Dwepdump must run until you collect at least 60 weak IVs

# Analysis

- After collecting enough information one can analyze it using tools like dwepcrack
- Sometimes you may have to go back and collect more packets (because the approach is probabilistic)
- Each weak IV for the first key byte provides a hint as to the first key byte with a 5% probability
- Having around 80 weak IVs guarantees success



# Other Tools of Interest

- Airsnort
  - Offers additional features like parallel cracking
  - Works constantly in the background to crack WEP keys
  - Allows capture over multiple networks
- Airjack
  - Provides features like carrying out DoS, determining ESSID for closed networks, establishing man in the middle attacks, setting MAC addresses of wireless cards, etc.

# Other Kinds of Attack

- Solar Winds
  - Has proprietary tools for all kinds of attacks
    - SNMP Password Cracker
      - SNMP: Simple Net Management Protocol
      - Used in network management systems to monitor network-attached devices
      - A brute force attack on this basically gives control to the attacker on all the network-attached devices

University at Buffalo The State University of New York

# Contd…

    - Router Password Attack
      - This wireless Tool lets you change the password of the router and then configure it to your liking
    - TCP connection reset program
      - Resetting TCP connections by setting the RST flag
- **DDOS**
  - Various tools on the internet to allow
    - Smurf attack – issue a large no. of ICMP requests from victim's spoofed IP, then get flooded with replies
    - Ping of Death – sending large (> 65,535 bytes) malformed ping request from victim's spoofed IP (also called long ICMP)
    - Syn Flood – send large no. of connection requests but do not reply to the syn-ack, resulting in half-open connections

University at Buffalo The State University of New York

# Popular Attacks

- Man-in-the-middle attack
- ARP Spoofing
  - Used to learn MAC address for a given IP address
  - ARP packets have no integrity protection, so, anyone can respond with incorrect information
  - This poisons the ARP cache of the requestor
  - Until the cache entry times out, the client uses an improper MAC address for the given IP address
- DOS attacks
- WPA Cryptographic DOS attacks
  - Because Michael provides only 20 bit protection against message modification attacks



# References


- Jon Edney and William Arbaugh, Real 802.11 Security, Addison-Wesley, 2004
- Maximum Wireless Security
  By Cyrus Peikari, Seth Fogie, Sams Publishing, 2003
- http://sectools.org/crackers.html
- http://www.solarwinds.com/