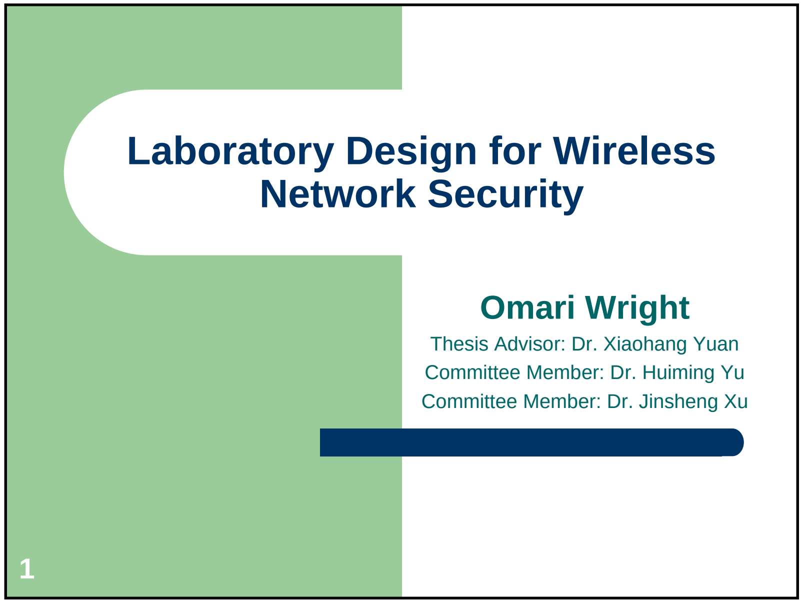
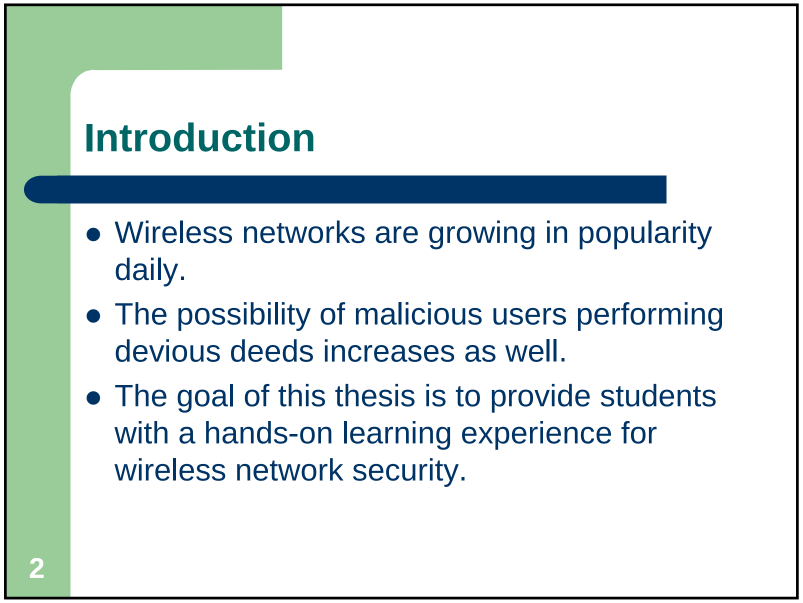


Laboratory Design for Wireless Network Security

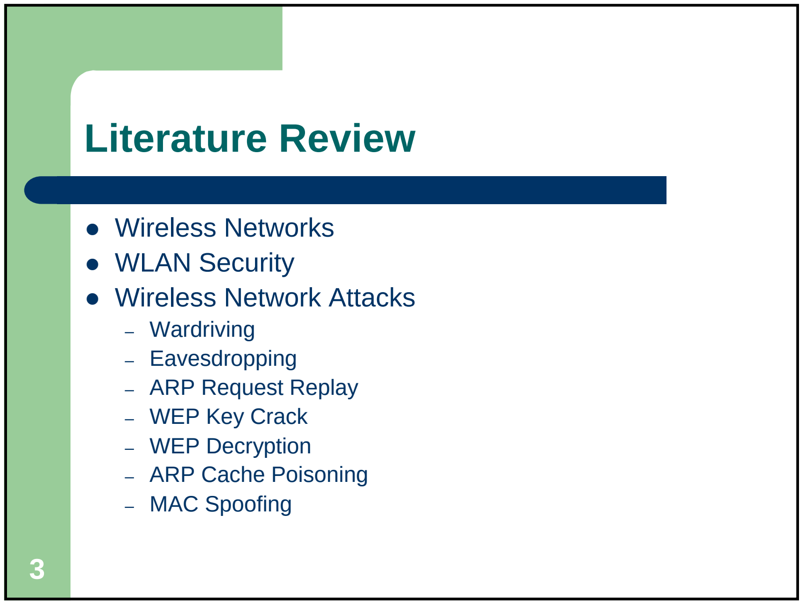
Omari Wright

Thesis Advisor: Dr. Xiaohang Yuan
Committee Member: Dr. Huiming Yu
Committee Member: Dr. Jinsheng Xu



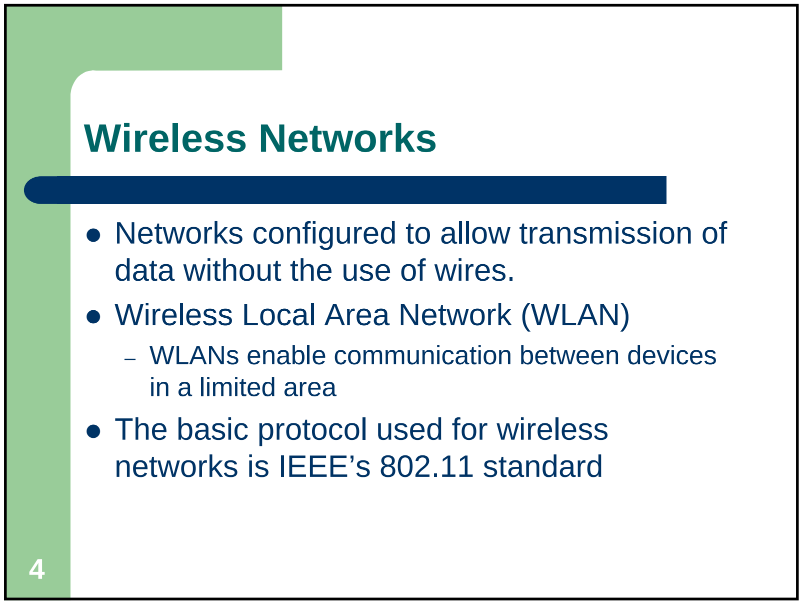
Introduction

- Wireless networks are growing in popularity daily.
- The possibility of malicious users performing devious deeds increases as well.
- The goal of this thesis is to provide students with a hands-on learning experience for wireless network security.



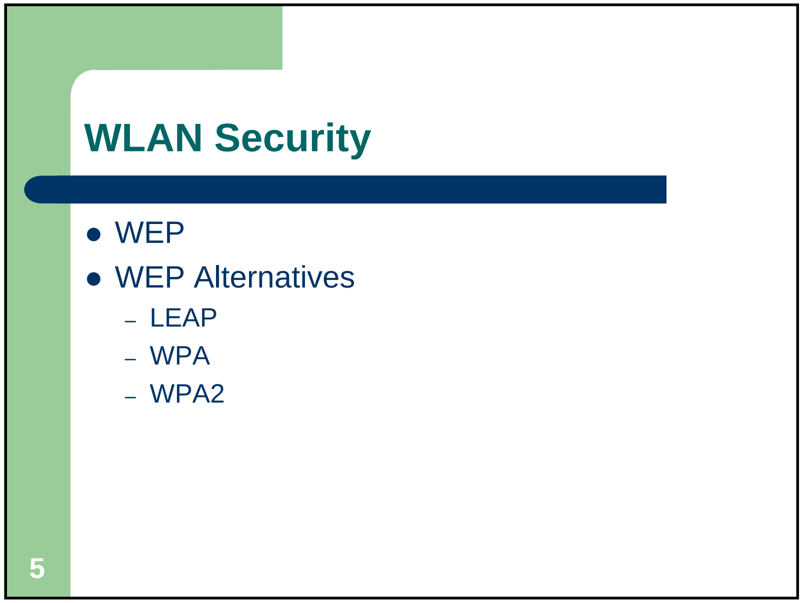
Literature Review

- Wireless Networks
- WLAN Security
- Wireless Network Attacks
  - Wardriving
  - Eavesdropping
  - ARP Request Replay
  - WEP Key Crack
  - WEP Decryption
  - ARP Cache Poisoning
  - MAC Spoofing



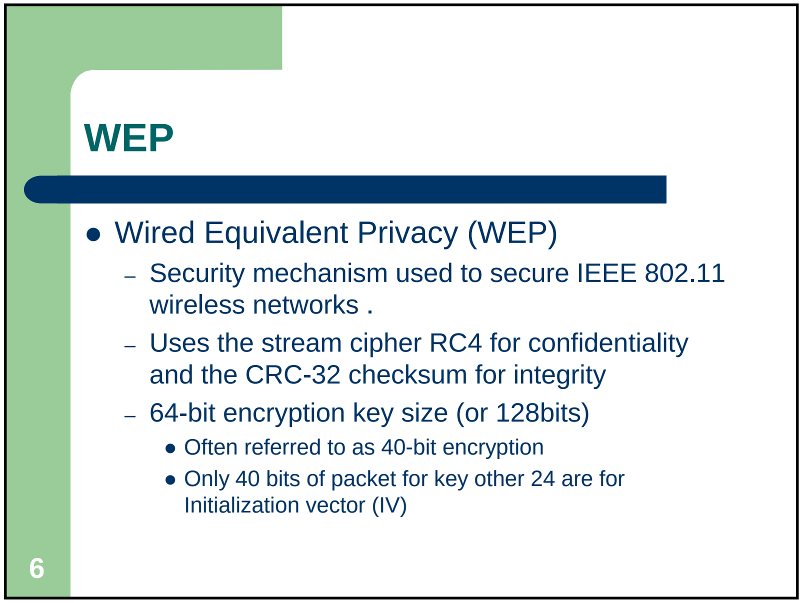
Wireless Networks

- Networks configured to allow transmission of data without the use of wires.
- Wireless Local Area Network (WLAN)
  - WLANs enable communication between devices in a limited area
- The basic protocol used for wireless networks is IEEE’s 802.11 standard



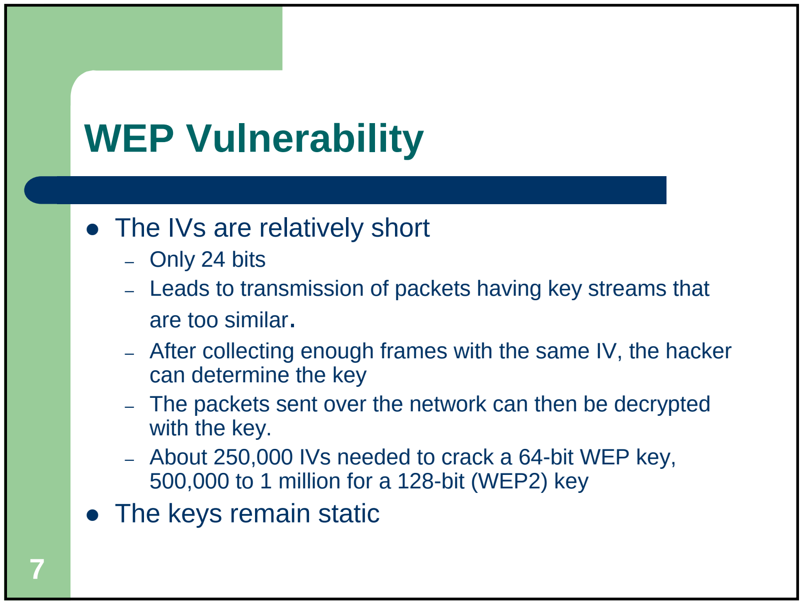
WLAN Security

- WEP
- WEP Alternatives
  - LEAP
  - WPA
  - WPA2



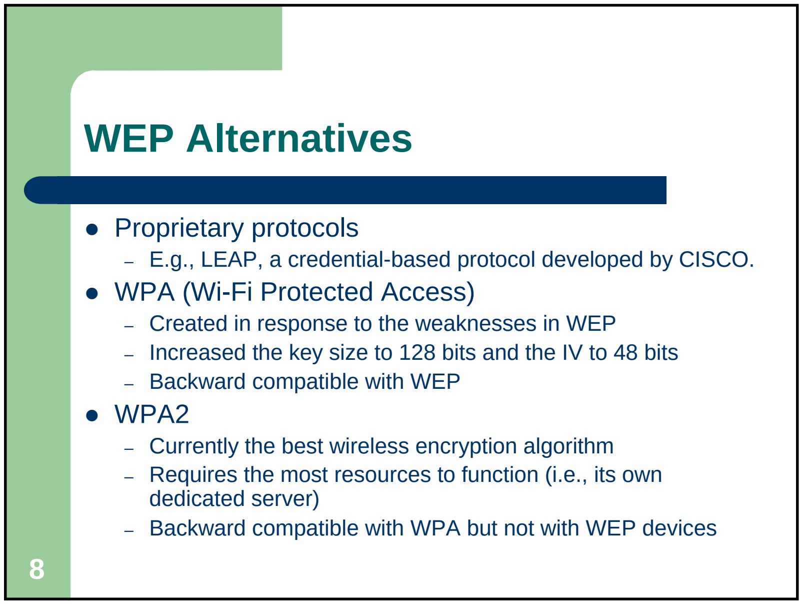
WEP

- Wired Equivalent Privacy (WEP)
  - Security mechanism used to secure IEEE 802.11 wireless networks .
  - Uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity
  - 64-bit encryption key size (or 128bits)
    - Often referred to as 40-bit encryption
    - Only 40 bits of packet for key other 24 are for Initialization vector (IV)



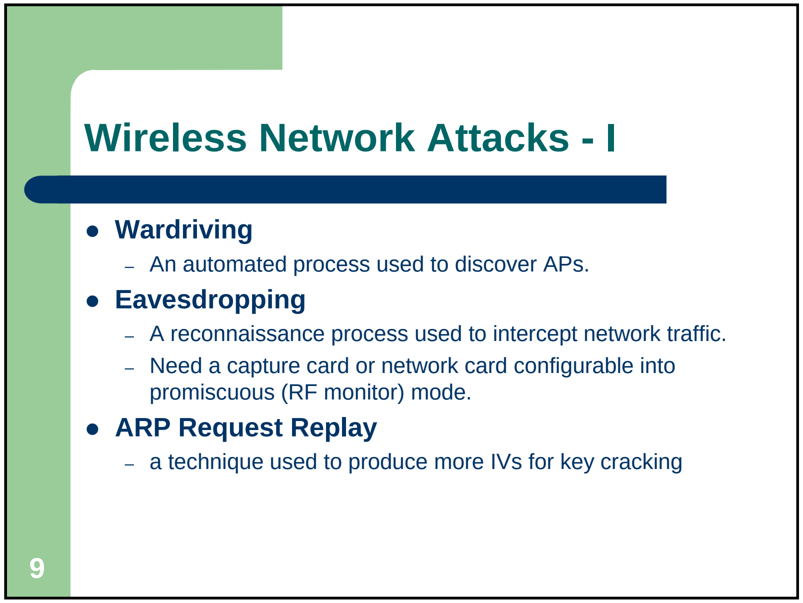
WEP Vulnerability

- The IVs are relatively short
  - Only 24 bits
  - Leads to transmission of packets having key streams that are too similar.
  - After collecting enough frames with the same IV, the hacker can determine the key
  - The packets sent over the network can then be decrypted with the key.
  - About 250,000 IVs needed to crack a 64-bit WEP key, 500,000 to 1 million for a 128-bit (WEP2) key
- The keys remain static



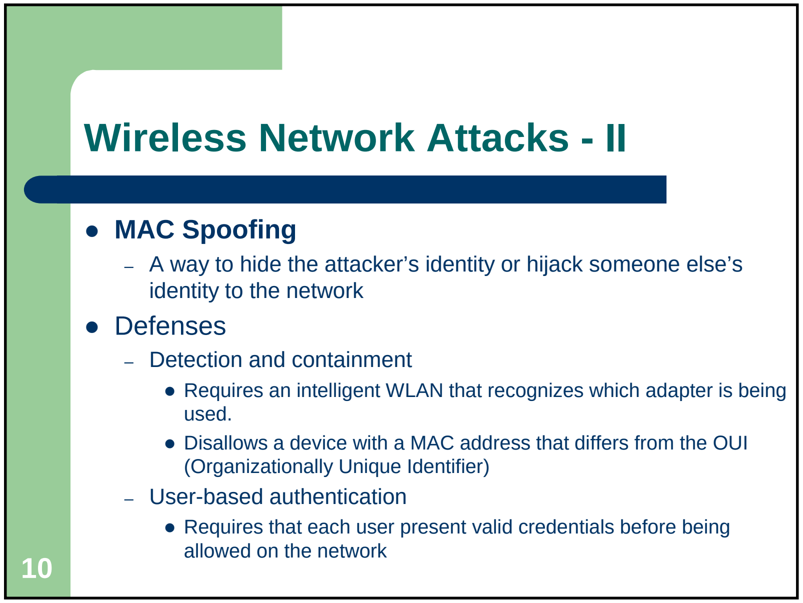
WEP Alternatives

- Proprietary protocols
  - E.g., LEAP, a credential-based protocol developed by CISCO.
- WPA (Wi-Fi Protected Access)
  - Created in response to the weaknesses in WEP
  - Increased the key size to 128 bits and the IV to 48 bits
  - Backward compatible with WEP
- WPA2
  - Currently the best wireless encryption algorithm
  - Requires the most resources to function (i.e., its own dedicated server)
  - Backward compatible with WPA but not with WEP devices



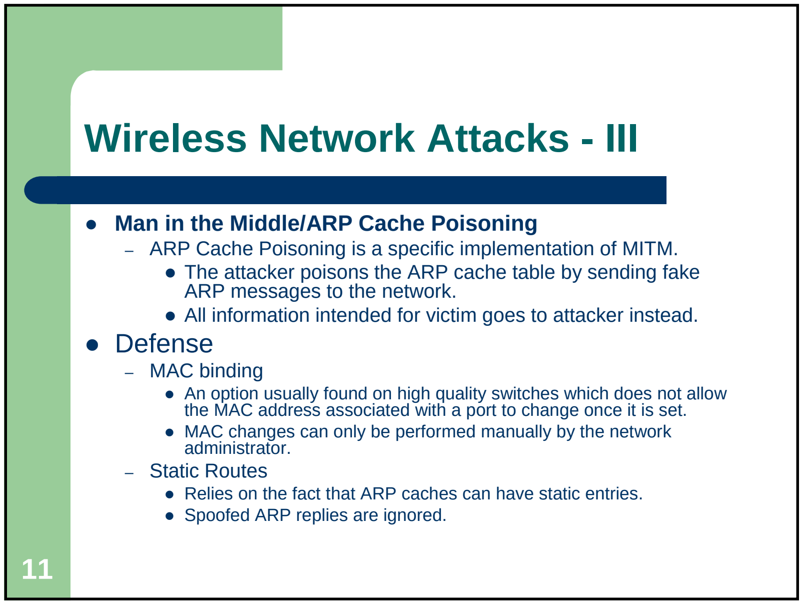
Wireless Network Attacks - I

- **Wardriving**
  - An automated process used to discover APs.
- **Eavesdropping**
  - A reconnaissance process used to intercept network traffic.
  - Need a capture card or network card configurable into promiscuous (RF monitor) mode.
- **ARP Request Replay**
  - a technique used to produce more IVs for key cracking



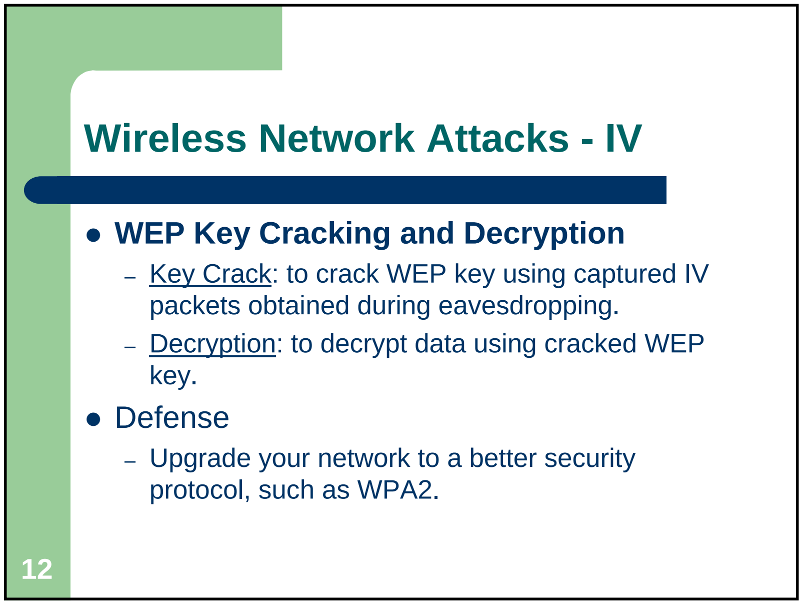
Wireless Network Attacks - II

- **MAC Spoofing**
  - A way to hide the attacker’s identity or hijack someone else’s identity to the network
- Defenses
  - Detection and containment
    - Requires an intelligent WLAN that recognizes which adapter is being used.
    - Disallows a device with a MAC address that differs from the OUI (Organizationally Unique Identifier)
  - User-based authentication
    - Requires that each user present valid credentials before being allowed on the network



Wireless Network Attacks - III

- **Man in the Middle/ARP Cache Poisoning**
  - ARP Cache Poisoning is a specific implementation of MITM.
    - The attacker poisons the ARP cache table by sending fake ARP messages to the network.
    - All information intended for victim goes to attacker instead.
- Defense
  - MAC binding
    - An option usually found on high quality switches which does not allow the MAC address associated with a port to change once it is set.
    - MAC changes can only be performed manually by the network administrator.
  - Static Routes
    - Relies on the fact that ARP caches can have static entries.
    - Spoofed ARP replies are ignored.



Wireless Network Attacks - IV

- **WEP Key Cracking and Decryption**
  - Key Crack: to crack WEP key using captured IV packets obtained during eavesdropping.
  - Decryption: to decrypt data using cracked WEP key.
- Defense
  - Upgrade your network to a better security protocol, such as WPA2.