Jordan Bayles
John Zeller
May 5, 2014

Outline
ECE 478: Network Security

1 1-page outline of project writeup

- Motivation - WEP was introduced in 1999 to provide confidentiality for WiFi similar to wired networks
- WEP Protocol breakdown
  - Infographic diagram showing WEP protocol makeup–to be created by us–and how it fits in the wireless stack
  - WEP-40
  - WEP-104
  - WEP-232
- WEP weaknesses
  - Repeat IVs after a small amount of packets
  - Single shared key among users
- Our implemented attacks
  - RC4 stream cipher attack to recover key
    - Sample file of saved packets
    - Overview of aircrack-ng script package - commands and what they do
    - Results of the attack - recovered key and analysis of the amount of effort required
  - 802.11 protocol attack
    - theoretical basis for the protocol attack
    - Graphic showing the elements of 802.11 that are exploited
- Remedies for WEP issues
  - Upgrade - 802.11i (WPA or WPA2)
  - Wepplus - private commercial solution
  - DynamicWEP - changes keys dynamically
- Conclusion

2 1-page outline of presentation

- Introduction
  - IEEE 802.11 Standard for WEP
  - WPA supercedes WEP
  - WEP-40 and WEP-104 deprecated with 802.11i standard (ie WPA2)
- WEP Protocol breakdown (unchanged from writeup)
- WEP weaknesses (unchanged from writeup)
- Our implemented attacks - will be expanded upon from writeup to include more practical, hands on approach to cracking WEP. Its a trivial protocol to crack so will be a easy way to include the audience
  - RC4 stream cipher attack to recover key
    - LIVE DEMO of stream cipher attack,using a basic Linksys router in class. WEP-40 is easy enough to crack it should be easy to include it in our presentation. This crack will be done the same way as in the writeup, and depending on the expected time we will either dedicate a portion of our presentation to cracking it, or have it cracked in the background (collecting and analyze packets)
  - 802.11 protocol attack
    - LIVE DEMO of protocol attack if possible, otherwise screenshots of relevant portions of the cracking process as well as taking a look at related file/code snippets will be included in the presentation
- Remedies for WEP issues (unchanged from writeup)
- Conclusion