CS 525M – Mobile and Ubiquitous Computing Seminar

Bradley Momberger
Randy Chong
• References used in this presentation:
  – Moskowitz: Weakness in Passphrase Choice in WPA Interface
    • http://wifinetnews.com/archives/002452.html
  – Edney & Arbaugh: *Real 802.11 Security: Wi-Fi Protected Access and 802.11i. ©2003 Addison-Wesley*
  – Jouni Malinen: Host AP driver for Intersil Prism2/2.5/3
  – RSA Laboratories: PKCS #5 v2.0: Password-Based Cryptography Standard
    • http://www.rsasecurity.com/rsalabs/pkcs/pkcs-5/
• **PTcracK**
  – There’s a Network Born Every Minute
  – Hybrid Passphrase Attack
  – Converts the Results of Passphrase Search to WPA Keys
  – Check Results of Generated Keys Against Intercepted Handshake Packets
• PMK = Pairwise Master Key
  – The shared secret between the client and the server
  – Can be generated from a passphrase
• The MAC addresses of each end of the connection and fresh values or “nonces” have to be sent in the clear before encryption keys can be generated.
• Any rogue node can monitor the traffic and learn all of the session information except the PMK.
• If the PMK is based on a passphrase, a rogue node may be able to guess the passphrase by matching the encryption keys to what is in use.
• Barring other security measures, the attacker can then gain access to the network.
• The most time-efficient way to guess a passphrase or other passphrase is through hybridized guessing.
Guesser

- Programmed from scratch
- Packaged in a general-purpose class
- Guess parameters specified at class instantiation
  - Minimum guess length
  - Maximum guess length
  - Maximum brute string length
- Three modes
  - Depth-First (default)
  - Breadth-First
  - Pure-Brute (fallback)
• Show Demo
Implementation

1) Retrieve the ssid from the access point
2) Compute the ssid length
3) Send a DISASSOCIATE command to the access point
4) Retrieve the PTK and the MAC addresses from the handshake packets
5) Use a hybrid algorithm to guess a pass phrase.
6) Generate the PMK with the guess
7) Generate a guessed PTK with the PMK
8) Check for a match between the PTK and the guessed PTK
   – Repeat steps 5 through 8 until a match is found

• We have implemented steps 5 through 8
• Hosted on Source Forge
  – Site contains source code release, documentation, and task list.
  – Program is released under GPL by force; contains other code acquired through the GPL.