CIS 700/002 : Special Topics : Wireless Tools Aircrack-ng, Reaver, Fern, etc.

Dagaen Golomb
CIS 700/002: Security of EMBS/CPS/IoT
Department of Computer and Information Science
School of Engineering and Applied Science
University of Pennsylvania

3 March 2017

In Other Words…

How to get free Internet from your neighbors!

Actually, this is the official disclaimer that this is for “research and personal use only”

Agenda

- WEP Cracking
  - Including SSID Uncloaking
- WPS PIN Attack
  - Will see current mitigations
- Deauth Attack to Influence Victim Behavior
- Pixie Dust Attack

WEP Cracking

- We went over the history and ideas behind these attacks – time to see it in action!
  - No need to reiterate details here
- Tools Covered
  - airmon-ng
  - airodump-ng
  - aireplay-ng
  - aircrack-ng

WPS Attack

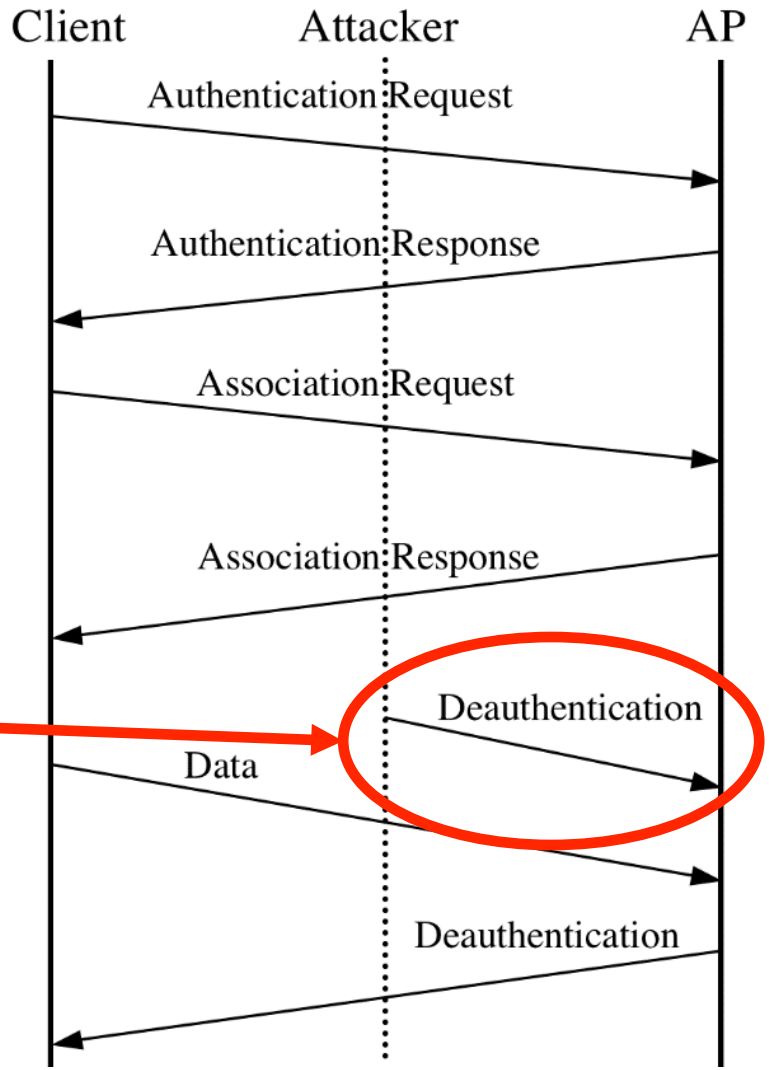

Serial No.:
01C10C11100003
MAC Address:
C0C1C0500D55
0484-0954
This symbol denotes the WPS feature.
8-Digit WPS PIN.

WPS Attack

- Exploit with the WPS PIN setup method
- Tools Covered
  - Reaver
- 8 digit pin is actually 4 + 3 + 1 (Checksum) = 10^4 + 10^3 = 11,000 combinations. At a few seconds per pin, this is feasibly brute-forcible.
- However, countermeasures have been enacted for newer hardware

Deauthentication Attack

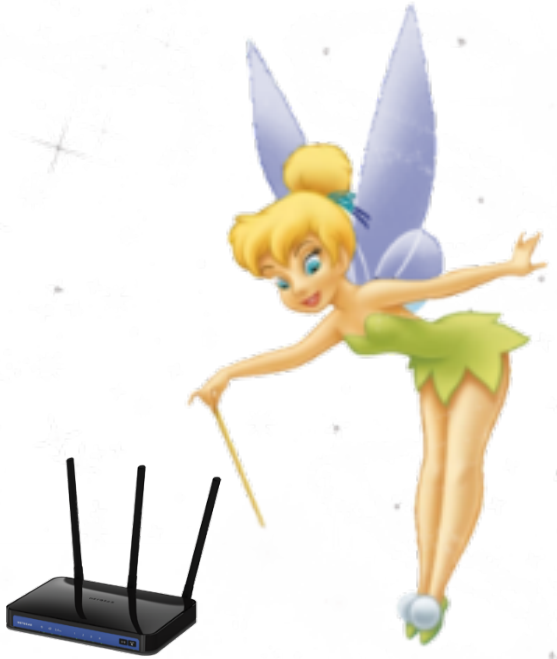
- Tools Covered
  - aireplay-ng (again)



Do this a lot!
Protocol does not require encryption for this packet

Pixie Dust Attack

- Tools Covered
  - Pixiewps was original tool
    - Will not cover
  - Reaver (again)
- Weakness in predictable or weak random number generation



Maintained list of known vulnerable hardware:
https://docs.google.com/spreadsheets/d/1tSlbqVQ59kGn8hgmwcPTHUECQ3o9YhXR91A_p7Nnj5Y/edit#gid=2048815923

Demo