Agenda

1. Introduction and Overview
2. Protocol Primer
3. Protocol Flaws
4. Existing Tools and Gap Analysis
5. Radiate
6. Theory into Practice: Radiate and Libnet
7. Closing Comments and Questions

Mike Schiffman

- Senior Consultant with @stake
  - The Premier provider of Digital Security Services
- Technical Advisory Board for Qualys, Inc.
- Consulting Editor for Wiley & Sons
- R&D background
  - Firewalk, Libnet, Libsf, Libradiate, Phrack Magazine
- Books:
  - Building Open Source Network Security Tools, Wiley & Sons
  - Hacker's Challenge I, Osborne McGraw-Hill
  - Hacker's Challenge II, Osborne McGraw-Hill

Overview

- What you will learn
  - Brief intro to the 802.11 protocol
  - Weaknesses in the 802.11 protocol
  - How to use libradiate to build custom 802.11 security tools
- What you should know
  - General understanding of the TCP/IP protocol suite
    - Primarily layers 2 - 3
  - General understanding of wireless
  - General network security concepts
  - The C programming language

Nomenclature

- Network Security Tool or Tool
  - A network security tool is an algorithmic implement that is designed to probe, assess, or increase the overall safety of or mitigate risk associated with an entity across a communications medium.
  - This is dry but it works
- Toolkit
  - An API, or set of APIs used to build Network Security Tools
  - A C programming library
  - “Component”

802.11 is Everywhere

- 802.11-based networks are wonderful inventions
  - Corporate America
  - Coffee shops, Hotels, Airports, “Residential ISPs”
- Many new products and services on top of 802.11
  - Newer, faster physical interfaces being turned out on top of the same layer 2 protocols
- However, there are a “few” security concerns…
  - We need a way to be able to test for security issues
  - Sure, some tools do exist
- But what we really need is a way to be able to test for arbitrary security issues with custom tools
  - We need a generic 802.11 toolkit

802.11 Primer

- Borne out of the IEEE 802 LMSC
- 802.11 WLAN standard
  - PHY layer: 802.11b 2.4Ghz up to 11Mbps
  - PHY layer: 802.11a 5Ghz up to 54Mbps
- Drop in replacement for Ethernet
  - Upper layer protocols should be none the wiser
  - This seamless integration comes at a stiff price – under the hood complexity

802.11 Primer: Physical Interface

- 802.11b is the most widely deployed
- Direct Sequence Spread Spectrum (DSSS)
  - 2.4GHz ISM Band
    - Industrial / Instrumentation, Scientific, Medical
    - 2.400GHz – 2.4835GHz
    - 14 channels or frequency divisions
      - 1 – 11 used in the United States
  - 1000mW power maximum
    - Most devices are 30mW – 100mW

802.11 Primer: MAC Sublayer Tidbits

- CSMA/CA
  - LBT (Listen Before Talk)
  - Exponential back off and retry
  - Collision avoidance via physical carrier sense and Network Allocation Vector (NAV)
    - Sent in most frames (duration ID)
    - Informs other stations how long the medium will be in-use
    - Virtual carrier sense (station waits until NAV is 0 before attempting to send)

Configuration Options

AD Hoc

Infrastructure

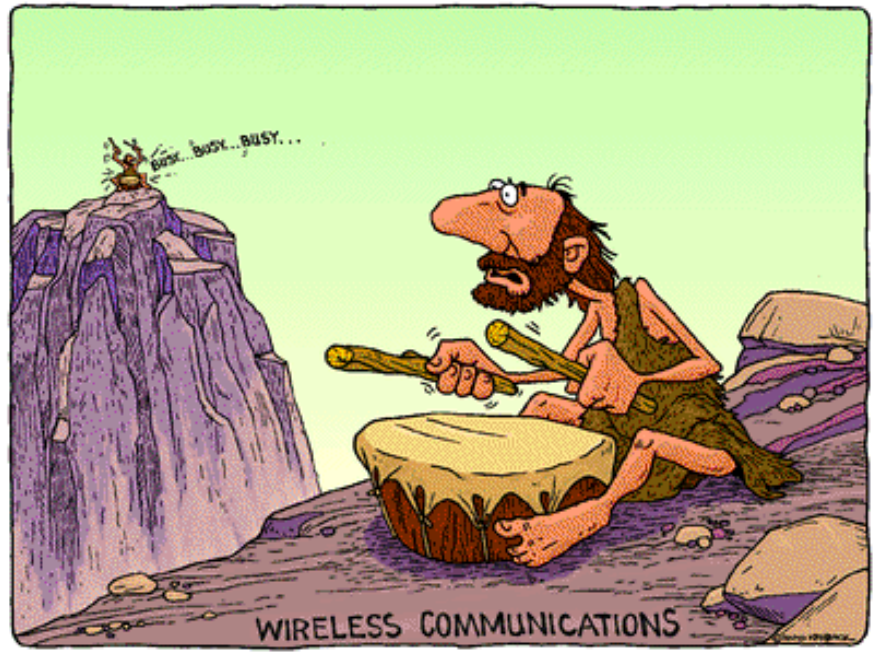
The Need for an 802.11 Wireless Toolkit

Invictus Ferramenta

Mike Schiffman

BlackHat Briefings July 2002

Version 2.0



@stake

Where Security & Business Intersect℠