Modern Network Infrastructure Security

Layer 2 Protocol Flaws Illustrated and Coded

May 2004

Mike Schiffman, Cisco Systems
Jeremy Rauch, Duncansoft Inc.

Agenda

- Introduction, overview, and what you'll learn
- Define Modern Network Infrastructure
- A brief introduction to libnet and libpcap
  - Needed to understand the tools
- Introduce our layer 2 protocols for the day
  - Ethernet, ARP, CDP, STP
  - Protocol laws, not implementation laws
- Code to examine these laws
- Closing comments and questions

Mike Schiffman

- Researcher for Cisco System 
  - Critical Infrastructure Assurance Group [CIAG]
- Technical Advisory Boards: Qualys, Sensory Networks, Vigilant, IMG Universal
- Consulting Editor for Wiley & Sons
- R&D, Consulting, Speaking background
  - Firewalk, Libipq, Libnet, Libsf, Libradiate, various whitepapers and reports
- Done time with: @stake, Guardent, Cambridge Technology Partners, ISS
- Current book:
  - Modern Network Infrastructure Security, Addison Wesley (2005)
- Previous books:
  - Building Open Source Network Security Tools, Wiley & Sons
  - Hacker's Challenge Book, Osborne McGraw-Hill
  - Hacker's Challenge Book, Osborne McGraw-Hill

Jeremy Rauch

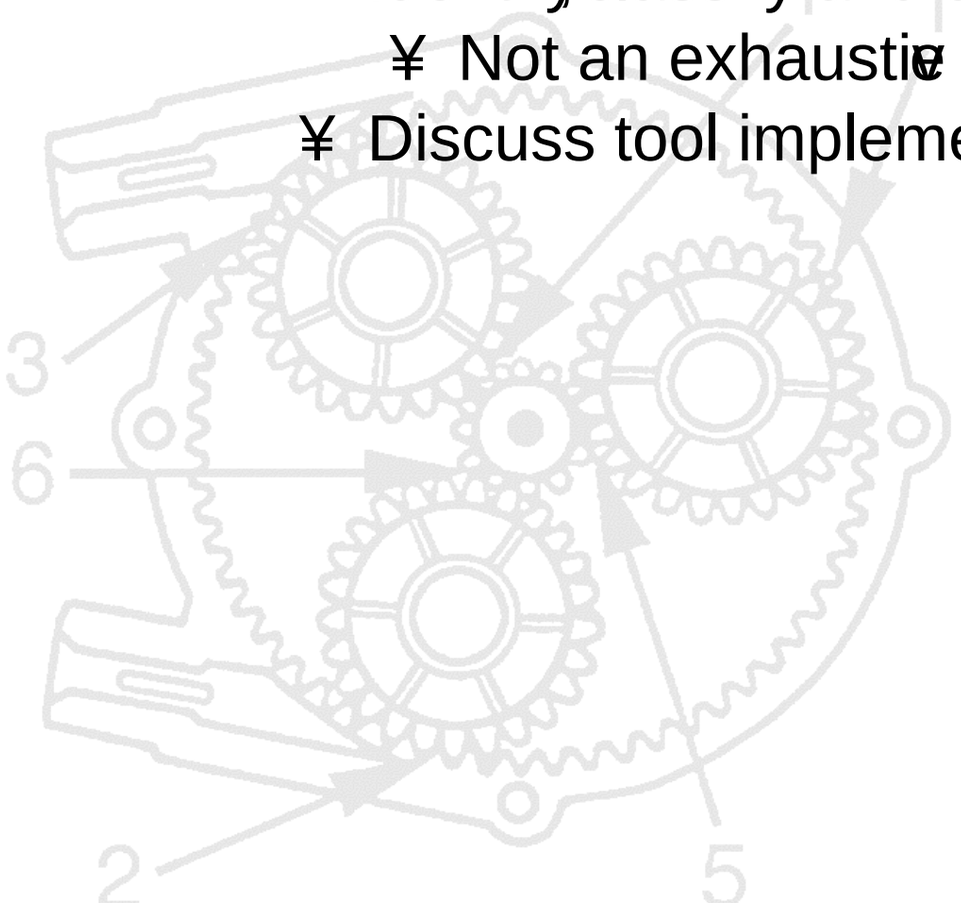
- CTO of Duncansoft, LLC
  - Startup developing security devices for 802.11 networks
- Past Development and Consulting background
  - Principle engineer of Tellium (now Zhone), designing + implementing optical switching products
  - Lead Engineer + Dev Manager for Network Associates Cybercop Unix IDS
  - One of the founders of SecurityFocus.com
    - Managed vulnerability + Unix content
    - Consulted for a variety of Fortune 500 clients, specializing in financial application vulnerability testing
    - Speaking + client training for a variety of conferences + clients for 7+ years
- Current book:
  - Modern Network Infrastructure Security, Addison Wesley (2005)
- Previous book:
  - Hack Proofing Your Network: Internet Tradecraft, First Edition, Syngress Press (2000)

Modern Network Infrastructure Security

- Modern networks are made up of a variety of devices
  - These devices rely on a set of "infrastructure protocols" to operate and get work done
    - Most obvious: TCP, UDP, IP
    - Pretty obvious: Ethernet, ARP, IPSec, PPTP
    - Not so obvious: routing protocols, QoS protocols, HA protocols
  - Many things going on in the network that are generally ignored when it comes to security
    - Perimeter issue is understood (firewalls)
    - Client security is understood (IDS and policy)
    - Infrastructure is largely ignored or misunderstood
- How can you evaluate and quantify risk when you don't know about a large portion of the things running on your network?

Methodology For Today

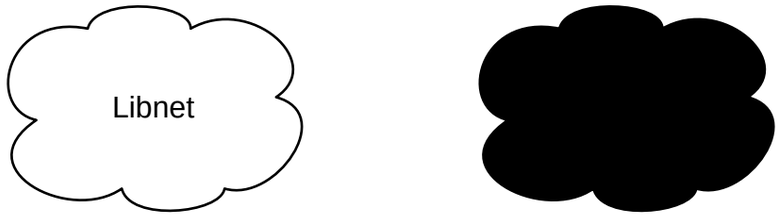
- Identify the protocols
- Outline general use pattern of the protocol
- Identify, classify and discuss a handful of protocol flaws
  - Not an exhaustive list
- Discuss tool implementation



C.I.A. Properties

- Protocol laws will be framed in terms of their impact on the C.I.A. properties of an information system
- C.I.A. properties measure a system's ability to handle the following:
- Confidentiality
  - Protection from unauthorized information disclosure
- Integrity
  - Protection from unauthorized modification
- Availability
  - Protection from downtime

A Brief Introduction to Libnet



- A C Programming library for packet construction and injection
- The Yin to the Yang of libpcap
- Libnet's Primary Role in Life:
  - A simple interface for packet construction and injection
- Libnet IS good for:
  - Tools requiring meticulous control over every field of every header of every packet
- Libnet IS not well suited for:
  - Building client-server programs where the operating system should be doing most of the work