

# The Completion Backwards Principle

## Bringing Layer 0 Issues To Layer 3

- geoffrey
- Defcon 0x0F

# Alarm Systems

- Fire
  - Actively detects a fire
  - Alerts inhabitants, and /or authorities
- Burglar
  - Detects intrusion into the facility premises
  - Alerts inhabitants, and /or authorities
  - Often co-exists with a Fire alarm system

# Anatomy of a Burglar Alarm

- Basic Topology
  - Panel
  - Sensors
    - Motion
    - Glass Break
    - Door Triggers
    - Smoke/Fire
  - Monitoring Method
    - What good is an unwatched alarm system?

# (D)Evolution of Monitoring

- Leased Lines
  - Dedicated & Expensive
- POTS Lines
  - Common in all buildings & Cheap
- Cellular/RF
  - Cheaper & Subject to outages
- Internet
  - Lowest cost
  - Subject to whims of your ISP/Script Kiddies

# Internet Monitoring Hardware

- DMP
  - ICOM/ICOM-E
- Honeywell
  - AlarmNet-i(7845i)



# DMP ICOM-E

- Choose udp or tcp
  - Default protocol is udp
- Port is Configurable
  - Default value is 2001
- AES is only available algorithm
  - 128 bit
- POTS Dialer if no Central Station contact

# Honeywell AlarmNet-i

- Only uses tcp
- Port 54109
- Choice of encryption algorithm
  - 256 bit AES (UL Certified)
  - Blowfish\* (Factory Default)
- POTS Dialer if no Central Station contact
- No open ports; ether identifies as Ademco

# IP Reporting Characteristics

- DMP
  - Uses port 2001
    - Port is configurable
  - Defaults to udp
  - Reports to CSC-1R
- AlarmNet-i
  - Uses port 54109
    - Port is not a configurable option
  - Only uses tcp for network traffic
  - Reports to AlarmNet 7810iR



# AlarmNet-i Traffic

- AlarmNet-i => 7810iR TCP [SYN] Seq=0 Len=0 MSS=1460
- 7810iR => AlarmNet-i TCP [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
- AlarmNet-i => 7810iR TCP [ACK] Seq=1 Ack=1 Win=5840 Len=0
- AlarmNet-i => 7810iR TCP [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=68
- 7810iR => AlarmNet-i TCP [PSH, ACK] Seq=1 Ack=69 Win=5772 Len=52
- AlarmNet-i => 7810iR TCP [RST, ACK] Seq=69 Ack=53 Win=5788 Len=0
- 
- AlarmNet-i => 7810iR TCP [SYN] Seq=0 Len=0 MSS=1460
- 7810iR => AlarmNet-i TCP [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1380
- AlarmNet-i => 7810iR TCP [ACK] Seq=1 Ack=1 Win=5840 len=0
- AlarmNet-i => 7810iR TCP [PSH, ACK] Seq=1 Ack=1 Win=5840 Len=68
- 7810iR => AlarmNet-i TCP [PSH, ACK] Seq=1 Ack=69 Win=5772 Len=68
- AlarmNet-i => 7810iR TCP [RST, ACK] Seq=69 Ack=69 Win=5772 Len=0

# ICOM-E Traffic

- ICOM-E => SCS-1R TCP [SYN] Seq=0 Len=0 MSS=1408
- SCS-1R => ICOM-E TCP [SYN, ACK] Seq=0 Ack=1 Win=299 Len=0 MSS=260
- ICOM-E => SCS-1R TCP [PSH, ACK] Seq=1 Ack=1 Win=2816 Len=51
- SCS-1R => ICOM-E TCP [ACK] Seq=1 Ack=52 Win=299 Len=0
- SCS-1R => ICOM-E TCP [PSH, ACK] Seq=1 Ack=52 win=299 Len=35
- ICOM-E => SCS-1R TCP [FIN, ACK] Seq=52 Ack=36 Win=2816 Len=0
- SCS-1R => ICOM-E TCP [ACK] Seq=36 Ack=53 Win=299 Len=0
- SCS-1R => ICOM-E TCP [FIN, ACK] Seq=36 Ack=53 Win=299 Len=0
- ICOM-E => SCS-1R TCP [ACK] Seq=53 Ack=37 Win=2815 Len=0
- 
- ICOM-E => SCS-1R TCP [SYN] Seq=0 Len=0 MSS=1408
- SCS-1R => ICOM-E TCP [SYN, ACK] Seq=0 Ack=1 Win=299 Len=0 MSS=260
- ICOM-E => SCS-1R TCP [PSH, ACK] Seq=1 Ack=1 Win=2816 Len=51
- SCS-1R=> ICOM-E TCP [ACK] Seq=1 Ack=52 Win=299 Len=0
- SCS-1R => ICOM-E TCP [PSH, ACK] Seq=1 Ack=52 Win=299 Len=19
- ICOM-E => SCS-1R TCP [ACK] Seq=52 Ack=20 Win=2816 Len=0
- ICOM-E => SCS-1R TCP [FIN, ACK] Seq=52 Ack=20 Win=2816 Len=0
- SCS-1R => ICOM-E TCP [ACK] Seq=20 Ack=53 Win=299 Len=0
- SCS-1R => ICOM-E TCP [FIN, ACK] Seq=20 Ack=53 Win=299 Len=0
- ICOM-E => SCS-1R TCP [ACK] Seq=53 Ack=21 Win=2815 Len=0

# Deployment Considerations

- Network traffic needs close monitoring
  - Worms may adversely affect alarm system
- Monitor System and Main Panel Config
  - Dialer lines may violate U.S. Govt. rules
    - DCID 6/9 Annex B
  - Defaults (DMP) allow config changes via LAN
    - Oversee install and config of panel/device(s)
  - LAN connectivity means access for users
    - Need segregation
      - Best to pull in separate ISP line & physically isolate

# Deployment Considerations

- Network QOS now important!!!
  - Chatty boxes retard system monitoring
  - Routing issues adversely affect monitoring
- Disaffected youth talk to your alarm
  - The Internet is an undesirable neighborhood
- Alarm system now network node
  - Flashlight luggers must befriend black t-shirts

# Disruption Scenarios

- No (apparent) attack surface
  - Speak IP
  - What happens if we flood the network?
    - Depends on your reporting window
  - What happens if we send repeated RSTs?
  - Can we poison arp?
    - Haven't had luck with this, as of yet
  - DNS poisoning doesn't seem to matter
    - Or does it?
    - Systems only use IPs

# One Solution

- Disclaimer
  - Not endorsed by U.S. Government
- Based upon
  - Common sense
  - My own experience
  - Purloined Install Guides

# My Solution

- Brought in separate DSL line
  - Different ISP from our Primary
  - DSL account is in individual's name
  - Basic Internet Service
- Bespoke embedded firewall
  - Soekris net4801
    - Moving to rack mountable Soekris net5501s
  - Linux System built from sources

# Why not COTS firewall

- Potentially less cost
- More control over configuration
  - Standardize platform/hardware across sites
- Unusual choices
  - Logger is syslog-ng
  - Include Logwatch and Logrotate
  - Include Ssmtp to move logs



# Firewall Issues

- How do we safely monitor logs?
  - logger over stunnel to central logserver
  - Logwatch & Cron use Ssmtp to email reports
- How often do we patch system?
  - Now controlled by staff
  - Patches only update code we want patched
    - No unwanted dependencies
- How to protect the firewall itself?
  - Customize ruleset as needed
  - Include Inline Snort functionality?

# Future

- Work with community members
  - Develop traffic signatures to identify devices
    - Hoping to identify MiTM attack possibilities
  - Testing effectiveness of encryption usage
    - Crypto is not my forte
    - System appears to use a timestamp for iv
  - Discuss possibility of IPSec usage
    - In the preliminary stages only
  - Releasing firewall codebase
    - All suggestions for improvement are welcome
    - <http://chickendance.deussexmachina.org/>

Questions?