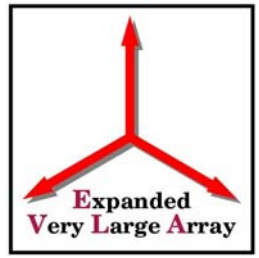
EVLA Monitor & Control Software PDR

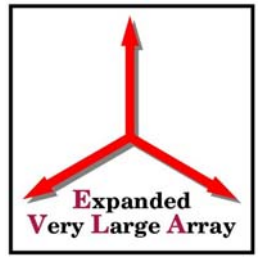
Monitor & Control Network Security

Requirements



- Accessibility
  - Operators
  - Engineers
  - Scientists
- Monitor vs. Control
  - Read vs. write
- Security
  - Acceptable risk

Access



- From M&C systems to antennas
- From VLA to antennas
- From AOC to antennas
- From NRAO to antennas
- From non-NRAO to antennas

Vulnerabilities

- M&C systems
- M&C/Antenna Network
- MIB
- Other ?

M&C systems (Linux, Solaris, Windows)

- Virus
- Root access
- Denial of Service
- M&C software itself

M&C and antenna network

- Network Devices
  - CISCO IOS NTP vulnerability
    - Announced May 8th
  - TCP/IP stack
- Network flooding

MIB vulnerabilities

- TCP/IP stack
- Telnet (authentication)
- HTTP server
- NTP
- Denial of service
  - Port flooding
- Human Error

Direct Access

- Firewall
  - Limit access based on
    - Source IP
    - Sender Digital Certificate
      - MIB awareness
  - Throttle flooding
  - Encryption precludes content filtering
- Can't guarantee packet integrity

Indirect Access

- Proxy service
  - Request proxy
  - Web Proxy
- Virtual antenna
  - Same client software
- Remote display
  - X11 or Citrix
    - slow