Securing Ground Control Systems

Computer Sciences Corporation

Mary Hunter / Tracy Dorsey
Securing Satellite Ground Control Systems

- Ensure real-time command and control functions performed by flight operators
- Reduce the cost of maintaining systems over the life of the mission
- Provide secure remote system access
- Enable un-manned spacecraft operations
Background

- Ground control systems traditionally are located on-site, and manned by flight operations team
- Technology advancements enabled ground control systems to function off-site and un-manned
- Security has become a major factor on all mission networks
- Lower mission cost without increasing risk
Network Foundation

Perimeter Network

Local Mission Network Closed

Administrative Network
Secure Perimeter Network

- Use access control list (ACL)
  - Let routers route – Firewall block traffic
- Filter inbound traffic and block unapproved traffic
- Use firewall rules on as-needed basis; review rules annually
Secure - Administrative Host

- Administrative systems require internet access, email, telnet and ftp services
- Systems reside on a less secure network, requires up to date patches, service packs, etc.
- Administrative system(s) set up to trust and receive data from the mission network but cannot initiate data transfers to the mission network
- Administrative systems to provide only non-critical mission services
- Limited number of users, no guest accounts, no anonymous ftp or telnet
- Select and use COTS security package to allow remote login and possibly allow user ability for request response
Secure - Mission Host

- Use standard “in-house locked down” system OS installation
  - Disable internet access, email, and telnet services
  - Disable unused ports
  - Allow outbound ftp only
  - Limited number of users, no guest accounts
  - Use COTS tools to enforce password rules
Secure - Mission Host (cont.)

- Automate system backups, perform backups on a frequent basis, and verify system backups
- Automate patch installation, provide reliable system depot
- Install and maintain virus protection software
- Use COTS tools where appropriate (IP filter, TCP wrappers, WU-FTP, ...)

Secure - Mission Application

- Use automated system to enable un-manned satellite operations
  - Monitor
    - Provide secure system monitoring
  - Alert
    - Operators and system administrators need system failure notification
  - Response
    - Privileged system operators and administrators can securely and remotely take action
System Monitoring

- Determine system thresholds that require monitoring for example:
  - Data acquisition, instrument parameters, data distribution, status of scheduled system activities, and system usage
- Configure system monitoring for notification levels and distribution of logs, displays, etc.
- Use scripts to format, store and distribute monitor data
Alert System

- Use paging or e-mail system to send notification to system administrators and/or operators
  - Determine method for indicating severity
  - Trigger the distribution of system data (logs, display pages)
  - Possibly trigger response system to take action
- Allows operators/administrators an increased knowledge of system state without having to be on-site
- Optional – Tune alert system
System Response

- **Manual Response**
  - After alert, log in and evaluate logs
  - Drive to facility if required

- **Automatic Response**
  - System begins fail-over procedure
  - System kicks off backup, purge, etc.

- **User Invoked Response**
  - Allow system administrators to invoke backups
  - Allow flight operators limited command capabilities
  - Allow for requests of system data
How it works

1. Monitoring System (data acquisition, system usage..)
   FTP's logs, events, data anomaly

2. Alert System detects anomalies and sends e-mail or numeric page to notify system administrator or operator depending on severity

3. Through perimeter network admin or operator views system logs
   Remote Administrator
   Secure login
   System response
   Perimeter Network
   Internet
   Mission Hosts
   Firewall
   E-mail, numeric page

4. Response system polls administrative system and retrieves response
   Response system initiates response
   Remote Operator
   Admin or operator formats response and stores on administrative system
   Severity indicator, logs, displays
   Administrative Host
   Closed Net
   Open Net

1. Monitoring System (data acquisition, system usage..)
   FTP's logs, events, data anomaly

2. Alert System detects anomaly sends e-mail or numeric page to notify system administrator or operator depending on severity

3. Through perimeter network admin or operator views system logs
   Remote Administrator
   Secure login
   System response
   Perimeter Network
   Internet
   Mission Hosts
   Firewall
   E-mail, numeric page

4. Response system polls administrative system and retrieves response
   Response system initiates response
   Remote Operator
   Admin or operator formats response and stores on administrative system
   Severity indicator, logs, displays
   Administrative Host
   Closed Net
   Open Net

1. Monitoring System (data acquisition, system usage..)
   FTP's logs, events, data anomaly

2. Alert System detects anomaly sends e-mail or numeric page to notify system administrator or operator depending on severity

3. Through perimeter network admin or operator views system logs
   Remote Administrator
   Secure login
   System response
   Perimeter Network
   Internet
   Mission Hosts
   Firewall
   E-mail, numeric page

4. Response system polls administrative system and retrieves response
   Response system initiates response
   Remote Operator
   Admin or operator formats response and stores on administrative system
   Severity indicator, logs, displays
   Administrative Host
   Closed Net
   Open Net

1. Monitoring System (data acquisition, system usage..)
   FTP's logs, events, data anomaly

2. Alert System detects anomaly sends e-mail or numeric page to notify system administrator or operator depending on severity

3. Through perimeter network admin or operator views system logs
   Remote Administrator
   Secure login
   System response
   Perimeter Network
   Internet
   Mission Hosts
   Firewall
   E-mail, numeric page

4. Response system polls administrative system and retrieves response
   Response system initiates response
   Remote Operator
   Admin or operator formats response and stores on administrative system
   Severity indicator, logs, displays
   Administrative Host
   Closed Net
   Open Net

1. Monitoring System (data acquisition, system usage..)
   FTP's logs, events, data anomaly

2. Alert System detects anomaly sends e-mail or numeric page to notify system administrator or operator depending on severity

3. Through perimeter network admin or operator views system logs
   Remote Administrator
   Secure login
   System response
   Perimeter Network
   Internet
   Mission Hosts
   Firewall
   E-mail, numeric page

4. Response system polls administrative system and retrieves response
   Response system initiates response
   Remote Operator
   Admin or operator formats response and stores on administrative system
   Severity indicator, logs, displays
   Administrative Host
   Closed Net
   Open Net

1. Monitoring System (data acquisition, system usage..)
   FTP's logs, events, data anomaly

2. Alert System detects anomaly sends e-mail or numeric page to notify system administrator or operator depending on severity

3. Through perimeter network admin or operator views system logs
   Remote Administrator
   Secure login
   System response
   Perimeter Network
   Internet
   Mission Hosts
   Firewall
   E-mail, numeric page

4. Response system polls administrative system and retrieves response
   Response system initiates response
   Remote Operator
   Admin or operator formats response and stores on administrative system
   Severity indicator, logs, displays
   Administrative Host
   Closed Net
   Open Net

1. Monitoring System (data acquisition, system usage..)
   FTP's logs, events, data anomaly

2. Alert System detects anomaly sends e-mail or numeric page to notify system administrator or operator depending on severity

3. Through perimeter network admin or operator views system logs
   Remote Administrator
   Secure login
   System response
   Perimeter Network
   Internet
   Mission Hosts
   Firewall
   E-mail, numeric page

4. Response system polls administrative system and retrieves response
   Response system initiates response
   Remote Operator
   Admin or operator formats response and stores on administrative system
   Severity indicator, logs, displays
   Administrative Host
   Closed Net
   Open Net
Automation Summary

- Monitoring system(s) -> ftp’s logs and display data to the administrative system
- Alert system sends e-mail or numeric page to notify system administrator or operator depending on severity
- Through perimeter network administrator or operator securely logs in and views system logs
- Optionally the administrator or operator could submit a system response
  - Response system running on the mission host polls the administrative host and retrieves system response
  - Response system approves and activates request
Recommendations

- Use firewall to protect mission network
- Use router to restrict access to the administrative network
- Use COTS tool to allow secure remote system access to administrative network only
- Add automation to mission application
Benefits

- Increase system security
- Reduce staffing
- Enable lights-out operations
- Lower mission costs
- Increase mission reliability
Contact Information

- Tracy Dorsey / Mary Hunter

NASA GSFC
Building 23 E120 Mailstop 453.7
Greenbelt, MD. 20774

(301) 286-9391
tdorsey2@csc.com