Building the Secure Management Infrastructure

Luis Luciani

Architect, Lights-Out products

HP

Scott Shaffer

Manager, Insight Manager Development

HP

HP WORLD 2003

Solutions and Technology Conference & Expo

Agenda

- Security & Systems Management
  - Usage
  - Protocols
  - Authentication
  - Authorization
  - Administration
- Securing Insight Manager 7
  - Data acquisition
  - Secure commands
- Securing the Lights-Out products
  - Access control
  - Directory service usage

Security & Management

- Assess your risk level
- Location, Location, Location
  - Intranet
  - Internet / DMZ
  - Hybrid (separate Management network)
- Physical Security
  - Management network

Protocols

- Ping
- SNMP
  - Community string password
  - Data encoded, nothing encrypted
- DMI
  - Generally based on OS RPCs
- WBEM
  - SSL-based
- WMI
  - over RPC or SOAP (SSL-based)
- Web
  - May be SSL-based
- LDAP
  - SSL-based

AAA

- Authentication
  - Local system
    - Accounts set on each system

      Example: Service Control Manager, other *nix tools
  - Domain / Directory
    - Accounts part of the domain or directory

      Example: Insight Manager 7, Lights-Out products, Rapid Deployment Pack
  - Embedded
    - Accounts inside the tools own user database

      Example: Insight Management Agents

AAA

- Authorization
  - Embedded
    - Built into the tool

      Example: Insight Manager 7, Rapid Deployment Pack, Insight Management Agents, Lights-Out products
    - Advantages

      Local control
  - Directory
    - Stored / manipulated in the directory

      Example: Lights-Out products
    - Advantages

      Centralized control

AAA

- Administration
  - Embedded
    - Built into the tool

      Example: Insight Manager 7, Rapid Deployment Pack
    - Advantages

      Easily accessed, local control
  - Directory
    - Leverages standard directory tools

      Example: Lights-Out products
    - Advantages

      Familiar, integrated

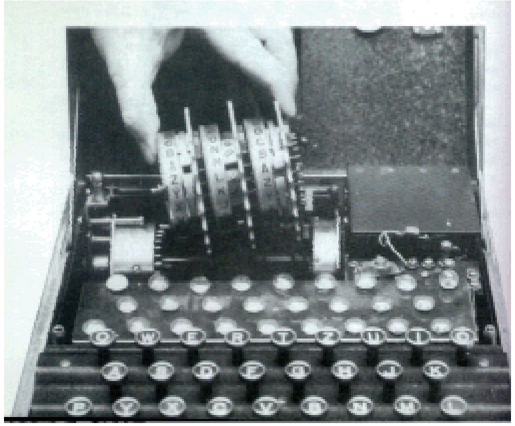
Securing Insight Manager 7

- Data acquisition
  - SNMP – read only!
  - DMI

- Secure commands

  Example: Software Deployment, Group Configuration

  - SSL-based
  - Protected by digital certificates



Securing Lights-Out Products

Best Practices:

- Use a separate management network
- Use directories
- Keep the remote console port set to “auto”
  - Remote console uses the Telnet protocol and Telnet IP port
  - Auto makes the port invisible to scans when not in use
- Use a different IP port for remote console and web access if within a DMZ

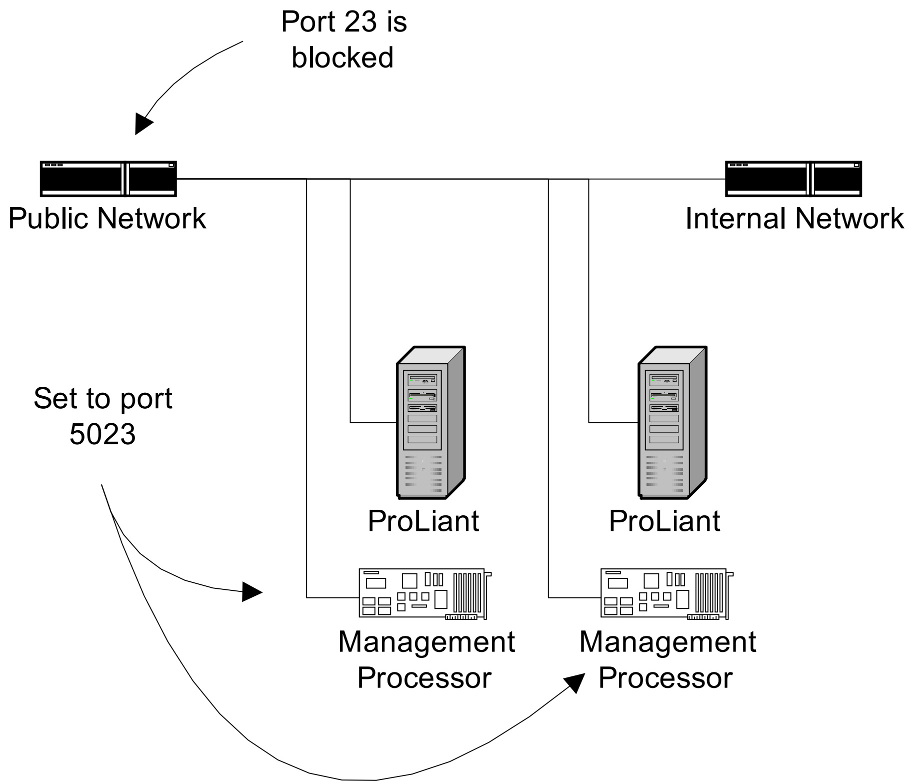
Securing Lights-Out Products

Best Practices (cont):

- Use client certificates
  - Minimize the risk of “man-in-the-middle” attacks
- Disable F8 Setup
  - Only necessary when local security cannot be guaranteed
- Keep remote console encryption turned on
  - There is no performance penalty
  - Telnet access is not possible
- Keep SSL set to 128-bit cipher strength

Securing Lights-Out Products

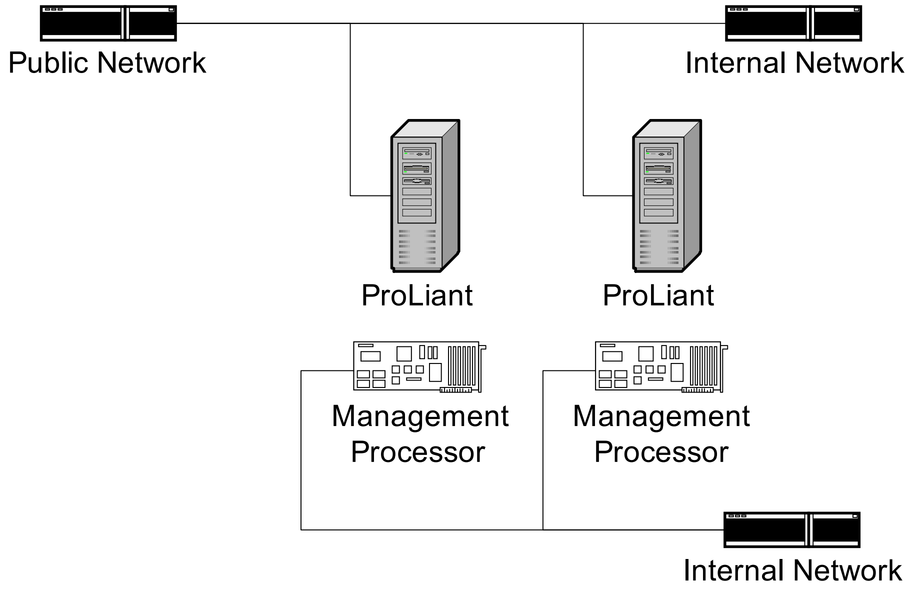
Lights-Out Products in DMZ on Single Production Network



- A non-standard Telnet port allows internal access but prevents public access
- Same can be applied to HTTP and HTTP ports

Securing Lights-Out Products

Lights-Out Products in DMZ on Management Network



- No logical path between production and management networks
- Security on management network is not critical if it is isolated

Securing Lights-Out Products
- Directories -

Advantages:

- Single point of administration of user accounts
- Changes take immediate effect domain-wide

Tips:

- Disable local accounts to provide maximum security
- Consider using having directory on the management network dedicated solely to management

Aspects

- Privacy
  - Sensitive data passed over SSL
  - Non-sensitive data passed over SNMP (very speedy!)
  - Moving to WBEM
- Trust
  - Digital certificate based
  - But no strong client authentication – weakens audit log
- Non-repudiation
  - All events logged
- Replayability
  - SSL-protected

More Information

- White Paper
  - Understanding Insight Manager 7 Security
- www.hp.com/servers/manage

Interex, Encompass and HP bring you a powerful new HP World.