

Desktop Security

Alan Stepakoff
ICIS - Desktop Services
January 14, 2004



Interoperable Computing Environment

- **Windows 2000, XP**

- ◆ ≈ 5500

- **Mac OS 9, 10.x**

- ◆ ≈ 1800

- **Linux Red Hat 8, 9**

- ◆ ≈ 150

Desktop Configuration

■ Standard Interoperable Environment

MS Word	Norton Anti-Virus (F-Prof)
PowerPoint	Meeting Maker
Excel	QuickTime player
Netscape	Real Player
Acrobat Reader	Timbuktu (VNC)
Eudora	Stuffit (TAR)
SMS or NetOctopus	

■ Systems are configured to a standard set of Protective Measures

- ◆ JPL specific security requirements in-line with NASA regulations
- ◆ Separate Protective Measure for each OS

■ All systems are part of an IT Security Plan

- ◆ Includes H/W, owner, SA, IP address, OS

User Privileges

■ Authorization

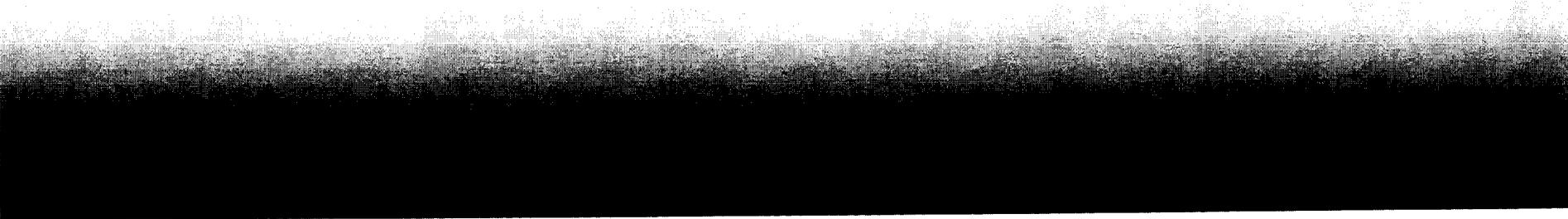
- ◆ Windows users authorize to Active Directory
- ◆ Macintosh and Linux users authorize to local system, considering Kerberos

■ Privileges

- ◆ Users are given System Administrative privileges
- ◆ Users are not given System Administrative responsibility
- ◆ Support Contractor has SA privileges and responsibility

JPL Information Services

System Management Requirements

- Monthly and ad-hoc reporting
 - New systems delivered secure
 - Security patches maintained monthly
 - Anti-Virus signature files maintained as needed
 - Emergency patches within 7 days
 - Quarterly Service Packs or point releases
- 

System Management-Current Tools

- Periodic ISS scans
 - ITSecure - Custom maintenance utility for Windows
 - SMS - Windows patch deployment
 - NetOctopus - Macintosh patch deployment
 - Norton Anti-Virus LiveUpdate
- 

Issues

- ISS scans - may take many scans to capture information
- ITSecure needs to be deployed quarterly
- SMS
 - ◆ Domain dependant
 - ◆ Too costly to prepare packages
- NetOctopus
 - Costly to prepare packages

System Management-Future Tools

- Periodic ISS scans
- Norton Anti-Virus LiveUpdate
- SUS
 - ◆ Easy to support
 - ◆ Responsibility is transferred to users
- PatchLink - NASA-wide tool
 - ◆ Unobtrusive data gathering and patch delivery
 - ◆ User can control reboot
 - ◆ Large patch repository
 - ◆ Cross platform
 - ◆ Upload data to IT Security Database to close SPL tickets and update configuration information