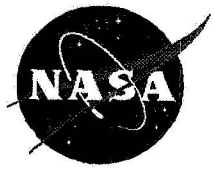
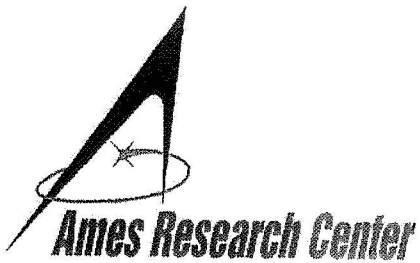
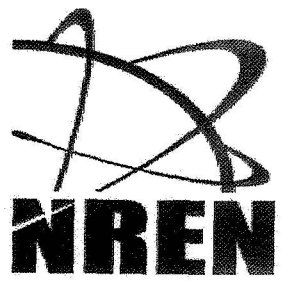


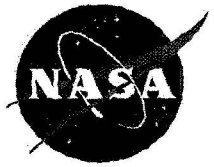


A Security Model for Space Based Communication

Thom Stone

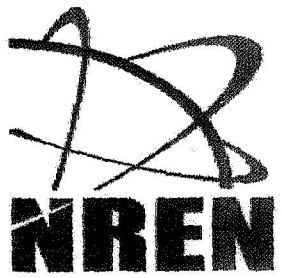
Computer Sciences Corporation





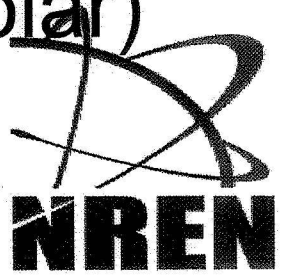
Prolog

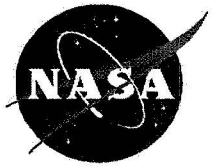
- *Everything that is not forbidden is compulsory -T.H. White*
- *They **are** after you…*



Monsters in the Closet

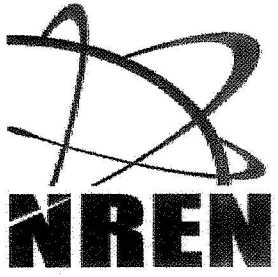
- Virus
- Trojans
- Denial of Service (DoS) attacks
- Phishing
- Spam and spyware
- Storms (Broadcast, terrestrial and solar)
- Intruders (virtual and real)

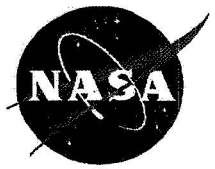




Security For Missions

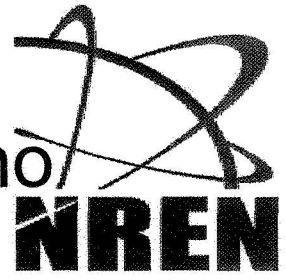
- Evolving space missions require much higher bandwidth and applications are growing in complexity
- Internet Protocols (IP) have become the standard for space as they have everywhere else
- Threats to all U.S. government communications are greater then ever
- There are more tools for security available but choices can be overwhelming

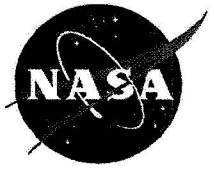


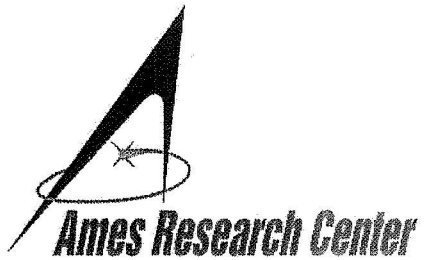


IP and Security

- The functionality and universality of the Internet create both opportunity and danger for future missions
- Threats are constantly evolving and new internet technologies open the door to new malevolence
- "Traditional" communications are just as or more insecure
- Market opportunities for new tools counterbalances threats but there is still no box with a "hacker / no hacker" switch

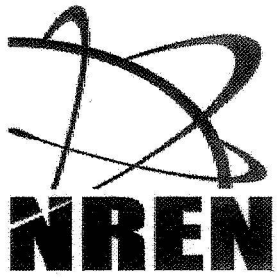






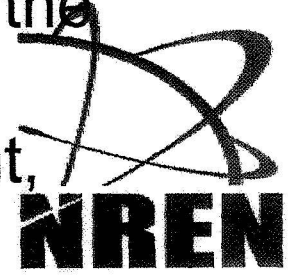
Tools

- Firewalls: Policy based, discriminate by protocol, port, address or by application based criteria
- Encryption: Has key distribution challenges
- Bastion host, enclave
- Tokens
- Intrusion detection
- Scanning, virus protection etc.

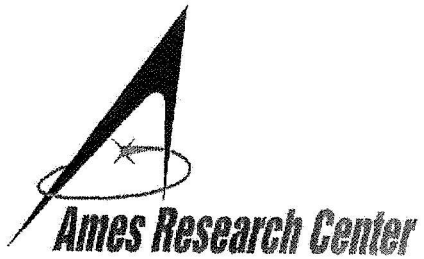


Federal Mandates

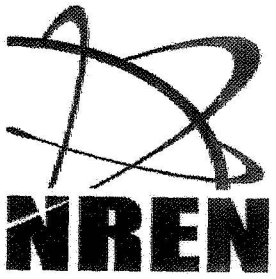
- Many regulations:
  - FISMA (Federal Information Security Management Act) is the Official policy implemented with:
    - NPR 2810.1A, NPR 1600.1
    - FIPS 199-200-201, NIST SP 800-53
    - OMB A-130
    - And on and on
- Bottom Line
  - Projects must have a security plan
  - Security planning integrated with project from the beginning
  - Extensive documentation and risk assessment, contingency plan etc. required



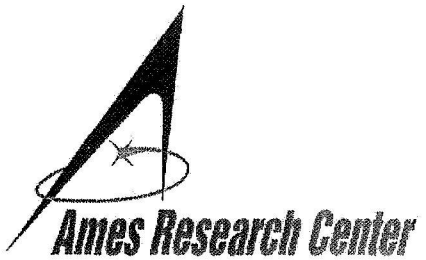
Integrated Approach



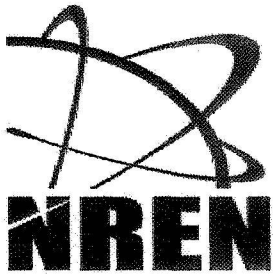
- Determine criticality of the system
- Determine risks
- Segregate functions
- Don't ignore threats besides those that come from outside (software failure, electrical fires, staff sabotage, hardware/software upgrades)
- Lifecycle vigilance

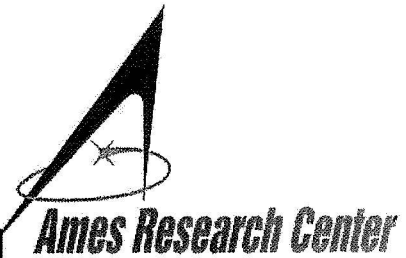


Threat Matrix



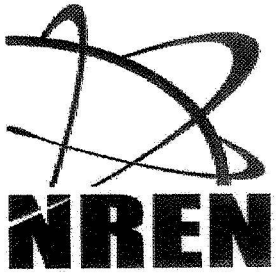
- Prevent breach of confidentiality, integrity or availability of the space system
- List threats (things of risk to the system), mitigation of the threats and a weighted likelihood and impact of the threat (hackers, virus, power failure)
- List vulnerabilities - those items that can actually happen even with present mitigation technology (mis-configuration, solar flare, funding cut)
- Go beyond the boilerplate - What really threatens your system



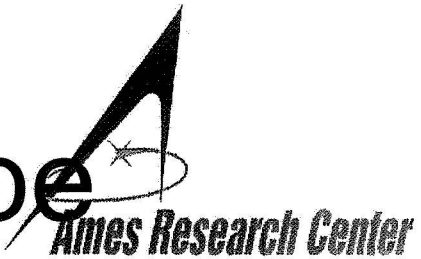


Contingency Planning

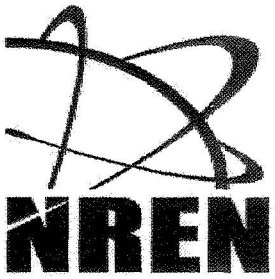
- What to do if operations center out of service
- What to do in cases when vulnerability happens
- Chances are better of getting through if you have a plan even if it does not work as you think



Mission Stages and type Data



- Stages:
  - Planning
  - building
  - launch
  - operations
  - onboard, data distribution
- Types:
  - Manned
  - Unmanned
  - Telemetry and data products
  - Commands and response



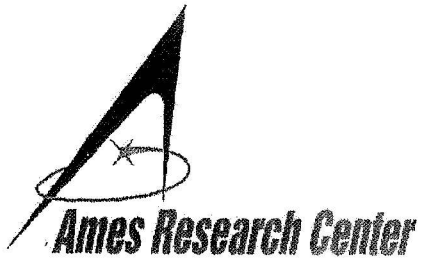
Planning, Assembly and Test Phases

Ames Research Center

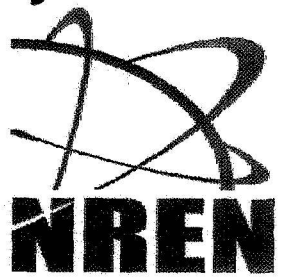
- Future missions will be multi-center efforts. This will require a secure multimedia collaboration tool for planning
- Testing in situ where payloads are assembled and monitoring on the ground before launch will require a well thought out security scheme

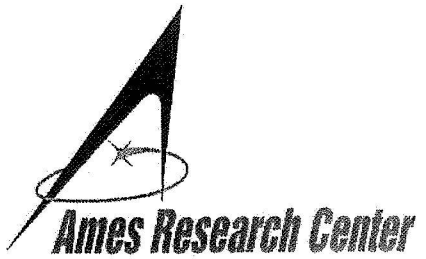
NREN

Space to Ground Communications



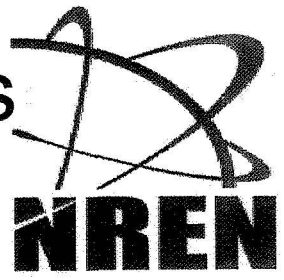
- Broadcast, anyone with the right dish can hear
- Threats are denial of service (DoS), spoofing, theft of data (accessibility, mission integrity, confidentiality)
- Encryption good for spoofing and theft but DoS attacks can be done analog so link-layer encryption of protocol is not needed



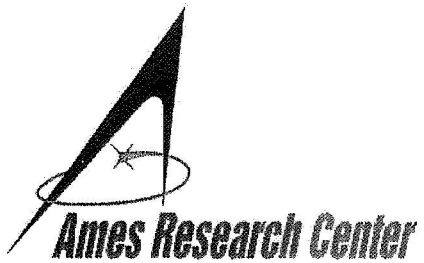


Secure Operations

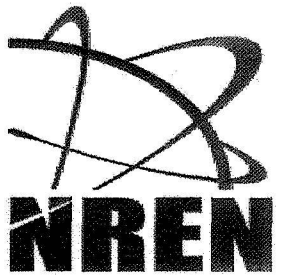
- Operations center is likely site for an attack
- Must document all procedures and have backup and recovery plans
- Separate functions on servers
- Create a secure enclave
- Frequent security scans and reviews



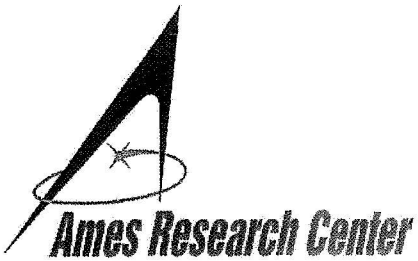
Security Framework

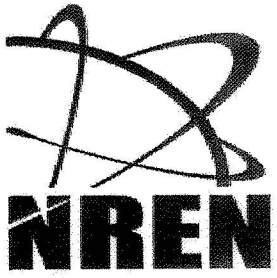


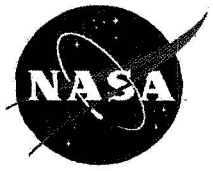
- Validate data
- Encrypt when needed - watch the keys
- Authenticate and authorize users
- Configuration and patch management
- Awareness of sensitive data
- Frequent scans and intrusion detection
- Audits and logging
- Procedures and practices



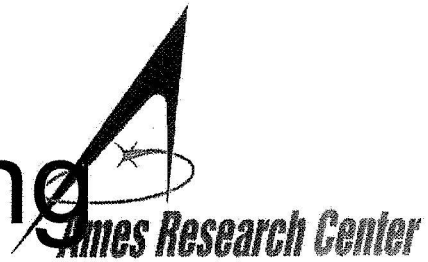
Space Data Security



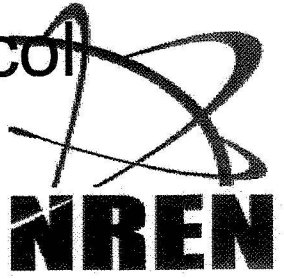


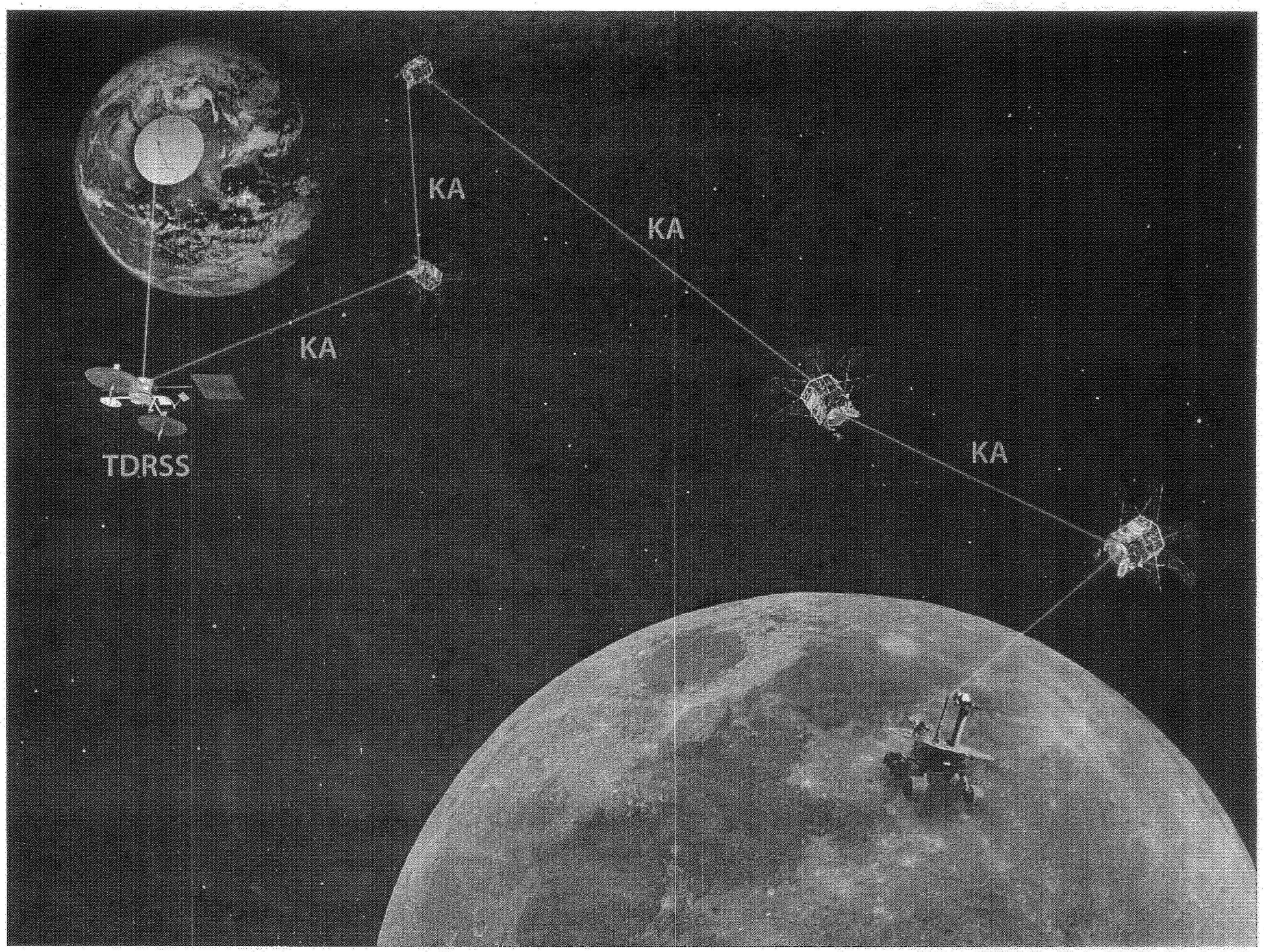


Commands and Routing Information

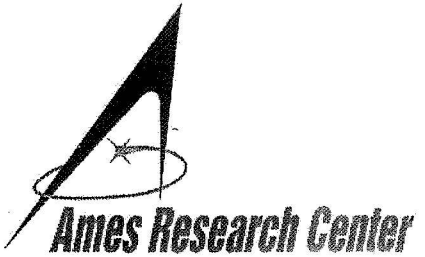


- Threats to spacecraft command and response and routing information exchange are snooping and spoofing
- Communications payload should be encrypted
- Protocol and framing do not need to be encrypted as makes routing difficult and DoS can be done analog easier than via protocol

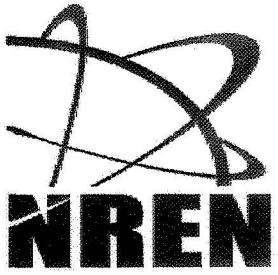


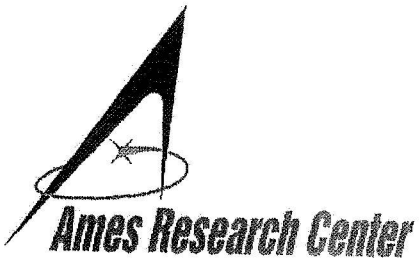

KA
KA
KA
KA
TDRSS

Data Distribution



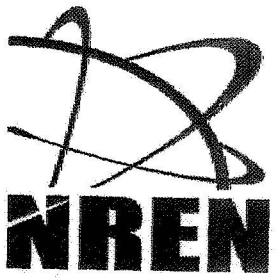
- Web based “publish-subscribe” model
- Isolate server - firewall wide area connection for only HTTP(S)
- Second Ethernet port for system updates, maintenance and data transfer. Two factor authentication for all access
- Use Web security assessment tools

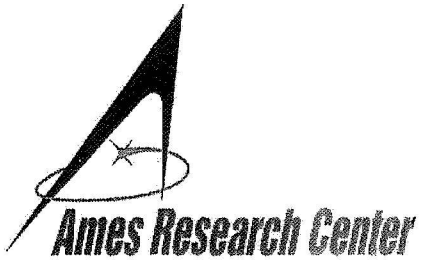




Picture here

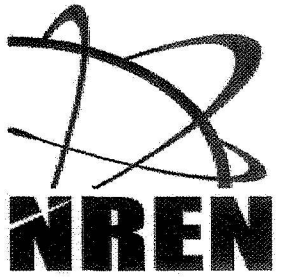
- Diagram of server two Ethernet one to wide area one to LAN with access server and data emitter

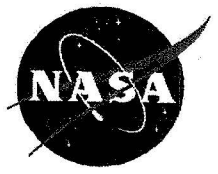


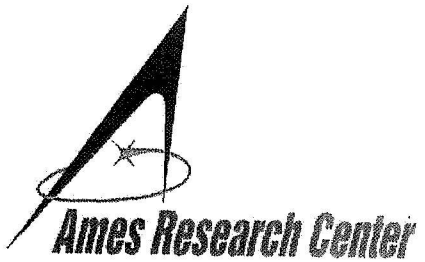


Manned Missions

- Triple redundancy rule must extend to communications security
- Must be transparent to the crew
- Future holds multimedia, voice over the Internet and other advanced Internet features







Lessons?

- We need to start thinking about security in a more organized manner
- Government mandates are not fun but can be an opportunity to do something about mission security
- Security is a process not a state of being