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) are becoming 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 creates both opportunity and danger for future missions
- Threats are constantly evolving and new internet technologies open the door to new malevolence
- “Traditional” space and ground communications can be 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 data flows by protocol, port, address or by application based criteria
- Frequent backups
- Public Key management
- Encryption: key distribution challenges
- Bastion host, enclave, authentication, authorization and accounting (AAA)
- Identity Management: Tokens, fingerprints, eye prints, psych profiles
- Intrusion detection
- Scanning, virus protection etc.

Definition

- Firewall - Appliance (hardware) or software that examines and filters Internet traffic
- Encryption key - Number used to mathmatically interact with a coded message to produce plain text
- Public key encryption - Use an outside authority to produce encryption key
- Bastion Host - Server used as single entrance to a network from the Internet

.

More Definitions

- Intrusion detection - Software that identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.
- Scanning - Examining software and files on a system to see if all security patches are in place and no malware is present
- DoS - Denial of Service attack - maliciously keeping network resources unavailable

The Cost of Securing a System

- Complexity
- User burden
- Lack of flexibility
- Performance degradation
- Difficulty implementing new features
- Additional hardware required
- Additional very skilled labor

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 mandated by NASA policy
  - Extensive documentation and risk assessment, contingency plan etc. required

Integrated(Holistic) Approach

- Determine criticality of the system
- Determine risks
- Segregate functions
- Don’t ignore physical and procedural threats (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 entire operations center out of service
- What to do when critical elements break
- What to do in cases when security is breached
- Chances are better of getting through if you have a plan even if it does not work as you think
- Test backup and recovery plans or they wont work when you need them

Mission Stages and type Data

- Stages:
  - Planning
  - Building
  - Launch
  - Operations
    - Onboard LAN operation
    - Science data distribution

- Types:
  - Manned
  - Unmanned
  - Telemetry and data products
  - Commands and response

Planning, Assembly and Test Phases

- 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

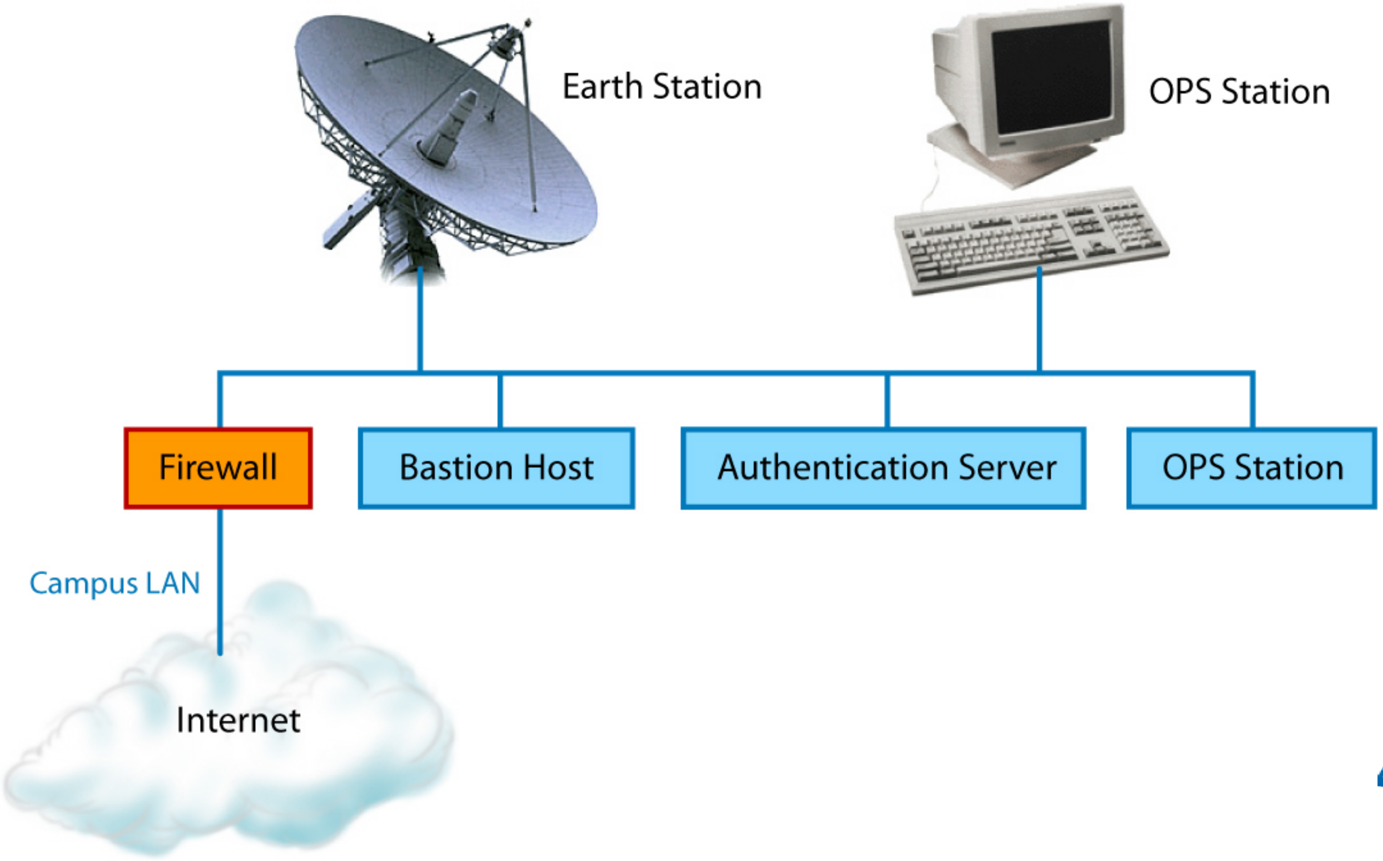
Space to Ground Communications

- Broadcast, anyone with the right dish can hear
- Transmitting more complex
- Threats are denial of service (DoS), spoofing, theft of data (accessibility, mission integrity, confidentiality)
- Communications is usually intermittent - Which outages are normal?

Secure Operations

- Operations center is likely site for an attack
- Must document all procedures, and have backup and recovery plans
- Firewall- Frequent policy review - Keep patches up to date!
- Separate functions on servers
- Create a secure enclave
- Intrusion detection- Protocol for contact with response organization
- Frequent security scans and reviews

Secure Operations Center



Who You Gonna Call

- Local Help Desk
- Center Chief Security Officer or staff
- CERT (Computer Emergency Response Team)
- Federal Law enforcement

Authentication and Firewalls

- Two factors - What you know, what you have or what you are: Password and:
- Secure tokens, biometric, behavior (how you key your password)
- RADIUS TACACS+ : Authentication, Authorization, accounting
- State oriented firewalls
  - Deal with voice, video,other applications
  - Check for strange network behavior
  - Address management (non-routable addresses)

Security Framework

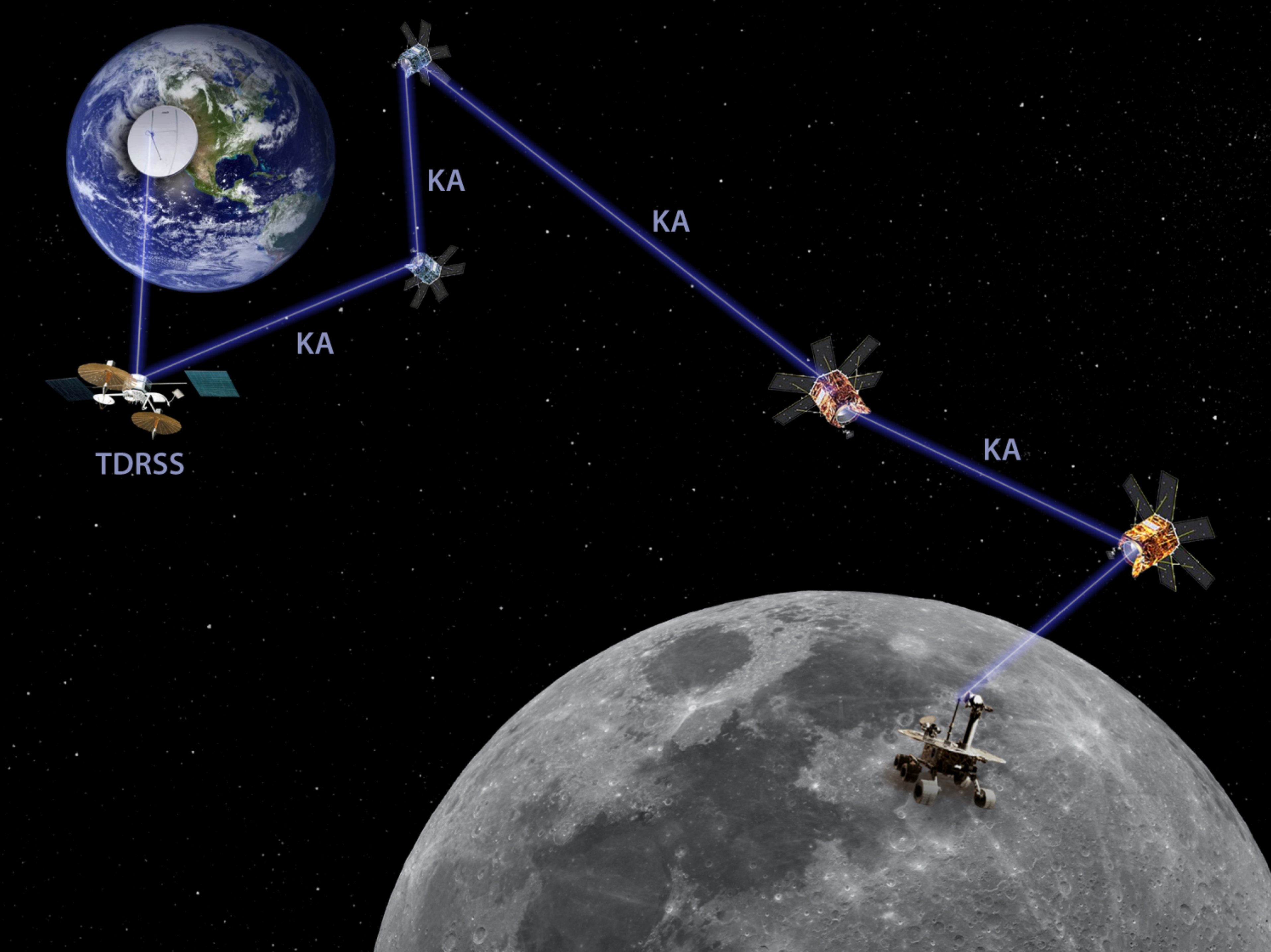
- Validate data
- Encrypt when needed - watch the keys
- Authenticate and authorize users
- Two factor authentication (token or biometric) a must
- Configuration and patch management
- Awareness of sensitive data
- Frequent scans and intrusion detection
- Audits and logging
- Procedures and practices

Space Data Security

- Investigator exclusive access
- Sensitive information
- Backup media.. Will it still be there when we are 65! Will it deteriorate?
- Catalog - Where is it? Is it current?
- Public availability of data products

Commands and Routing Information

- Threats to spacecraft command and response and routing information exchange:
  - snooping (eavesdropping)
  - Spoofing (sending bogus commands)
- Command data should be encrypted
- Protocol and framing should not be encrypted
  - Makes routing difficult
  - Analog jamming easier than IP DoS (denial of Service attack)


KA
KA
KA
KA
TDRSS

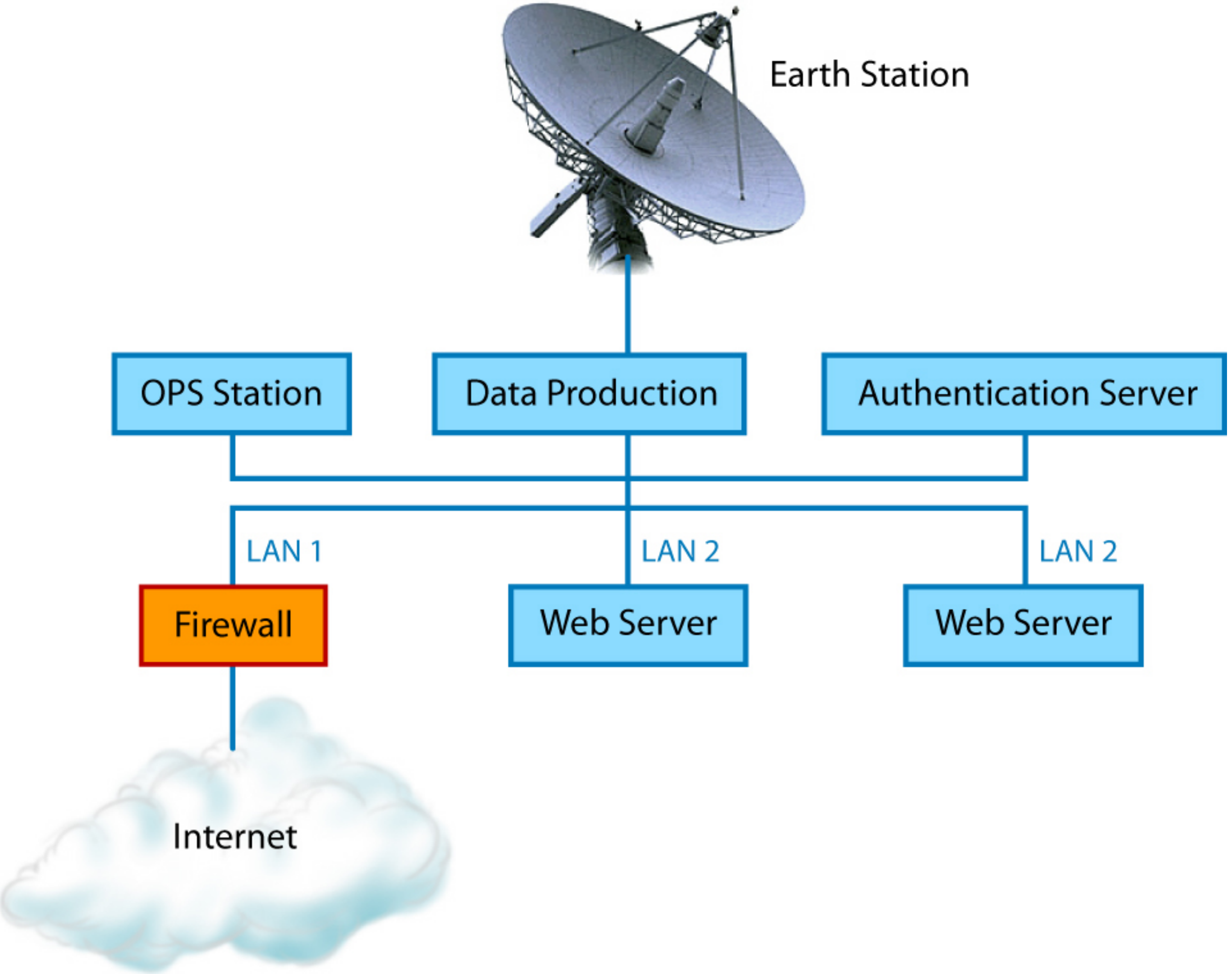
Data Distribution

- 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

NASA

mes Research Center

Secure Web Services



Earth Station

OPS Station

Data Production

Authentication Server

LAN 1

LAN 2

LAN 2

Firewall

Web Server

Web Server

Internet

NREN

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