SECURITY FOR SPACE SYSTEMS: A RETROSPECTIVE

A look at security in space from the ‘old’ days to the present

Howard Weiss
27 May 2024

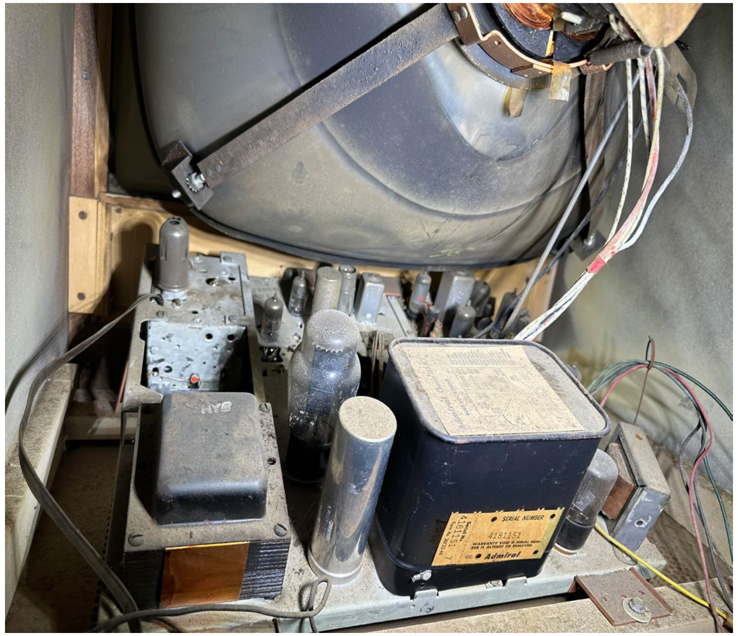
AGENDA

1. Who am I - early beginnings…
2. Computing the way I did it in the early days (1970s)!
3. Cybersecurity for Civilian Space – 30 years

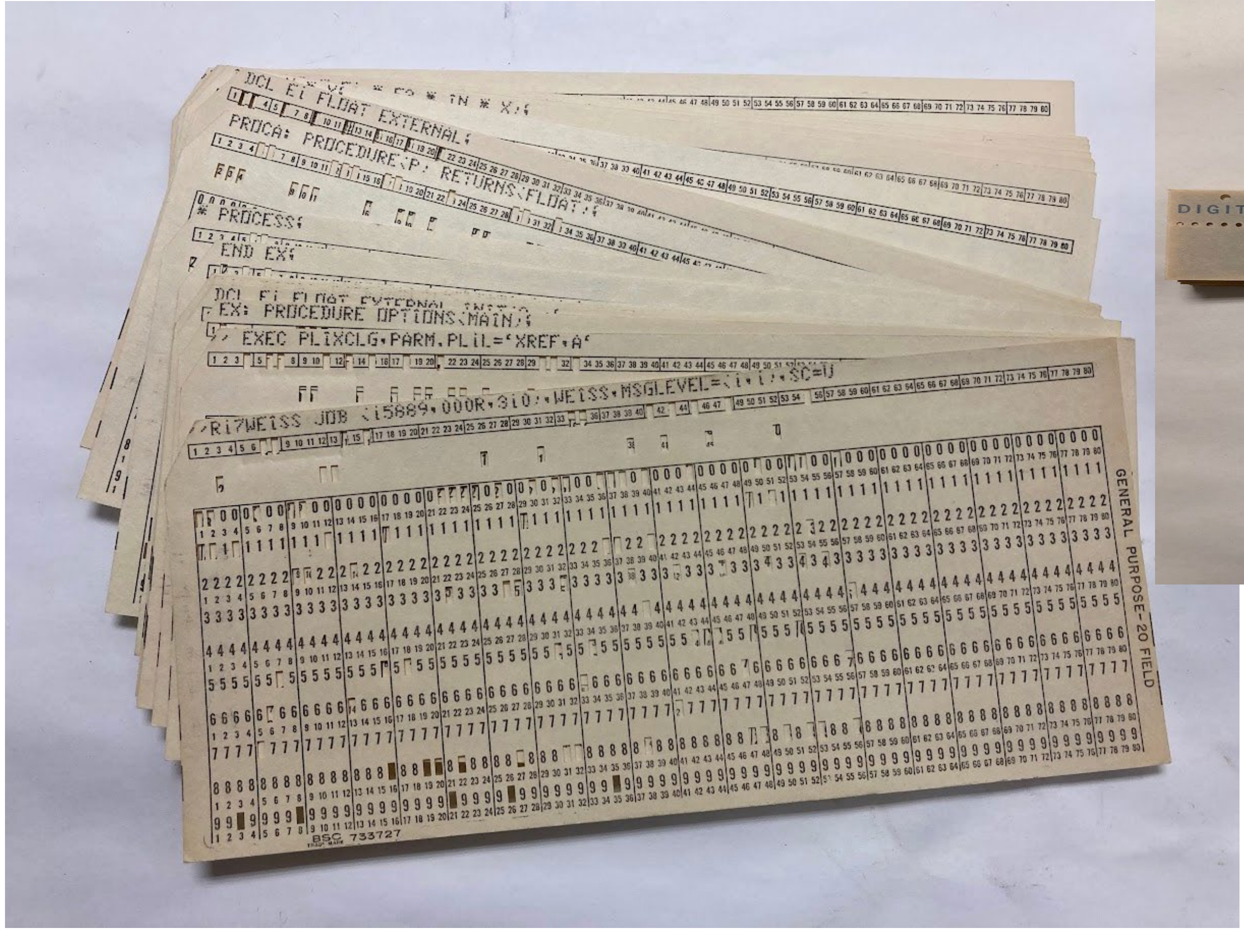
   - the “OLD” days (90s and early 2000s)
     - Security + civilian space
     - CCSDS + Security
     - Security Standards & Testing

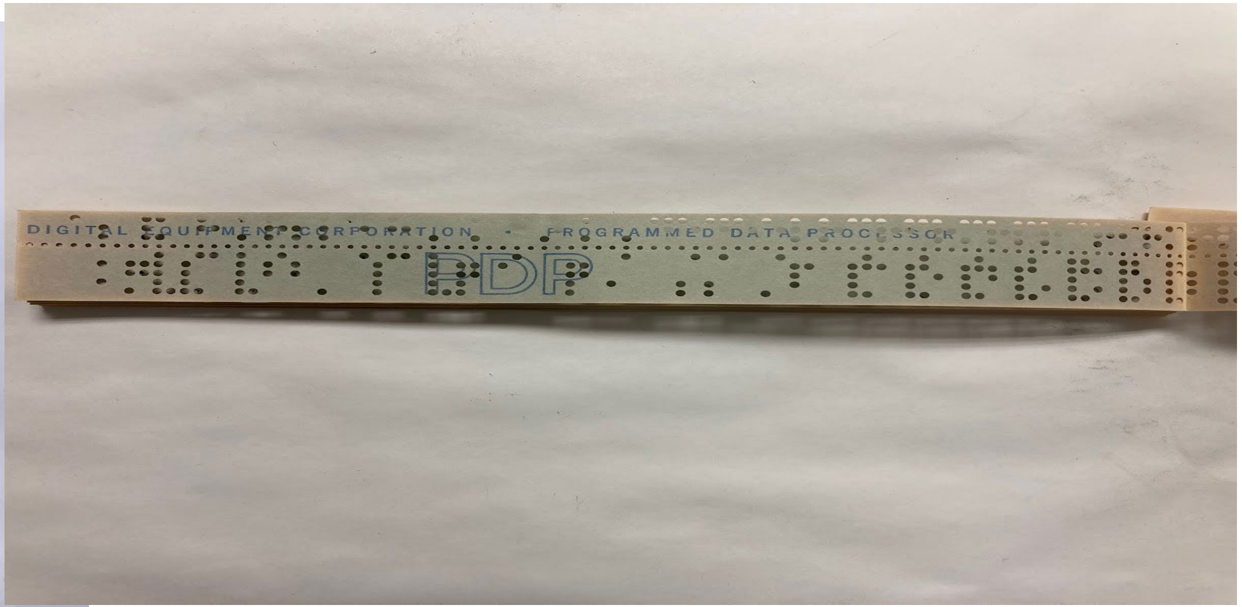
   - the ‘modern era’
     - Now
     - The future

EARLY BEGINNINGS – A BUDDING ENGINEER….



COMPUTER PROGRAMMING IN THE 70'S





PERSONAL COMPUTERS CIRCA THE 80'S!

CYBERSECURITY 101 – THE EARLY DAYS

- **Originally called COMPUTER SECURITY (COMPUSEC)**
  - Primarily concerned with operating system security (not much has changed!) for mainframes – MULTICS!
  - Multilevel secure operating systems
    - Formal verification of operating system security functions (nothing more/nothing less than required)
- **Later combined with cryptography to be called INFORMATION SECURITY (INFOSEC)**
  - Operating systems utilizing cryptography
    - Secure data at-rest
    - Networking - Secure data in transit
    - Encrypted file systems (secure data at rest)
    - New computing paradigms such as distributed computing, client-server – move away from mainframes
- **Later called INFORMATION ASSURANCE**
  - Same as before but now with a different name
- **Currently CYBERSECURITY**
  - Cool new name!
  - Cloud computing security!

SECURITY FOR SPACE (WAY BACK IN THE OLD DAYS)

- **Military:**
  - Fully encrypted space links from ground-to-space
  - Pre-loaded keys for mission duration (later use over-the-air keying)
  - Government developed crypto algorithms
- **Civilian (circa 1993):**
  - For the most part: No security and No encryption
    - Open command links/Open downlinks
    - Some expensive commercial bulk encryptors available (see next slide)
  - No requirements for secure operations
  - Personal experiences:
    - CCSDS "Security 101" Briefing in 1993:
      - "*that is great for military systems, but we are civilian science missions, and no one cares about us*."
    - Jet Propulsion Laboratory (JPL)
      - "*we operate in deep-space and an attacker would need a gigawatt of power and a 70m antenna to harm us*."
    - NASA Goddard Space Flight Center
      - "*our command sequences are so hard to understand, no one would be able to figure them out*."

COMMERCIAL SPACECRAFT SECURITY DEVICES (2001-13)

RAINBOW TECHNOLOGIES MYKOTRONX

Information & Communication Security

Company | Solutions & Services | Products | Rainbow Worldwide

Space Communications

Commercial Space Products Links

MYK-14 Ground Unit

MYK-41 Centurion ASIC

MYK-42 DES ASIC

Related Documents

Rainbow Mykotronx Commercial Space Products

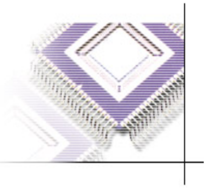
Rainbow Mykotronx Site Directory

About Rainbow Mykotronx

Rainbow Technologies Home

MYK-42 ASIC

Exportable Command Link Decryptor for Commercial Satellite Systems



This exportable VLSI microcircuit implements the Centurion algorithm, which safeguards command links in commercial satellite ground and flight components. Key features include built-in authentication, Electronic Codebook operation mode, and interface compatibility with Caribou and Cardholder devices.

Features and Benefits

- Exportable commercial algorithm.
- Pin-for-pin compatibility with Cardholder and Caribou.
- Command format compatibility with Cardholder and Caribou.
- Telemetry format compatibility with Cardholder and Caribou.
- Continuous data mode format (128 bits).
- Two command authenticate formats—Ternary and Binary.
- Maximum uplink rate of 20 Mbps (22,123 commands per second).
- Built-in self-test (BIST).
- Meets QML Class V MIL requirements
- DESC-qualified QML gate array manufacturer
- Radiation-hardened for space applications; 100K Rad (Si). Total dose: (>300K functional)

Specifications

Data Rate:	1bps to 20 Mbps
Operating Voltage:	4.5 to 5.5 VDC
Power Consumption:	TBD
Data Interface:	CMOS levels
Format:	NRZ-L, NRZ-M
Processing:	DESC-qualified QML CMOS gate array
Testing:	MIL-PRF-38535/MIL-STD-883 Level "S"
Additional Testing:	Group E and DPA Available
Temperature Range :	-55 to +125° C
MTTF:	>10M Hours per MIL-HDBK-217E
Technology:	0.6 micron Triple Level Metal Bulk CMOS gate array
Package:	84-pin ceramic flat pack

RAINBOW TECHNOLOGIES MYKOTRONX

Information & Communication Security

Company | Solutions & Services | Products | Rainbow Worldwide

Space Communications

Commercial Space Products Links

MYK-14 Ground Unit

MYK-41 Centurion ASIC

MYK-42 DES ASIC

Related Documents

Rainbow Mykotronx Commercial Space Products

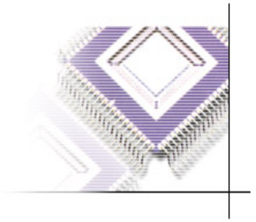
Rainbow Mykotronx Site Directory

About Rainbow Mykotronx

Rainbow Technologies Home

MYK-41 Centurion ASIC

Downlink Encryptor/Decryptor



A radiation-hardened VLSI chip for embedment applications, the MYK-41 VLSI encrypts or decrypts using the DES algorithm.

Features and Benefits

- Cryptographically compatible with DES FIPS Pub 46.
- Operates in Electronic Codebook (ECB) or Output Feedback (OFB) mode.
- Off-the-shelf QML "Q" availability.
- Binary TTL data format.
- Maximum data rate of 160 Mbps with system clock at 20 MHz.
- Subject to export controls.
- Meets QML Class Q requirements of MIL-PRF-38535.
- DESC-qualified JAN CMOS gate array manufacturer.
- Radiation hardened for space applications.

Specifications

Data Rate:	1bps to 160Mbps
Operating Voltage:	4.5 to 5.5 VDC
Power Consumption:	40 mW/MHz (nominal)
Data Interface:	I/O--32-bit parallel TTL, Clocks--CMOS
Format:	NRZ-L
Processing:	DESC-qualified JAN CMOS gate array
Testing:	Functional and progagation delays; Group E and DPA available.
Temperature Range:	-55 to +125° C
Technology:	Sub-micron CMOS
Package:	172-pin ceramic flat pack

Raytheon

Gryphon AES AVE KI-55

Complete TT&C Security Solution

General-Purpose AVE for simultaneous authenticated command uplink decryption and mission/telemetry downlink encryption

Key Specifications

- Uplink Algorithm:
  - AES-256 (NIST FIPS-197) Modes: GCM, ECB, CTR, and CFB
  - Authenticated Command Modes: GCM and ECB with VCC (Vehicle Command Count)
- Downlink Encryptor Algorithm:
  - Fail-Safe Redundant AES-256 Modes: GCM, CTR, and CFB
  - Random number generator (RNG) for initial vector generation
- Over-the-Air Rekey (OTAR):
  - AES-256 ECB per KMI 3240 Key Wrap Spec
  - In-band or in-flight transferring of black key

This Type 1 TT&C provides both Uplink and Downlink COMSEC protection in a single compact unit.

Features available for the first time in a space crypto solution:

- Multiple cryptographic modes and flexible synchronization logic support many mission profiles and CONOPS
- GCM cryptographic mode supports variable length authenticated commands up to 32k bytes in length
- Integrity verification downlink option is ideal for tactical applications, such as UHF radios
- Multiple authenticated command channels enable direct payload or satellite tasking from tactical and/or multiple users

- Highly integrated single chip embedded ASIC within the AVE reduces footprint and power
- Unclassified; designed for releasability

Additional Advantages:

- Protects data through TS/SCI
- Interoperable with KIV-7M, Enhanced Suite B Gryphon GOE
- Miniaturized AVE is an ideal choice for SmallSat, NanoSat, and CubeSat
- Over-the-Air Rekey (OTAR) capability to extend mission service life and allow dynamic crypto net management

EARLY CIVILIAN THREATS - 1999:

HACKER NEWS NETWORK

1999 - http://www.hackernews.com

Security Analysis of Satellite Command and Control Uplinks

By Brian Oblivion, L0pht Heavy Industries

> "Many critical information paths flow over satellites orbiting our earth. A box floating in space seems to be a likely target for hacker groups or renegade nation-states…
>
> There are two methods of compromising a satellite by an external threat vector. One is an attack directly on the Satellite by a rogue Ground Station. The second is an attack on the Master Ground Station…
>
> Space mission protocol design information is available on NASA sites..."

MORE THREATS - 1999

By TRIBUNE NEWS SERVICES

PUBLISHED: March 1, 1999 at 1:00 a.m. | UPDATED: August 11, 2021 at 12:04 a.m.

Computer hackers have seized control of one of Britain's military communication satellites and issued blackmail threats, The Sunday Business newspaper reported.

The paper, quoting security sources, said the intruders altered the course of one of Britain's four satellites, which are used by defense planners and military forces around the world.

The sources said the satellite's course was changed just over two weeks ago. The hackers then issued a blackmail threat, demanding money to stop interfering with the satellite.

"This is a nightmare scenario," said one intelligence source. Military strategists said that if Britain were to come under nuclear attack, an aggressor would first interfere with military communications systems.

"This is not just a case of computer nerds mucking about. This is very, very serious, and the blackmail threat has made it even more serious," one security source said.

MORE 'RECENT' THREATS - 2007

Hackers commandeer US government satellites

Blame China

Dan Goodin   Fri 28 Oct 2011 // 07:03 UTC

Hackers interfered with two US government satellites on four separate occasions in 2007 and 2008, according to a report scheduled to be released next month by a congressional commission.

In June 2008 and again in October of the same year, a Terra AM-1 earth observation satellite operated by NASA experienced interference at the hands of hackers, *Bloomberg Businessweek* reported, citing the unreleased report. The draft doesn't elaborate on the interference, but it said the sessions lasted two minutes in the first incident and nine minutes in the second incident.

It also said "the responsible party achieved all steps required to command the satellite," although the hackers didn't actually exercise control over the craft.

A Landsat-7 earth observation satellite jointly managed by NASA and the US Geological Survey was commandeered for 12 minutes or longer on two occasions in October 2007 and July 2008, the report stated.

CCSDS – SCOPE AND ORIGINS

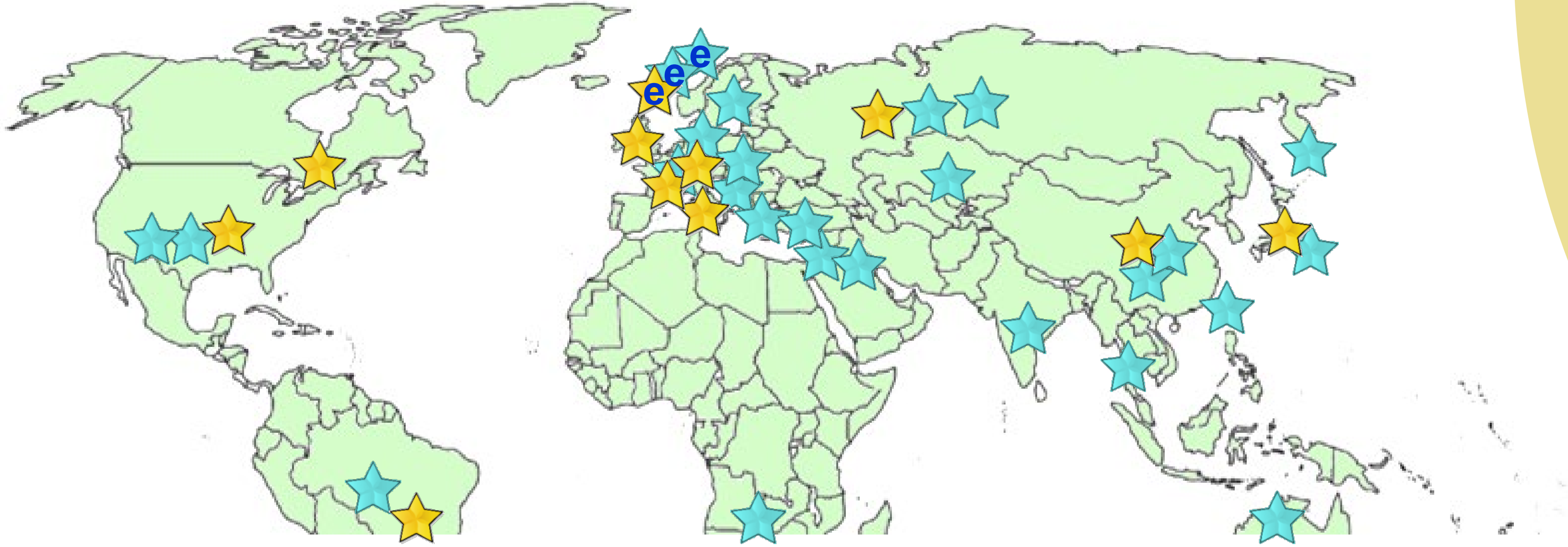
- **CCSDS == 'Consultative Committee for Space Data Systems'**
  - www.ccsds.org
- **CCSDS was founded in 1982 to develop standards at the lower layers of the protocol stack (telemetry, telecommand).**
  - Scope has expanded to cover standards throughout the entire ISO communications stack, plus other data systems areas (architecture, archive, security, XML exchange formats, etc.)
- **The primary goal of CCSDS is *interoperability* between communications and data systems of space agencies' vehicles, facilities, missions and programs.**

CCSDS + <u>SECURITY</u> (*A NEW AWAKENING!*) – MID 90'S

- **CCSDS was concerned with 'traditional' space communications protocol standardization, e.g.:**
  - Standardization and Interoperability (saves money, off-the-shelf)
  - Link layer frames
  - Telecommand (TM) (ground-to-space)
  - Telemetry (TC) (space-to-ground)
  - Advanced Orbiting Systems (AOS) (full duplex)
  - Space Link Extension (SLS)
- **Traditionally, no security concerns – '*we only do science missions*'**
  - To address security issues for civilian space missions:
    - CCSDS Security Working Group (SecWG) was created !

BACKGROUND: CCSDS PARTICIPATION

- **CCSDS – An Agency-Led International Committee**
  - 11 Member agencies
  - 33 Observer Agencies
  - 26 nations represented
  - 139 Commercial Associates
  - ~200 attendees at Spring/Fall meetings
- **Also functions as an ISO Subcommittee**
  - TC20/SC13 - Space Data & Info Transfer Systems



MEMBER AGENCIES

ASI/Italy
CNES/France
CNSA/China
CSA/Canada
DLR/Germany
ESA/Europe
FSA/Russia
INPE/Brazil
JAXA/Japan
NASA/USA
UKSA/UK

OBSERVER AGENCIES

ASA/Austria
BELSPO/Belgium
CAS/China
CAST/China
CLTC/China
CSIRO/Australia
DCTA/Brazil
DNSC/Denmark
EgSA/Egypt
ETRI/Korea
EUMETSAT/Europe
EUTELSAT/Europe
GISTDA/Thailand
HNSC/Greece
IKI/Russia
ISTRAC/India
KARI/Korea
KAZCOSMOS/Kazakhstan
KFKI/Hungary
MBRSC/UAE
MOC/Israel
NCST/USA
NICT/Japan
NOAA/USA
NSO/Netherlands
SANSA/South Africa
SSC/Sweden
SSO/Switzerland
SUPARCO/Pakistan
TASA/Taiwan
TsNIIMash/Russia
TUBITAK/Turkey
USGS/USA

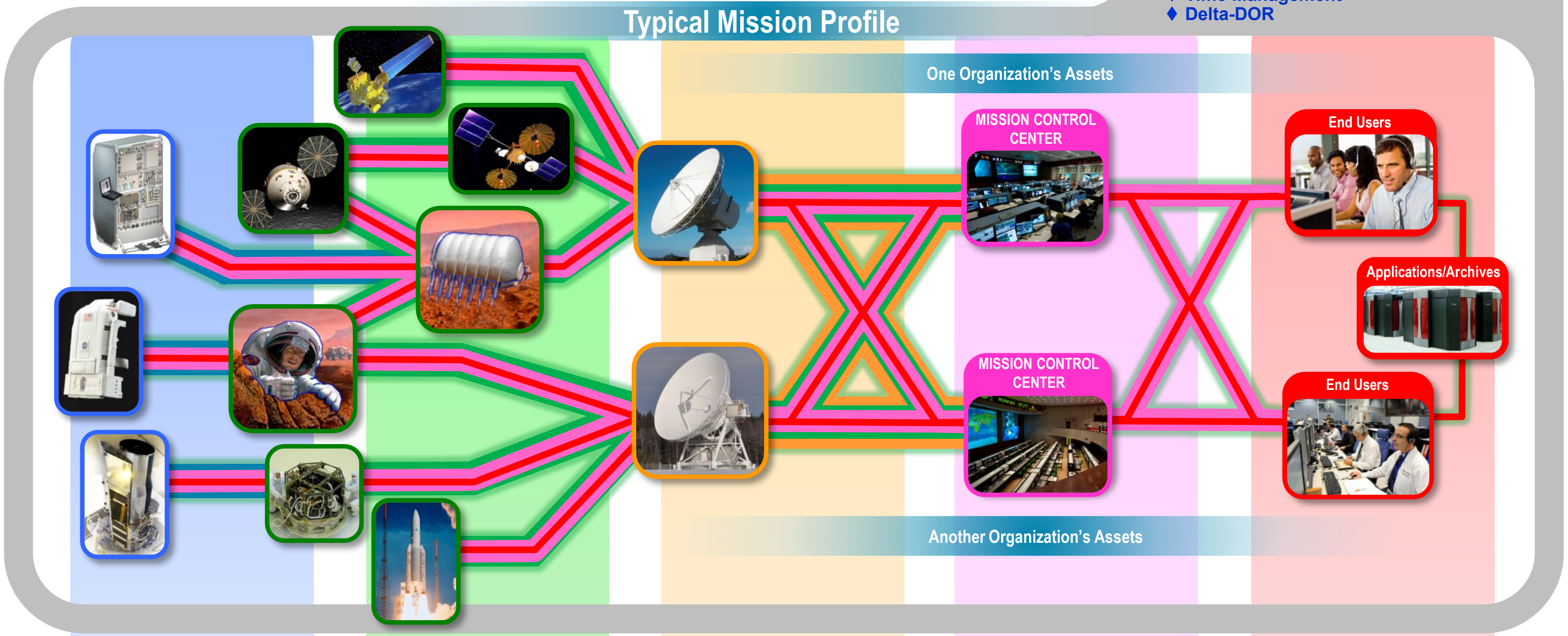
CCSDS ORGANIZATION OVERVIEW

Six Areas + working groups

- ♦ Working Group (producing standards)
- ♦ Birds-Of-a-Feather stage (pre-approval)
- ♦ Special Interest Group (integration forum)

Systems Engineering

- ♦ Systems Architecture
- ♦ Security
- ♦ Space Assigned Numbers Auth.
- ♦ Time Management
- ♦ Delta-DOR



Spacecraft Onboard Interface Services

- ♦ Onboard Wireless WG
- ♦ Application Supt Services
- ♦ Subnet Services

Space Link Services

- ♦ RF & Modulation
- ♦ Space Link Coding & Sync.
- ♦ Data Compression
- ♦ Space Link Protocols
- ♦ Optical Communications
- ♦ Space Data Link Security

Cross Support Services

- ♦ Service Management
- ♦ Transfer Services
- ♦ Cloud Computing BOF

Space Internetworking Services

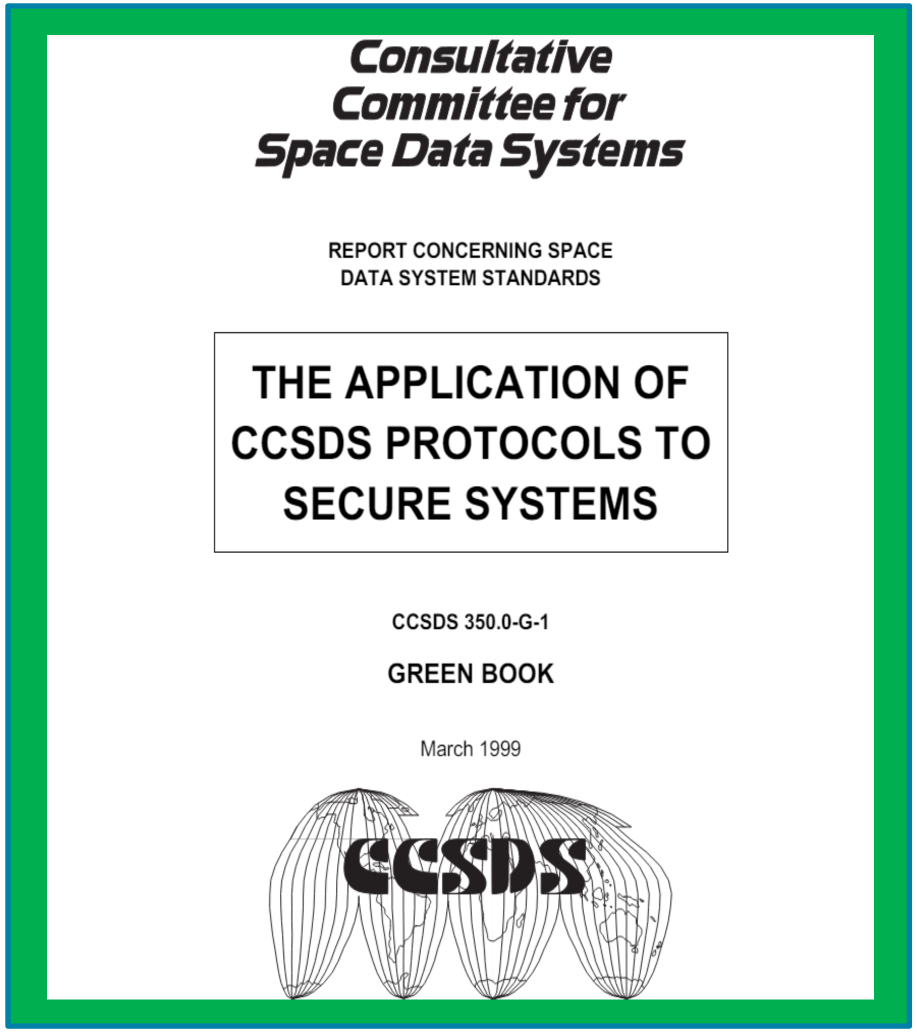
- ♦ Motion Imagery & Apps
- ♦ Delay Tolerant Networking
- ♦ Voice
- ♦ CFDP Revisions

Mission Ops & Info Mgt Services

- ♦ Data Archive Interoperability
- ♦ Navigation
- ♦ Spacecraft Monitor & Control
- ♦ Mission Planning & Scheduling

CCSDS SECURITY WORKING GROUP: A HUMBLE BEGINNING

- First efforts to bring security to the attention of CCSDS and Agency mission planners



Consultative Committee for Space Data Systems

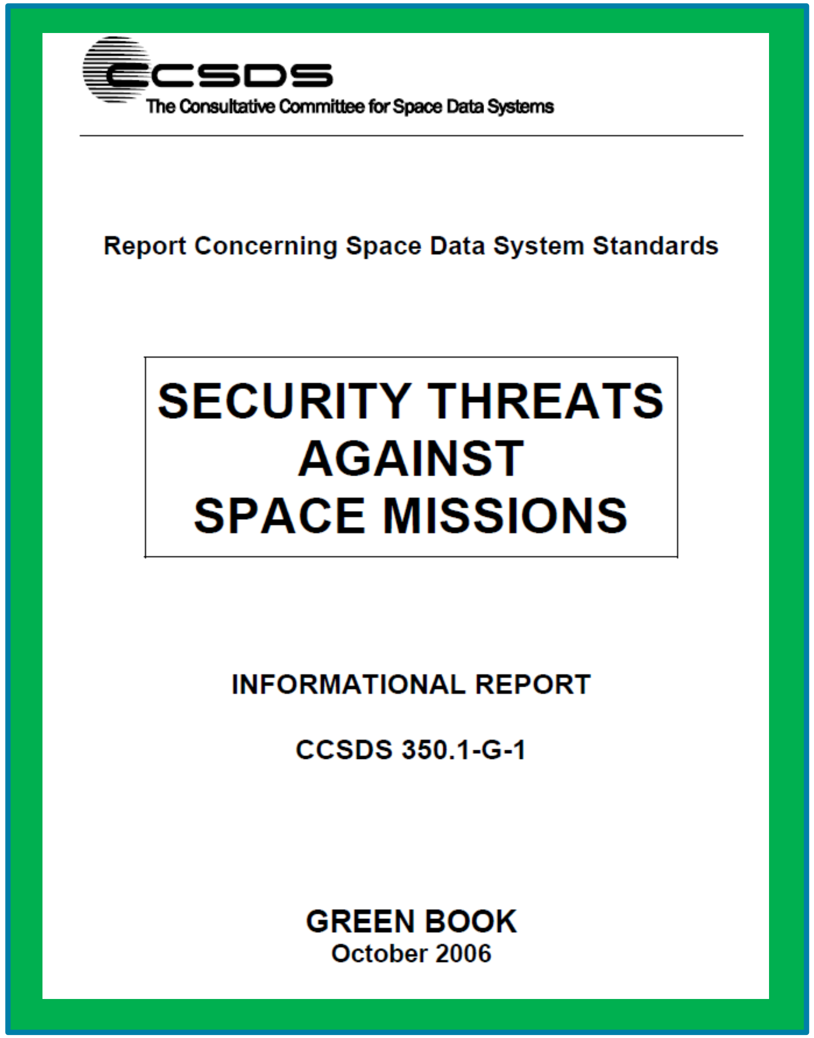
REPORT CONCERNING SPACE DATA SYSTEM STANDARDS

THE APPLICATION OF CCSDS PROTOCOLS TO SECURE SYSTEMS

CCSDS 350.0-G-1

GREEN BOOK

March 1999



The Consultative Committee for Space Data Systems

Report Concerning Space Data System Standards

SECURITY THREATS AGAINST SPACE MISSIONS

INFORMATIONAL REPORT

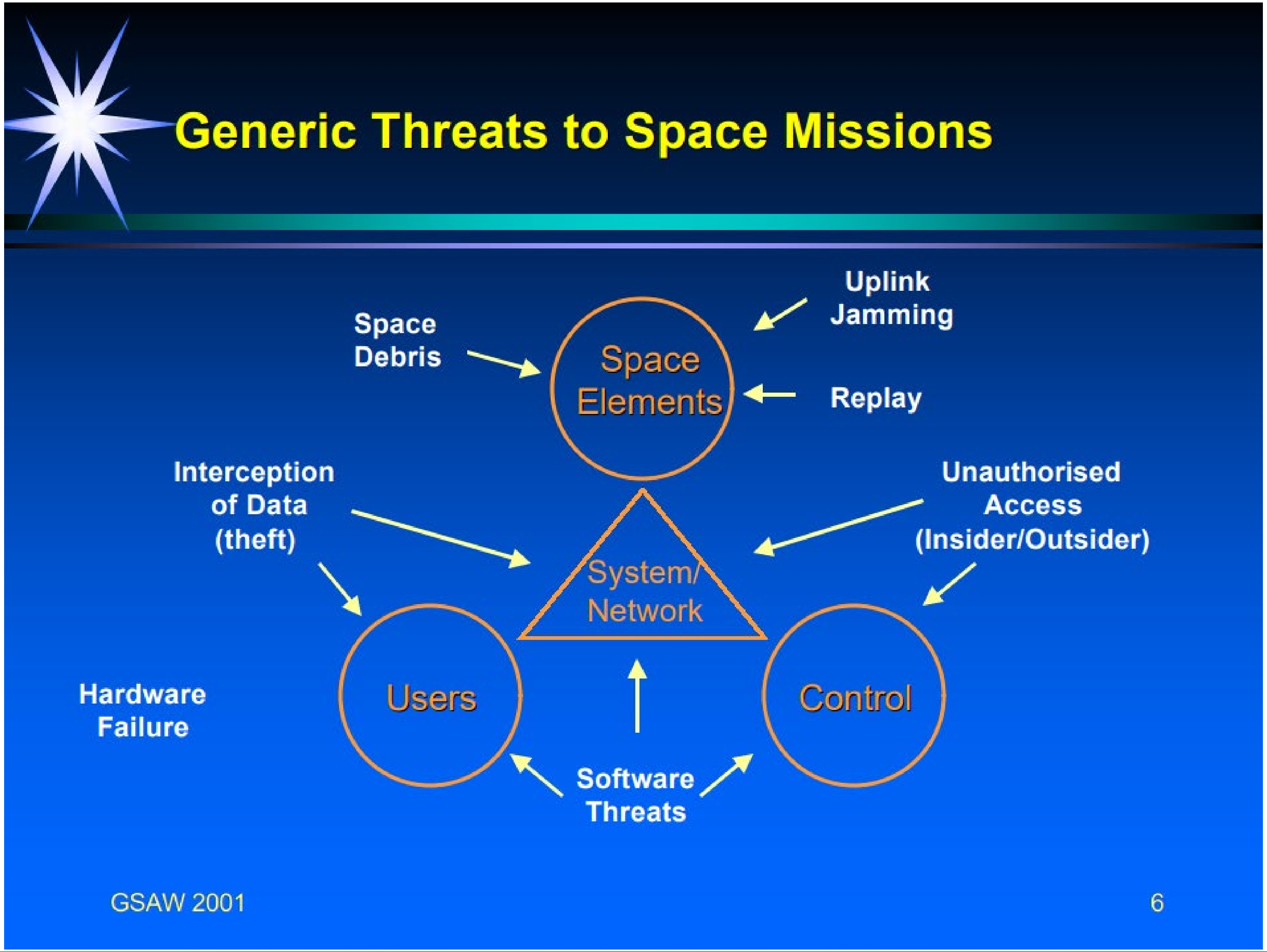
CCSDS 350.1-G-1

GREEN BOOK

October 2006

THREAT DEPICTION FOR MISSION PLANNERS

Intent: scare the pants off mission planners to get them to pay attention to security!



INTERNET PROTOCOLS IN SPACE – WITH SECURITY!

Consultative Committee for Space Data Systems

RECOMMENDATION FOR SPACE DATA SYSTEM STANDARDS

SPACE COMMUNICATIONS PROTOCOL SPECIFICATION (SCPS)—
NETWORK PROTOCOL
(SCPS-NP)

CCSDS 713.0-B-1

BLUE BOOK

May 1999

Consultative Committee for Space Data Systems

RECOMMENDATION FOR SPACE DATA SYSTEM STANDARDS

SPACE COMMUNICATIONS PROTOCOL SPECIFICATION (SCPS)—
SECURITY PROTOCOL
(SCPS-SP)

CCSDS 713.5-B-1

BLUE BOOK

May 1999

Note:
This current issue includes all updates through Technical Corrigendum 1, dated August 2010.

Consultative Committee for Space Data Systems

RECOMMENDATION FOR SPACE DATA SYSTEM STANDARDS

SPACE COMMUNICATIONS PROTOCOL SPECIFICATION (SCPS)—
TRANSPORT PROTOCOL
(SCPS-TP)

CCSDS 714.0-B-1

BLUE BOOK

May 1999

Note:
This current issue includes all updates through Technical Corrigendum 1, dated November 2006.

Consultative Committee for Space Data Systems

RECOMMENDATION FOR SPACE DATA SYSTEM STANDARDS

SPACE COMMUNICATIONS PROTOCOL SPECIFICATION (SCPS)—
FILE PROTOCOL
(SCPS-FP)

CCSDS 717.0-B-1

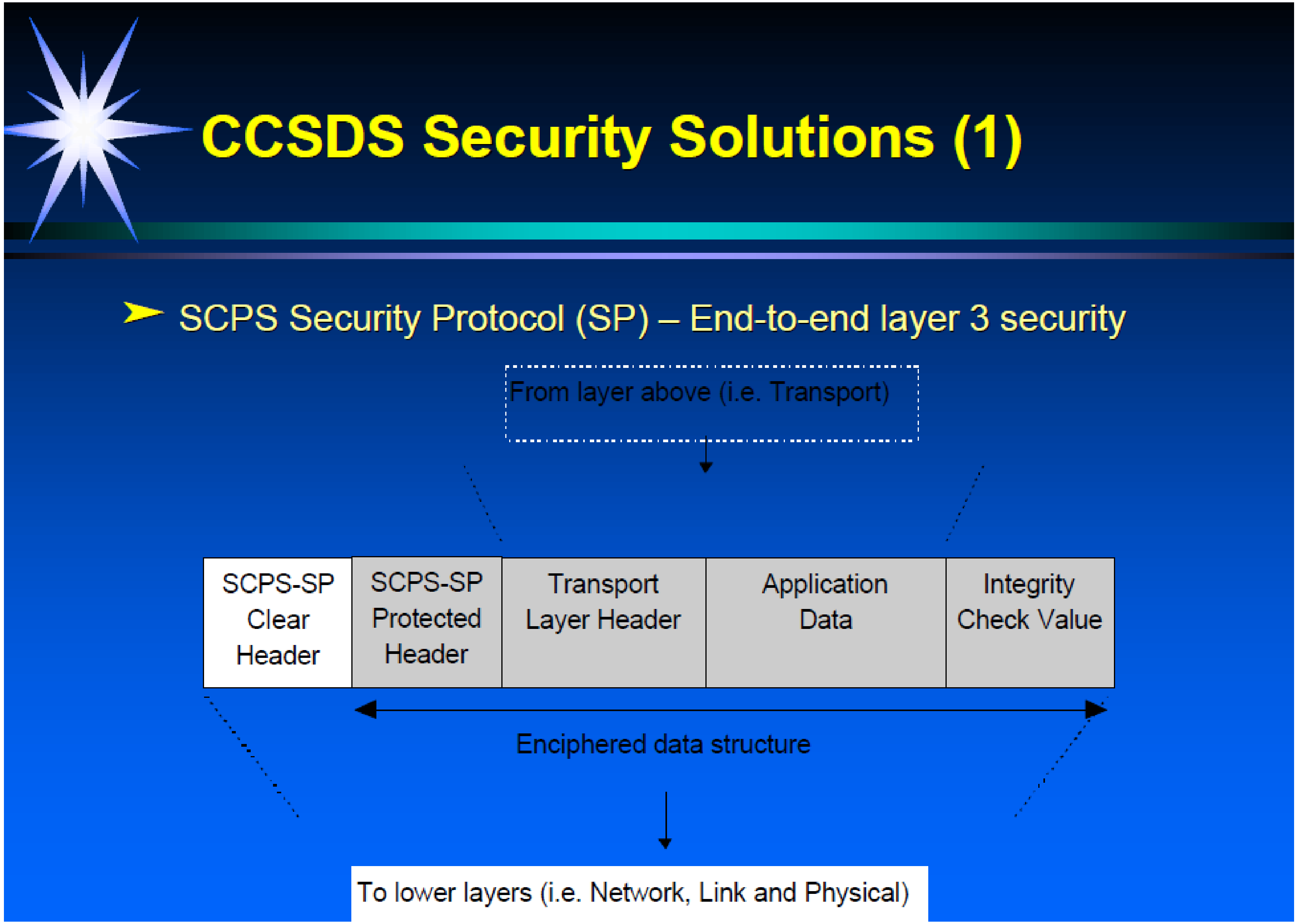
BLUE BOOK

May 1999

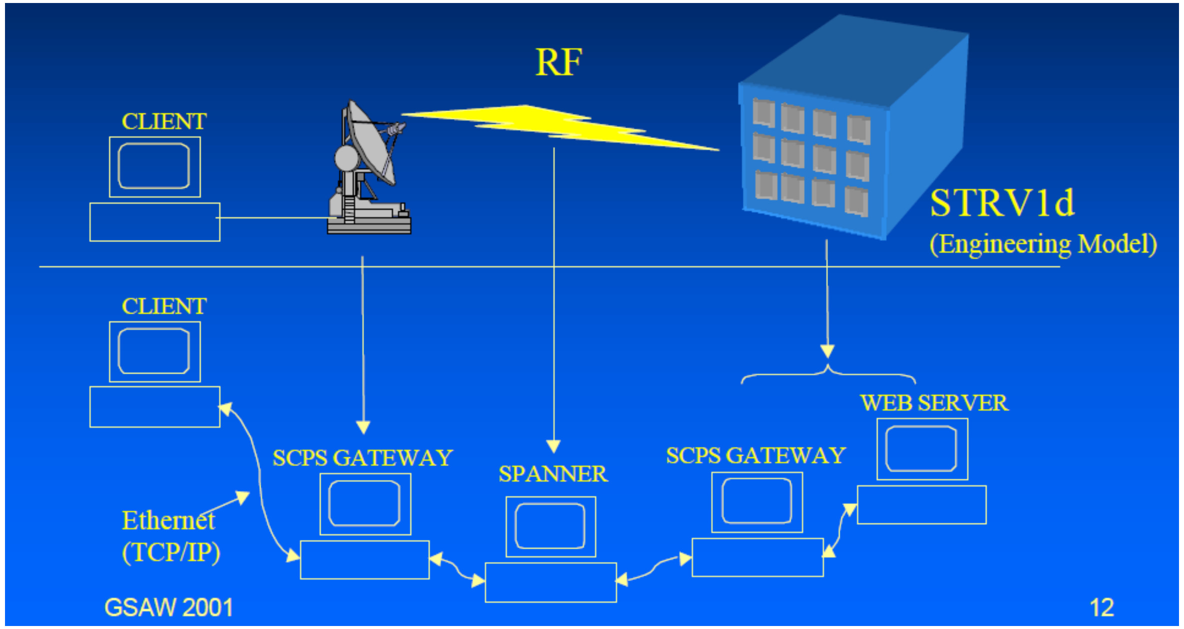
SCPS-SP –SECURITY PROTOCOL

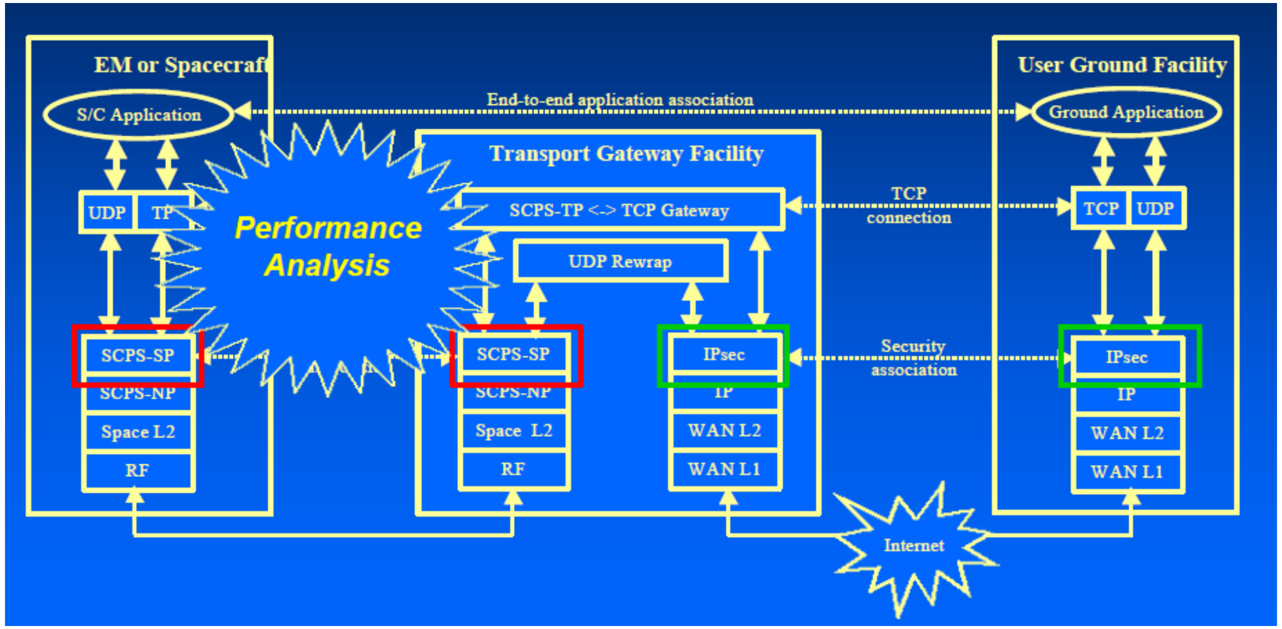
skinny version of IPSec –

- low overhead,
- less bits



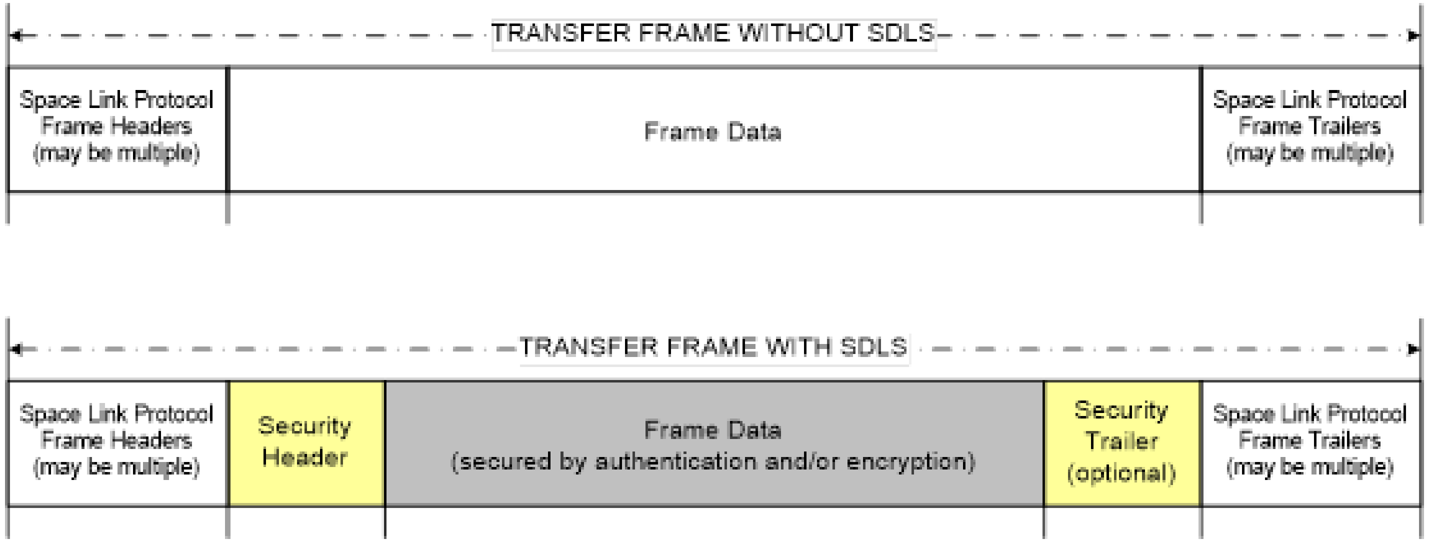
SCPS-SECURITY PROTOCOL TESTING





SPACE DATA LINK SECURITY (SDLS)

- **No standardized security for use with traditional space link layer protocols:**
  - Telecommand (TC)
  - Telemetry (TM)
  - AOS
- **Created a 'security shim' to provide security for existing link layer protocols**

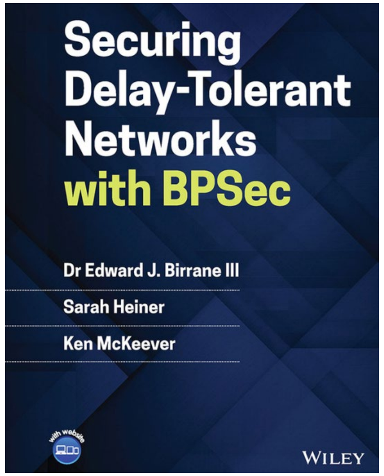


1998: INTERPLANETARY INTERNET/DELAY TOLERANT INTERNET - THE BEGINNING OF BUNDLES

- Initial meeting on interplanetary networking at MCI on 2 February 1998.
- JPL, MITRE, MCI, SPARTA
- 25 years of research and development

INTERPLANETARY NETWORK AKA DELAY TOLERANT (DTN)

- **SCPS provided internet-like capabilities for near-earth**
  - TCP/IP not designed for long-delay environments with intermittent connectivity
  - SCPS provided capabilities - but **not** for deep-space delays or orbital obscurations
- **Next step – Interplanetary Internet (IPN) -> Delay and Disruption Tolerant Networking (DTN)**
  - NASA + CCSDS + IETF + ESA + JAXA + KARI
  - Based on store and forward architecture with assumption of intermittent connectivity
  - Bundle Protocol (BP) Specification (IETF: RFC 9171 (BPv7), CCSDS: 734.2-B (old 2015))
  - Bundle Protocol Security Protocol (BPSec) (IRTF: 6257, IETF: RFC 9172, CCSDS: in progress)
  - Use cases:
    - Deep-space with long delays
    - Intermittent connectivity situations (e.g., no infrastructure)
    - Example Use Cases:
      - Space – lunar and deep-space
      - Terrestrial - sensor networks
      - Minimal infrastructure environments (e.g., 3rd world)



[RFC Home] [TEXT|PDF|HTML] [Tracker] [IPR] [Errata] [Info page]

EXPERIMENTAL
Errata Exist

Internet Research Task Force (IRTF) — S. Symington, The MITRE Corporation
Request for Comments: 6257 — S. Farrell, Trinity College Dublin
Category: Experimental — H. Weiss
ISSN: 2070-1721 — P. Lovell, SPARTA, Inc.
May 2011

Bundle Security Protocol Specification

Abstract

This document defines the bundle security protocol, which provides data integrity and confidentiality services for the Bundle Protocol. Separate capabilities are provided to protect the bundle payload and additional data that may be included within the bundle. We also describe various security considerations including some policy options.

This document is a product of the Delay-Tolerant Networking Research Group and has been reviewed by that group. No objections to its publication as an RFC were raised.

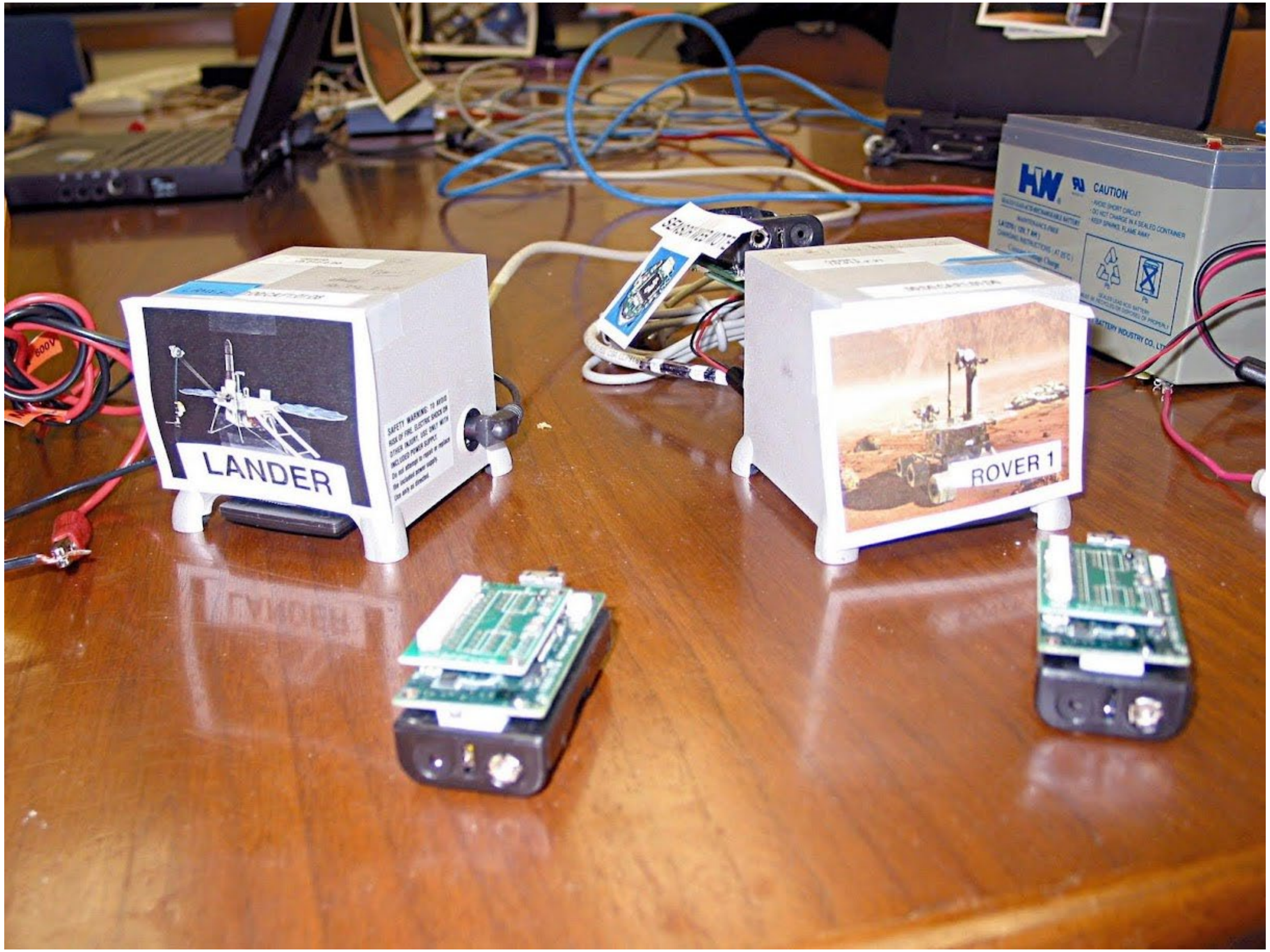
Status of This Memo

This document is not an Internet Standards Track specification; it is published for examination, experimental implementation, and evaluation.

This document defines an Experimental Protocol for the Internet community. This document is a product of the Internet Research Task Force (IRTF). The IRTF publishes the results of Internet-related research and development activities. These results might not be suitable for deployment. This RFC represents the consensus of the Delay-Tolerant Networking Research Group of the Internet Research Task Force (IRTF). Documents approved for publication by the IRSG are not a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6257.

EARLY DESKTOP EXPERIMENTATION OF DTN



PUBLISHED CCSDS SECURITY DOCUMENTS

- Blue Books (recommendations/standards):
  - CCSDS 352.0-B: CCSDS Cryptographic Algorithms
  - CCSDS 355.0-B: Space Data Link Security Protocol
  - CCSDS 355.1-B: Space Data Link Security Protocol Extended Procedures
  - CCSDS 356.1-B: Network Layer Security Adaptation Profile
  - CCSDS 357.0-B: CCSDS Authentication Credentials
- Magenta Books (best practices)
  - CCSDS 350.8-M: Information Security Glossary of Terms
  - CCSDS 351.0-M: Security Architecture for Space Data Systems
  - CCSDS 354.0-M: Symmetric Key Management
- Green Books (rationale/guidance/information)
  - CCSDS 350.0-G: The Application of Security to CCSDS Protocols
  - CCSDS 350.1-G: Security Threats Against Space Missions
  - CCSDS 350.4-G: CCSDS Guide for Security System Interconnection
  - CCSDS 350.5-G: Space Data Link Security Protocol – Summary of Concept and Rationale
  - CCSDS 350.6-G: Space Missions Key Management Concept
  - CCSDS 350.7-G: Security Guide for Mission Planners
  - CCSDS 350.9-G: CCSDS Cryptographic Algorithms

RECENT WINS (2022) (NASA PERSPECTIVE)

NOT MEASUREMENT SENSITIVE

NASA TECHNICAL STANDARD

Office of the NASA Chief Engineer

NASA-STD-1006A

Approved: 2022-07-15
Supersedes NASA-STD-1006 w/Change 1

SPACE SYSTEM PROTECTION STANDARD

APPROVED FOR PUBLIC RELEASE – DISTRIBUTION IS UNLIMITED

[SSPR 1] Programs/projects shall protect the **command stack with encryption** that meets or exceeds the Federal Information Processing Standard (FIPS) 140, Security Requirements for Cryptographic Modules, Level 1.

- *Missions using Consultative Committee for Space Data Systems (CCSDS) should consult CCSDS 350.0-G, The Application of Security to CCSDS Protocols; CCSDS 355.0-B, Space Data Link Security Protocol; and CCSDS 352.0-B, CCSDS Cryptographic Algorithms. Note that FIPS 140 compliance meets and exceeds the cryptographic specifications of CCSDS 352.0-B. All missions should implement CCSDS 232.1-B-2, Command Operations Procedure-1; but by itself, CCSDS 232.1-B-2 is insufficient to meet this requirement.*

THE FUTURE??

France wants to arm satellites with guns and lasers by 2030

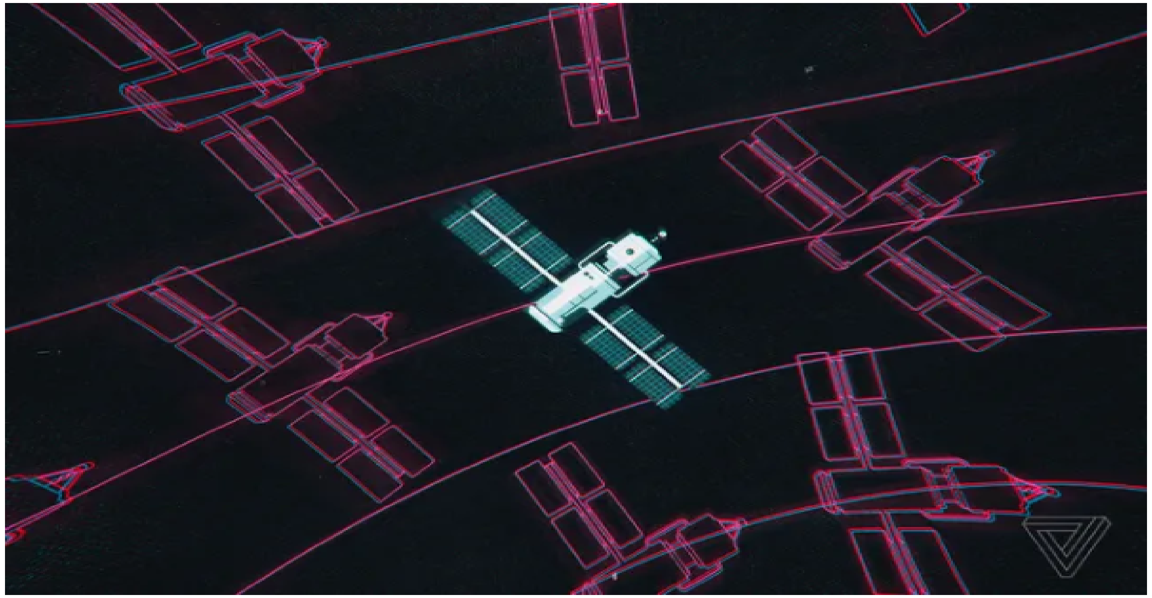


Illustration by Alex Castro / The Verge

/ Just after it announced that it was creating its own Space Command

By Andrew Liptak
Jul 28, 2019, 5:09 PM EDT

0 Comments (0 New)

Earlier this month, French President Emmanuel Macron announced the creation of a French space force that would be responsible for defending its satellites. It looks like they're serious about that: France's Minister of Defense announced a program that would develop nano satellites equipped with guns and lasers, according to *Le Point* (via *Task & Purpose*).

SUMMARY/CONCLUSIONS

- **It's been a wonderful ride!**
- **Civilian space agencies didn't think they needed security, nor did they want it**
- **The Internet changed everything!**
  - Everything was now a target including the civilian science missions that had not been worried about security
- **The Internet was wide open with little or no security (aka, "The Wild West")**
  - IPSEC, IKE, HTTPS, TLS, SSH, SFTP changed that environment –not secure yet but its much better
- **Space was stuck in the 'who cares about us?' perspective**
  - That thought pattern has changed – many new security initiatives! MORE work to be done.
  - Internet security protocols were useful for ground systems
  - New protocols needed for spacecraft beyond the 'traditional' CCSDS link layer protocols
    - SCPS + Security
    - DTN + Security
    - Space Data Link Security (used with 'traditional link layer protocols')
    - Authentication Credentials
    - Key Management

THE END

Questions?
Comments?
Tomatoes? ☺