Space Mission
Communications Security

Nick Shave, Gavin Kenny
Logica UK Limited

Howard Weiss
SPARTA Inc

James Stanier
DERA
Presentation Overview

- Background and Security Issues
- Space Mission Security Requirements
- CCSDS Security Solutions
- The STRV Security Flight Protocol Experiment
- Encrypted CCSDS Space Experiment
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…”
Background

- Current space missions requiring security have bespoke solutions
  - Military space - many missions with many solutions
  - space station, NOAA/Eumetsat, some commercial missions
- SCPS-Security Protocol (SP)
  - first development to standardise security within space missions
  - STRV 1b Testing (1996), SCPS-SP included but limited in scope
- CCSDS link layer security
  - UK Defence Evaluation Research Agency programme
  - has evolved into ECSE payload on STRV 1d
- NASA & IRTF Inter-PlanNet (IPN) internet in space initiative
  - Security is key aspect of this work
Security issues

➢ Space missions need to protect
  » spacecraft and ground equipment
  » information and data contained within the systems
  » communications and data processing services

➢ Space mission security services are very important
  » especially as network interconnectivity increases…
  » ‘shouldn’t wait for a problem to happen’
  » must tailor to space mission application (wide spectrum)

➢ Security standardisation is good
  » enables interoperability and compatibility

➢ Various arguments for location of security in stack
  » application, network, data link/physical?
Generic Threats to Space Missions

- Space Debris
- Interception of Data (theft)
- Hardware Failure
- Software Threats
- Uplink Jamming
- Replay
- Unauthorised Access (Insider/Outsider)
### Example Civil Space Mission Threats:

**International Science Mission**

<table>
<thead>
<tr>
<th>Applicable Threats</th>
<th>Impacts</th>
<th>Probability (1-5)</th>
<th>Security Mechanisms to Counter Threat</th>
</tr>
</thead>
</table>
| Unauthorised Access        | • Disruption of operations  
                           • System damage  
                           • Potential loss of mission  | 3                 | • Authentication of commands  
                           • Access control in control centre  
                           • Access control in cross support network  
                           • No use of open networks |
| Interception of data       | Loss of proprietary data                     | 1                 | Encryption                                                                 |
| Software threats           | • Undesirable events  
                           • System damage  | 1                 | • Evaluation  
                           • COTS product use |
Security- services & mechanisms

» Data Confidentiality
  » implemented by encryption

» Authentication
  » can be implemented by adding a unique digital signature to the user data unit that cannot be created by an unauthorised entity

» Data Integrity
  » can be implemented by including an integrity check value with the data which is computed from the data itself

» Access Control
  » achieved via establishing user information bases with details of access rights and utilisation of other services (e.g. authentication)
  » needs effective password administration
  » Not supplied by basic IPsec or SCPS-SP
SCPS Security Protocol (SP) – End-to-end layer 3 security

From layer above (i.e. Transport)

SCPS-SP Clear Header  SCPS-SP Protected Header  Transport Layer Header  Application Data  Integrity Check Value

Enciphered data structure

To lower layers (i.e. Network, Link and Physical)
CCSDS Security Solutions (2)

Data Link Security – Point-to-point ‘conventional’ Layer 2 packet TM/TC security
STRV 1d (DERA microsat, launched Nov 2000)

Security Demonstration Objectives

- Demonstrate integrated security in space mission data systems
  - establish Space VPN (SVPN)
  - develop space mission security confidence in **public domain**
  - show security options enable tailoring to mission application

- SCPS-SP and IPsec performance comparison
  - primarily efficiency comparison in flight environment
  - evaluate different system configurations
  - evaluate different security service options (e.g. AH, ESP,...)

- Demonstrate link security and network layer security interaction

- Contribute to ‘baseline security platform’ for other agencies and organisations to participate
STRV Security Protocol Demo - architecture options: End-end IPsec

**Windriver IPsec Implementation**

Algorithm: DES

**COTS IPsec Implementation**

End-to-end application association

TCP connection

End-to-end security association

**EM or Spacecraft**

S/C Application

UDP

TCP

IPsec

IP

Space L2

RF

**User Ground Facility**

Ground Application

TCP

UDP

IPsec

IP

VPN

Internet

Windriver IPsec Implementation

Algorithm: DES

COTS IPsec Implementation

Link Layer Security (ECSE)
STRV Security Protocol Demo - architecture options: Trusted gateway

Performance Analysis

EM or Spacecraft
- S/C Application
  - UDP
  - TP
- SCPS-SP
- SCPS-NP
- Space L2
- RF

Transport Gateway Facility
- SCPS-SP
- SCPS-NP
- Space L2
- RF
- UDP Rewrap
- IPsec
- IP
- WAN L2
- WAN L1

User Ground Facility
- Ground Application
  - TCP
  - UDP
  - TCP connection
  - IPsec
  - IP
  - WAN L2
  - WAN L1

Internet

End-to-end application association

Security association
STRV Security Protocol Demo - architecture options: 
End-end SCPS-SP via trusted SCPS gateway

**Transport Gateway Facility**

- SCPS-TP <-> TCP Gateway
- UDP Rewrap

**Performance Analysis**

- End-to-end application association
- Security association
- TCP connection

**User Ground Facility**

- TCP
- UDP

**EM or Spacecraft**

- S/C Application
- SCPS-SP
- SCPS-NP
- Space L2
- RF

**Ground Application**

- SCPS-SP
- IP
- WAN L2
- WAN L1
The Encrypted CCSDS Space Experiment (ECSE) Objectives

- Aim of ECSE is to build on testing of the secure CCSDS protocols by providing a demonstration platform onboard STRV1d whilst satisfying requirements for the UK MOD.

- Objectives of ECSE are to demonstrate operation of:
  - ESA Packet Telecommand encrypt/decrypt, authentication, validation and anti-replay attack
  - ESA Packet Telemetry encrypt/decrypt functionality
  - Extraction of security management functions onboard the spacecraft and simplified processing of these security management functions

- First flight implementation the CCSDS Data Link Layer security solution
ECSE: Current Status

- ECSE has been developed by DERA and Astrium
- Functionality of ECSE demonstrated on ground testbed including encrypt/decrypt, authentication and validation
- Currently being flown onboard STRV1d
- Telemetry at 10kbit/s, telecommand at 1kbit/s
- Software is currently being modified to accept full encrypt/decrypt capabilities
- Additional aim is to implement SCPS protocols (including SCPS-SP) over the CCSDS link layer security system
DERA STRV Spacecraft Launched Nov 2000 (Ariane 5)

- After approx. 1 month, TC receiver anomaly on both spacecraft
  - Currently attempting to recover mission

Security Protocol Flight Demo currently limited to ground-based performance analysis using Logica/SPARTA SCPS reference implementations:

- Good ‘science’ still possible
- SCPS-SP and IPsec performance comparison
- Various security configurations and service options to be evaluated
- Different algorithms (MD5?)
- Plans to investigate key management aspects
- Link up to DERA Engineering Model STRV via Net (TBC)
Future Developments

- STRV ground-based Security Demo completed in May 2001
  - Future paper will be published
- New concepts and configurations for space mission security will be demonstrated
  - IPsec
  - SCPS-SP
  - End-to-end security (remote ground station to spacecraft)
  - Trusted SCPS Gateway
  - Key management aspects (TBC)
- Possibilities for future flight demonstration to be investigated
- CCSDS plans are developing to integrate security further with the space mission data system standardisation architecture