How Secure are Our Satellites?

Richard Jaenicke
Director, Marketing
Safety & Security-Critical Products




Audience Survey - Satellite Vulnerability

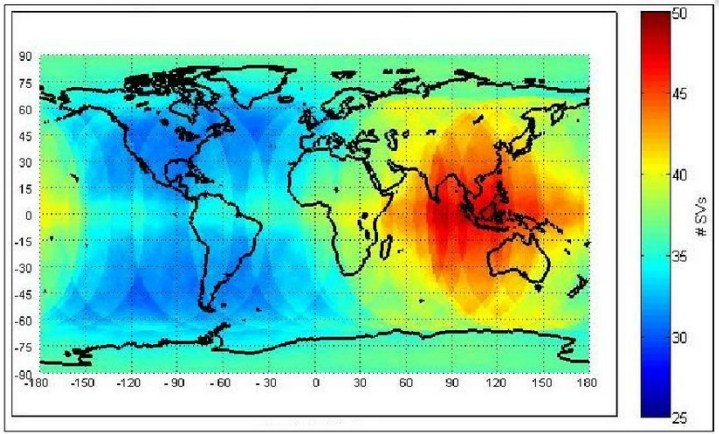
Do you agree or disagree with these statements?

- Most satellites in operation are older, long before software-defined architectures, making them less vulnerable to hacking.
- If GPS satellites were compromised, it's not that big of a problem because we could get by using paper maps or digital map databases without real-time GPS input.
- Data sent to and from a satellite is secure because most satellites encrypt communications.
- If a hacker does get inside a satellite, then they can pretty much do what ever they want, from covertly altering the data to disabling the satellite.

GPS for Navigation

Modern navigation includes

- Map database
- Real-time location ← GPS
- Real-time traffic
- Real-time weather (flight sys)



Average # of visible GNSS satellites

[Rizos, Higgins, Johnston 2010]

Global Navigation Satellite Systems (GNSS):

GPS (US), Glonass (Russia), Galileo (EU), BeiDou/Compass (China)
regional: IRNSS (India), QZSS (Japan)

Satellite-Based Augmentation System (SBAS)

WAAS (US-FAA), WAGE (US-DoD), EGNOS (EU), GAGAN (India), MSAS (Japan), SDCM (Russia)
Commercial: Starfire, Starfix/OmniSTAR, Atlas

We Depend on Satellites

GPS

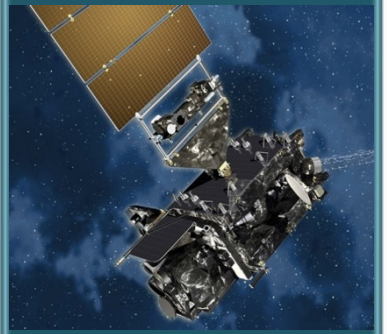
Precise Timing

- Navigation
- Financial
- Power Grids
- Internet

Comms

- TV Uplinks & Subscriptions
- Voice for Airborne & Remote Areas

Weather

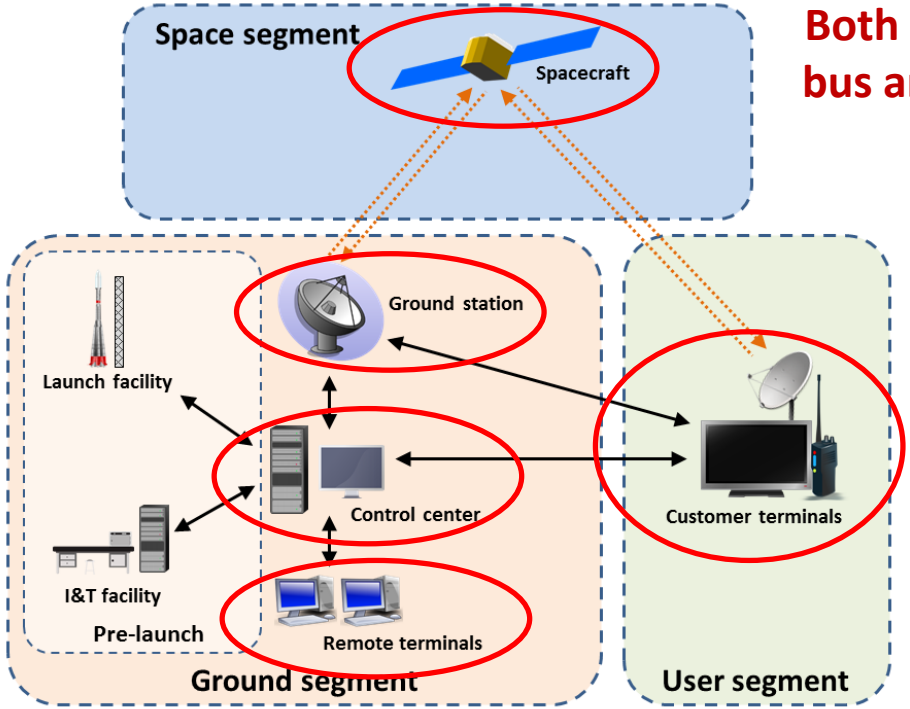


- Agriculture
- Public Safety
- Transportation

Imaging

- Agriculture
- Military
- Intelligence
- Arms Control

Satellite Vulnerability



Both spacecraft bus and payload

Satellite Attack Vectors

- **Physical attack**
  - Anti-satellite missile
  - “Inspector” satellite
- **Electro-Magnetic (EM) attack**
  - Jamming, EM pulse, etc.
- **Cyber attack**
  - from ground station
  - fake ground station
  - another satellite
- **Supply chain**

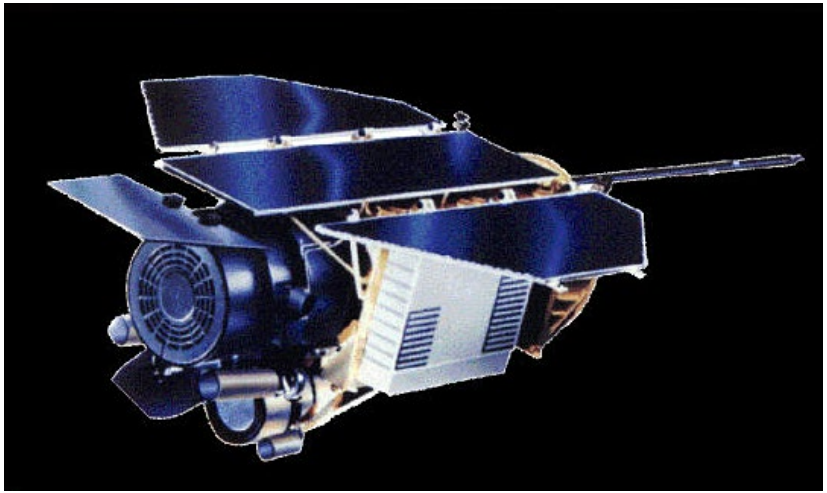
Long History of Satellite Hacking

One of the earliest:

- **1998 blinding of US-German ROSAT**
  - Intrusion at Goddard by Russian hackers

More recently:

- **2014 hack of a weather satellite server**
  - Chinese attack on NOAA server caused a 2-day outage



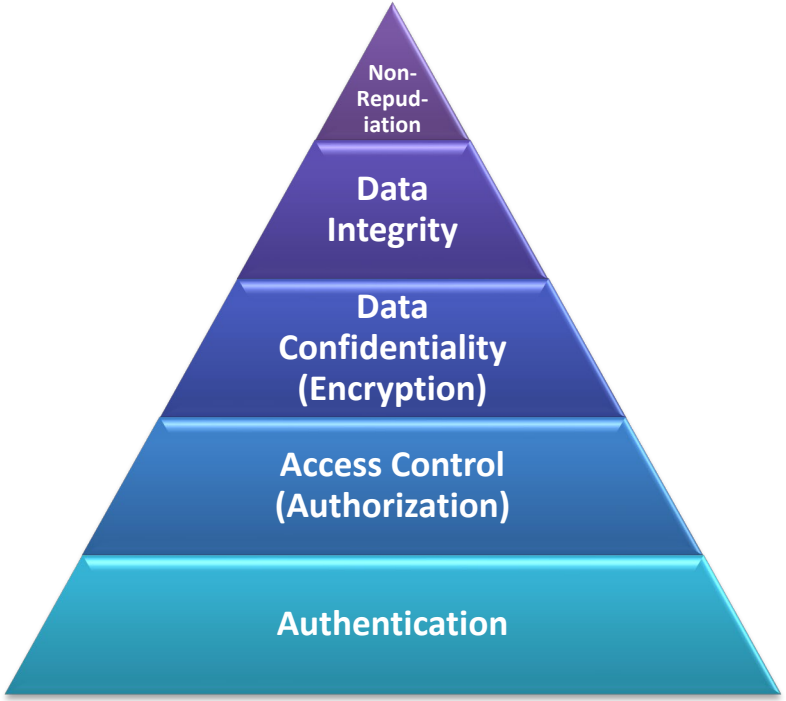
ROSAT Satellite X-ray Telescope

Security Responses

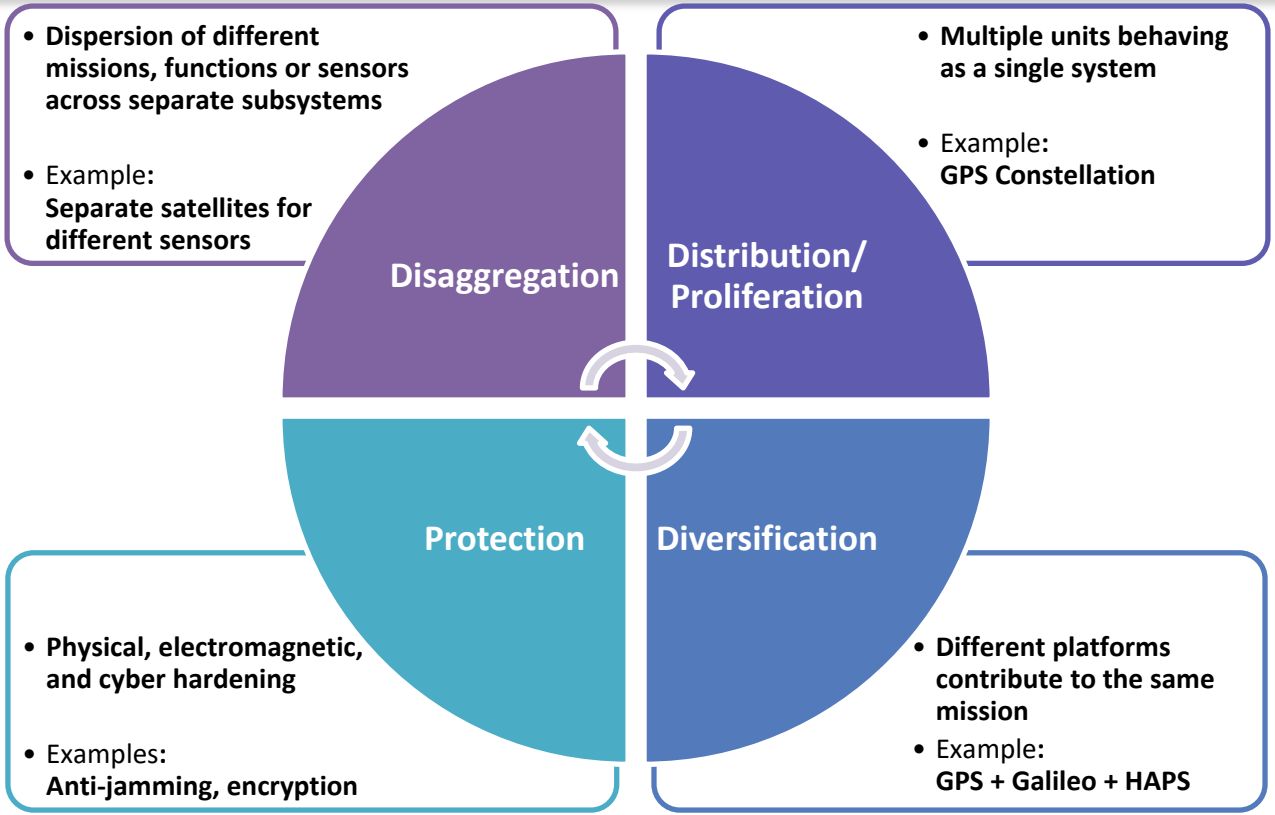
- **Physical**
  - Maneuverability, active defense
- **EM**
  - Anti-jamming, EM hardening
- **Cyber**
  - Real-time anomaly detection
  - apply general InfoSec (ISO 7498-2)

→ **Too hard to ensure survivability, so change to resilience**

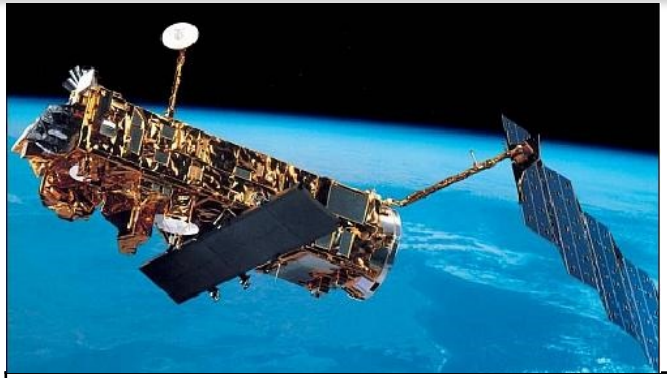
ISO 7498-2 Security Services

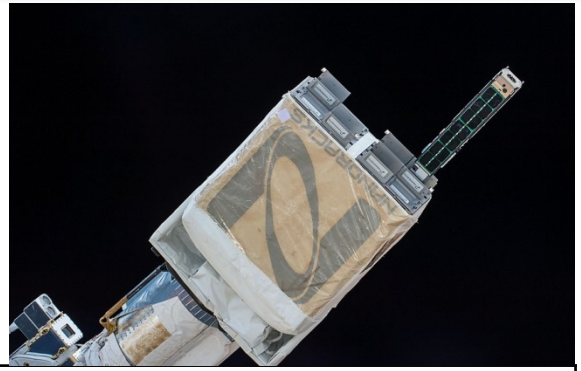


Achieving Satellite Resilience



Trends from Resilience Goal



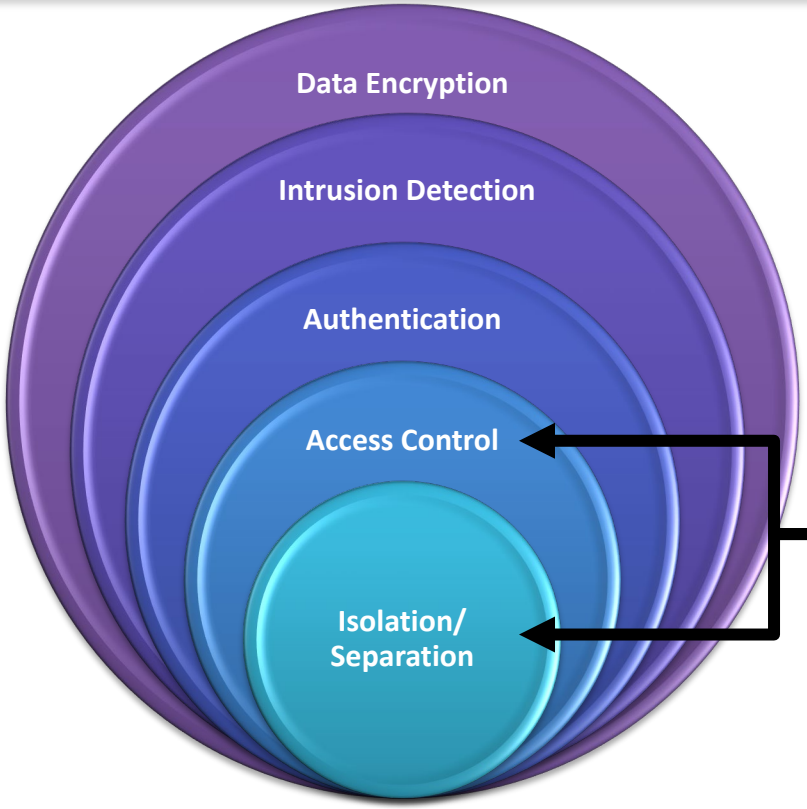


Large, multi-function satellites	→	Smaller, less expensive satellites, deployed in clusters
Complex proprietary architectures	→	Rapid technology insertion
Built for 15-20 year life spans	→	Shorter life spans and more frequent launches
Designed for safety and survivability	→	Recognized need to detect cyber intrusion and isolate

Implications for Embedded Technology

Smaller satellites	• Reduced SWaP → less memory and multiple functions per processor
Shorter life span	• Reduced cost → COTS hardware and software →supply chain risks
Higher number of satellites	• Can distribute NRE over larger group
Rapid technology insertion	• Modular open system architecture, including security architecture
Need for cyber intrusion detection and isolation	• Can't punt on security requirements

Satellite Information Security Layers



Security Required for all parts:

- Spacecraft (Bus)
- Payload
- Ground Station

INTEGRTY™-178
Separation Kernel

The only COTS OS certified to NSA's Separation Kernel Protection Profile (SKPP)

Example New Satellite: GPS III

- GPS Mission Data Unit is 70% digital
- 3x more accurate
- 8x better anti-jam capability
- Design life of 15 years
- Compatible with L1C
  Global Navigation Satellite System (GNSS)
- “Designed to evolve to incorporate new technology and changing mission needs”

Audience Survey - Satellite Vulnerability

Green Hills SOFTWARE

Do you agree or disagree with these statements?

- Most satellites in operation are older, long before software-defined architectures, making them less vulnerable to hacking. **No, they have less security, making them easier to hack.**
- If GPS satellites were compromised, it's not that big of a problem because we could get by using paper maps or digital map databases without real-time GPS input.
  No, GPS timing signals are critical for financial transactions, power grids, and more.
- Data sent to and from a satellite is secure because most satellites encrypt communications. **Yes, most satellites fielded after 2008 use some encryption.**
- If a hacker does get inside a satellite, then they can pretty much do what ever they want, from covertly altering the data to disabling the satellite.
  Yes, unless they use an NSA-level separation kernel like INTEGRITY-178 tuMP.