Improving the Cyber Resiliency of the F Prime Flight Software Framework

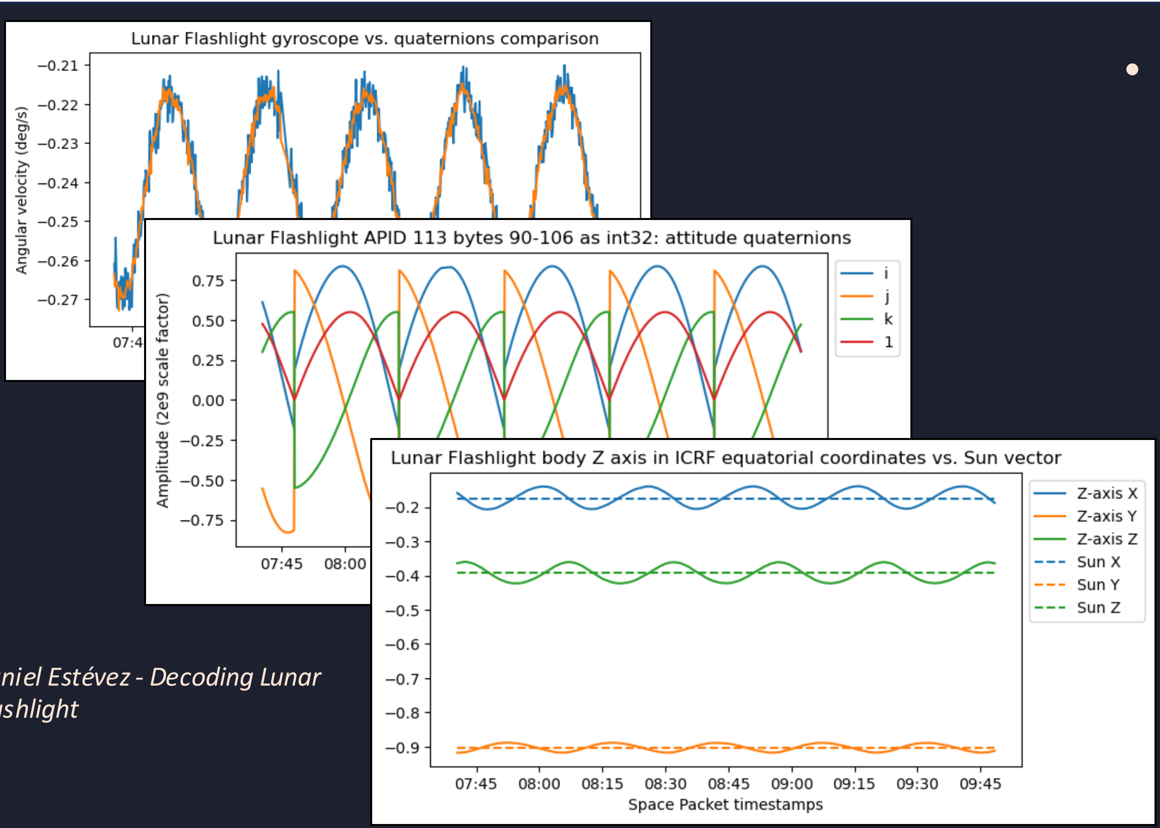
Steven Doran
NASA Jet Propulsion Laboratory

Jet Propulsion Laboratory
California Institute of Technology

Why Should You Care About Cybersecurity?

- Satellite's will have to operate in an increasingly contested Cybersecurity Environment
  - Small Satellites are extremely vulnerable to malicious attacks due to their limited budgets and their use of open-source software and COTS hardware
  - Small Satellites have transitioned from research and prototyping to providing services used by millions of users (Earth Monitoring, Internet Access, Military Applications, etc.)
  - The approach of ”security by obscurity" and “were a university not a nation-state” is obsolete

Who's Watching?


Lunar Flashlight gyroscope vs. quaternions comparison

Lunar Flashlight APID 113 bytes 90-106 as int32: attitude quaternions

Lunar Flashlight body Z axis in ICRF equatorial coordinates vs. Sun vector

Daniel Estévez - Decoding Lunar Flashlight

- Who is monitoring your Satellite and what are their intentions?
  - 2008/2009 Landsat-7/Terra EOS AM-1
  - 2022 – Viasat
  - 2022 – Lunar Flashlight Decoded by Amateur Radio Enthusiast

F’ FSW Framework Cybersecurity Roadmap

- The increased adoption of JPL’s F’ FSW Framework by both Universities and NASA is an opportunity For F’ to lead in defining a standard for a minimum level of cyber resiliency in both current and future Small Sat missions
  1) Automated generation of Software Build of Materials (currently manual)
     - Identify F’ software supply chain
     - Scan for known vulnerabilities
  2) Daily static code analysis on F’ software source repository
  3) Penetration testing against F’ on a representative testbed to find cyber vulnerabilities

F’ FSW Framework Cybersecurity Roadmap (cont.)

- Future Planned Improvements
  1) Implement the Consultative Committee for Space Data Systems (CCSDS) Space Data Link Security Protocol (SDLS) as default
     - Removes common vulnerabilities that are easily exploited: man-in-the-middle attacks, spoofing, replay attacks, etc.
  2) Implement standard Uplink Encryption w/ key management
     - AES-GCM encryption standard
  3) Implement a more verbose logging for intrusion detection
     - Monitor system health and operations in order to prevent an attack if other security standards fail (Defense in depth)

F’ FSW Framework Cybersecurity Roadmap (cont.)

- Future Planned Improvements (cont.)
  4) Randomize command opcodes for each F’ Deployment
     - Prevents missions from using default opcodes that are open source
     - Reduces Remote Code Execution (RCE)
       - RCE vulnerabilities are vulnerabilities that are commonly rated a 9-10 on a scale of 1-10 in the CVE standard
  5) Develop a standard operating procedure for cybersecurity
     - Educate the Small Sat community on best-practices for for a cyber-resiliency
     - Reduces the burden on Small Sat missions to use vital resources on cybersecurity where an implementation of such practices has already been done

Jet Propulsion Laboratory
California Institute of Technology