Cybersecurity Analysis Challenges of Legacy Ground Data System©

Adans Y. Ko, Thea Nudo, Karen Liao, Brian Kahovec
Jet Propulsion Laboratory, California Institute of Technology
4800 Oak Grove Dr., Pasadena, CA. 91109
adans.Y.Ko@jpl.nasa.go,
thea.g.nudo@jpl.nasa.gov,
karen.g.liao@jpl.nasa.gov,
brian.j.kahovec@jpl.nasa.gov
rick.t.hoang@jpl.nasa.gov

Overview

Most of the legacy space missions operated on a decades-old Ground Data System (GDS). Unfortunately, decades ago, IT security design is done separately from the design of GDS' mission operational capabilities. This incoherent practice left many security vulnerabilities without notice in an extended mission phase mission. Identifying the vulnerabilities that may exist in a legacy GDS becomes urgent. Unknown threats can exploit the mission operation without knowing the cybersecurity vulnerabilities. The threats can affect one or all of the GDS capabilities. For example, tampering with spacecraft commands, unauthorized use of a system to create unwanted science products, and disrupting a command uplink. The consequence can cause a mission to end with losing the spacecraft. However, it is a daunting task to perform a cybersecurity risk assessment on a decades-old system.

Mars Science Laboratory Project (MSL) mission, the Curiosity rover launched on November 26, 2011, landed on Mars on August 5, 2012, and looked for evidence of an environment that supported microbial life on Mars. To support MSL's mission operations, a substantially complex GDS was developed before launch over a decade ago [1] (see Figure 1: Sample Generic In-situ Rover and Lander GDS Diagram).

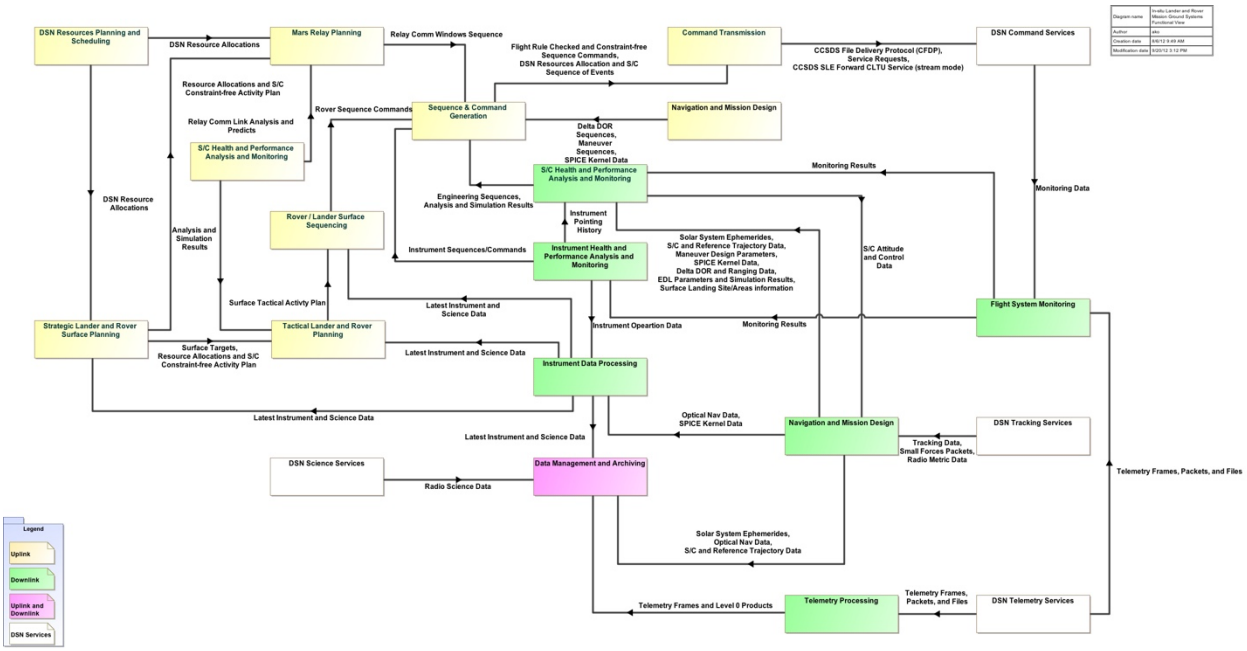

Figure 1: Sample Generic In-situ Rover and Lander GDS Diagram

Challenges

We have learned many challenges that prohibit us from adequately analyzing a legacy mission's GDS to conduct its cybersecurity risk assessment from the recent cybersecurity risk assessment for MSL GDS [2].

The major challenges to conducting a legacy mission's cybersecurity analysis are: 1) A typical project resources are allocated in the spacecraft health and safety, science return, and operational efficiency areas over cybersecurity engineering. 2) GDS design and engineering documents are antiquated or missing. 3) Mission GDS subject matter experts left the project for many years. 4) False sense of acceptable cybersecurity risks in mission GDS.

Exploits

Many legacy missions stay with end-of-life hardware and unsupported third-party software with their legacy applications. In addition, the absence of software security design when the GDS was developed more decade-old made the mission GDS extremely vulnerable to cyber threats. Without a deep dive and effective cybersecurity system analysis, the missions' potential cyber threats are unknown. One of the common exploits is caused by a software design flaw. The following kernel software flaw caused a cyberattack on Google android is an example of a

software error design exploit.

The CVE-2015-1805 was a flawed implementation of the pipe_read and pipe_write implementations in fs/pipe.c in the Linux kernel before 3.16. The incorrect code calls may result in memory corruption due to an overrun IO vector array. It will allow Android phone users to exploit this vulnerability to cause a denial of service or escalate users to gain root privileges via a rootkit-like application[3]. Google has confirmed Nexus 5 and Nexus 6 devices were abused by a rooting app that can be downloaded on the internet that can escalate root privileges for an Android phone user[4]. This vulnerability was rated as a critical severity issue because an actor can execute malicious code by escalating it with a root privilege[5]. Use of a rooting application, an untrusted party triggers the vulnerability by executing the problem codes with a root privilege. Hence, they can load a malicious program and manage to exploit the system to its full extent. The following is an example of the use of the publicly available rooting tool, the KingoRoot app, to exploit a system's vulnerabilities, escalating users with root privileges on an Android phone. A similar exploit is due to a software security error in a legacy mission GDS, which can cause a temper mission support data, execution of unauthorized mission software, or tamper spacecraft commands. The worse consequence may cause a mission loss of the spacecraft.

Conclusion

The number of IT security vulnerabilities increased four times in the past decade[6] (See Figure 2). It is significant for space missions to know their cybersecurity risk posture and keep the status current. A design for mission GDS must include cybersecurity requirements from the physical layer to the operations layer. Apply vulnerability fix patches often. Do not stay with unsupported hardware and software. Account for the cybersecurity design and sustaining in the budget.

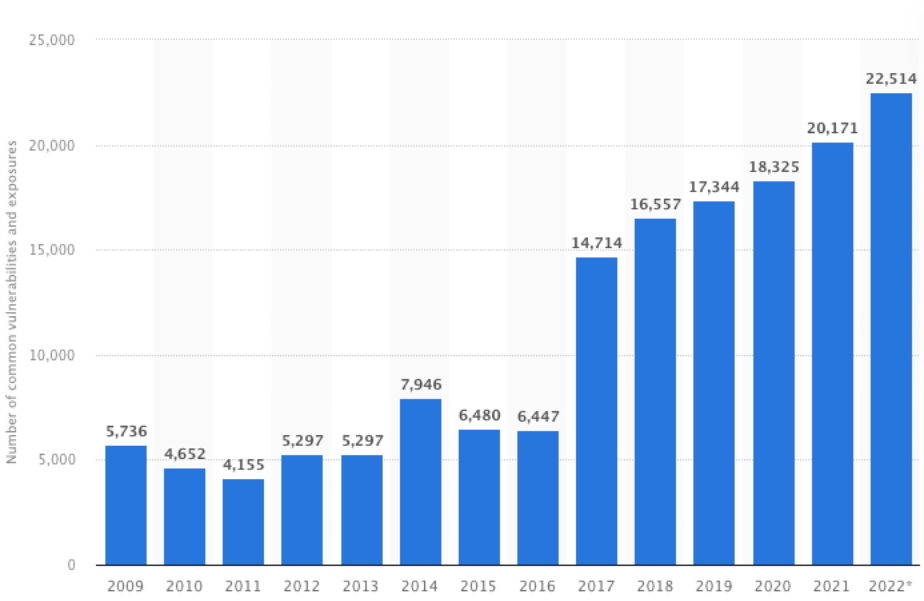

Figure 2: Number of common IT security vulnerabilities and exposures (CVEs) worldwide from 2009 to 2022

Acknowledgement

The research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration (80NM0018D0004).

Reference:

[1] A. Y. Ko and M.Vogt, "The Present and Future of AMMOS Mission and Planning and Sequencing System", June 2006, SpaceOps Conference, Rome, Italy.

[2] Gary Stonebumer, Alice Goguen, and Alexis Feringa, Risk Management Guide for Information Technology Systems, July 2002. Pp. 8 - 26, National Institute of Standards and Technology Special Publication 800-30.

[3] https://www.cve.org/CVERecord?id=CVE-2015-1805

[4] https://source.android.com/docs/security/bulletin/advisory/2016-03-18

[5] https://www.zimperium.com/blog/zimperium-applauds-googles-rapid-response-to-unpatched-kernel-exploit/

[6] https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/