Cyber Threat Assessment of Uplink and Commanding System for Mission Operation

Mr. Adans Y. Ko
Mission Operations Assurance Manager
Dr. Kymie M. C. Tan
Ground System Engineer
Mr. Ferner Cilloniz-Bicchi
Software Security Engineer
Mr. Grant Faris
Chief Mission Operations Assurance Manager
Jet Propulsion Laboratory, California Institute of Technology
4800 Oak Grove Dr.
Pasadena, CA. 91109
Adans.y.ko@jpl.nasa.gov
Kymie.Tan@jpl.nasa.gov
Grant.Faris@jpl.nasa.gov

Most of today's Mission Operations Systems (MOS) rely on Ground Data System (GDS) segment to mitigate cyber security risks. Unfortunately, IT security design is done separately from the design of GDS' mission operational capabilities. This incoherent practice leaves many security vulnerabilities in the system without any notice. This paper describes a new way to system engineering MOS, to include cyber threat risk assessments throughout the MOS development cycle, without this, it is impossible to design a dependable and reliable MOS to meet today's rapid changing cyber threat environment.

I. Introduction

A typical GDS implements its IT security capabilities without any knowledge of the system's characteristics and risks. By in large, most of the GDSs use a "cookie cutter" approach for their implementation, for example, a one-size-fits-all firewall and VPN solution to secure its perimeters, to keep attackers outside the GDS system. It is very common to find out islands of credential databases were used in mission operation, to authenticate and authorize users, in which, duplicates of user credential records, inconsistent user profile updates, and negligence of user account decommissions are a few of many problems due to this error-prone design. Lastly, a Secured SHell (SSH) mechanism is used to secure data (a.k.a. transport layer security), however, this does not address threats to data confidentiality and data integrity. The protection of data is one of the essential reasons to keep attackers away from stealing mission critical data and intellectual property [1,2].

This paper presents the recent work on the cyber threat risks assessment for an uplink system in a typical MOS. An uplink system usually comprises of mission planning, S/C and ground resource management, sequence and command generation, and command radiation. The results of the risks assessment illustrate the benefits of accounting cyber threat risk assessments to build a dependable and reliable GDS.

II. Purpose and Scope

The purpose of this risk assessment task is to identify the vulnerabilities that may exist in a spacecraft's uplink communications and its supporting ground infrastructure services, to determine if those vulnerabilities can be exploited within the current threat environment. This effort will identify the threats capable of exploiting such vulnerabilities, the likelihood of threat occurrence, the resulting mission impact, and the safeguards/countermeasures required to mitigate the risks presented by those vulnerabilities.

III. Approach and Methodology

The approach for this assessment follows the method put forward by the National Institute of Standards and Technology in its Special Publication 800-30 - "Risk Management Guide Information Technology Systems" [3].

A. System Characterization

An uplink and commanding system [4,5] plays a critical role in NASA flight projects, in particular, it provides mission scientists and engineers with science and mission planning, sequencing, command translation, and on-board command execution capabilities, allowing them to successfully plan, command, control, and execute their science and mission objectives. Project scientists use mission and science planning tools to search and analyze science opportunities; the results from these searches will lead them to plan science observations and science experimental activities.

The mission planning and sequencing capabilities include spacecraft and ground constraints checking and resource management. A view of mission plans, resource profiles, and observation targets' image footprints are depicted to scientists for their final confirmation of the science activities that will be performed on the spacecraft (S/C).

Project engineers use sequence and commanding tools to design engineering activities to perform varies activities, for example, S/C telecom subsystem configuration to receive uplink commands and downlink science and engineering data, S/C navigation and guidance and control, and S/C health and safety monitoring.

These science and engineering activities are translated into command sequences and they are verified against a set of spacecraft flight rules and constraints, and resources allocations. Finally, the constraint- free sequences are compiled as on-board programs, to be uplinked and executed onboard.

In Figure 1, it illustrates an example of a critical uplink path (connection lines in red), which starts with resources scheduling, mission planning, sequence generation, command translation, and command uplink to the S/C. A sample set of mission critical data are also illustrated in Fig. 1 with yellow-colored boxes and-beige colored boxes with red text.

A sample set of mission critical data:

i. Deep Space Network (DSN) Station Passes
ii. DSN View Periods
iii. DSN Resources Allocation
iv. Science and Engineering Activities
v. Conflict-free Mission Plan (aka Integrated mission Activity Plan)
vi. Science and Engineering Sequence
vii. Verified Integrated Sequence
viii. Command Packet File.

B. Threat Identification

Three potential threats are capable of undermining a mission, via an uplink system infrastructure. The threats and vulnerabilities described here are based upon a conceptual uplink system in a reference mission.

- Tampering with S/C commands:
  - Create malicious commands that may be sent to the S/C.
- Tampering with mission support data
  - Use of incorrect input values for mission and science product generation.
- Unauthorized use of uplink system
  - Create unwanted mission and science products.

C. Vulnerability Identification

In general, cyber attackers spend most of the time to collect data from a target system. Attackers follow an attack vector, which is a path to hack into a target system, using various cyber attack tools. Their goal is to find the vulnerabilities in target system (weakest link) from attack vector, to penetrate the target system and launch their attacks.

The following example illustrates use of attack vector to identify an uplink system's vulnerabilities:

- Bypass Perimeter:

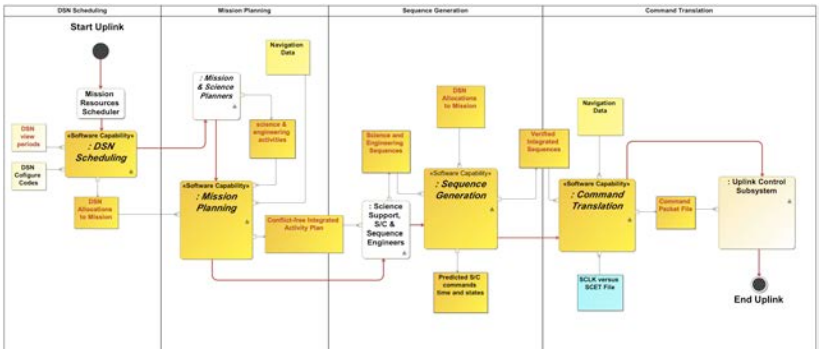

Figure 1 Uplink System Control and Data Flow

- Vulnerability: Break into mission operation firewalls.
- Resources available: Air-Crak, Cain and Abel, Pwdump, etc.

- Establish Presence:
  - Vulnerability: Impersonate as a mission user to access MOS. Identify vulnerable uplink server.
  - Resources available: wireshark, snort, Dsniff, etc.
- Execute Attacks:
  - Vulnerability: Intercept and collect mission data. Execute uplink software.
  - Resources available: Exploit Database, SNational Vulnerability Database, CERT Vulnerability, etc.
- Maintain Presence:
  - Vulnerability: Attacker's payload (virus) stays in MOS without notice. Setup backdoors.
  - Resources available: Rootkis.

Another set of uplink system vulnerabilities can be observed by actual mission operation. For examples: 1) Malicious commands created, undetected, and executed onboard; 2) Malicious commands created but detected and recovered; 3) Malicious mission support used to generate uplink products; 4) Uplink software was used to generate unwanted uplink products.

D. Control Analysis

In order to prevent and mitigate a myriad cyber security risks. The Multi-Mission Ground Systems and Services organization in Jet Propulsion Laboratory (JPL) has started to implement common security services, to counter-measure the potential cyber threats to NASA deep space missions [6]. The services will be a centralized and configurable to a mission without individually implemented by each project. Examples of the common security services are:

1. ID Management:
   a) Strengthen "attacker bypass perimeter" and "establish presence" positions in the attack vector.
   b) Implement VPN and VIP.
   c) Provide ID Management core services to missions: Manage distributed (local and remote) identity data from a centralized service.
   d) Authentication and authorization, such as: Manage user ID/Password (or PKI credentials) with group / role based associated permissions.
   e) Automatic temporary password reset.
2. Protect information confidentiality & integrity (management of settings/rules):
   a) Strengthen "execute attacks" position in the attack vector.
   b) Encryption & integrity checking of data.
   c) Encryption & integrity checking of Message transactions (via Message bus).
3. Enforce and execute security policies and decisions:
   a) Strengthen all positions in the attack vector.
   b) Restriction on number of login attempts (management of platform security settings).
   c) Web Page posting restrictions (management of Web container permissions)
   d) Protect cross-site hacker attacks, e.g. Denial of Service attacks (management of patches & security settings)
4. Inter-centers Federated Security Service [7]
   a) Strengthen "attacker bypass perimeter" and "establish presence" positions in the attack vector.
   b) Cross-domain authentication and authorization mechanisms to support sharing of services.

E. Likelihood Determination

The likelihood that a potential vulnerability could be exercised by a given threat-source can be described as high, medium, or low. The standard DREAD model [8] is a collection of five key areas that are used to assess both the likelihood of attack and the mission impact:

1. Reproduce-ability
2. Exploitability
3. Discoverability
4. Damage potential,
5. Affected entity

Each threat is given a score (3, 2, or 1) for each of the attributes: Tables 1-1, 1-2, and 1-3 illustrate the outcome of likelihood determination of attack to an uplink system. The mission impact assessment will be discussed in the next section (F. Impact Analysis).

To derive an overall likelihood rating that indicates the probability that a potential

vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered: Threat-source motivation and capabilities; Nature of the vulnerability; Existence and effectiveness of current controls.

Criteria	High (3)	Medium (2)	Low (1)
Reproduce-ability		Attacker randomly edits the S/C command file.	Attacks with perfect timing in the uplink process and in-depth knowledge with S/C commands.
Exploitability		Attacker understands of uplink and assembly programming skill, to retrieve the right file type.	A skillful attacker with in-depth domain knowledge in uplink operation process, ground data system, and DSN, in order to achieve this attack.
Discoverability	Access to specific command sequences at the right time, with the matching meta data, and in the exact database.	Access to a specific target command sequences are verified throughout uplink plan and sequence generation phases.	

Table 1-1 Tampering with S/C Commands Likelihood Determination Matrix

Criteria	High (3)	Medium (2)	Low (1)
Reproduce-ability		Attacker randomly retrieve and edit data, usually support data are human readable.	
Exploitability		Requires some mission domain knowledge to make sense of support data.	
Discoverability	Support data are part of mission system, however, finding the uplink support data has small chance than finding any type of support data.		

Table 1-2 Tampering with Mission Support Data Likelihood Determination Matrix

Criteria	High (3)	Medium (2)	Low (1)
Reproduce-ability		Attacker has to go through the attack vector the same way again.	.
Exploitability		Requires some mission domain knowledge to find correct input data.	
Discoverability		Uplink tools are a small set of software in an entire ground data system.	

Table 1-3 Unauthorized Use of Uplink Software Likelihood Determination Matrix

F. Impact Analysis

This step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of vulnerability. In the DREAD model [8] above, mission impact is described in terms of "Damage Potential" and "Affected Entity". Through the course of this study these impact statements was modified to better suit the present assessment, which are ranked from High (H), Medium (M), and Low (L) with a score 3, 2, and 1 respectively.

1. Uplink malicious commands to S/C:
   - Damage Potential (H, 3): Disruption to S/C and/or loss of mission data
   - Affected Entity (H, 3): Loss of S/C or science results are a major catastrophic failure to PI and NASA. It is also an agency-wide embarrassment to NASA. It will be very costly to recover S/C from anomaly and recapture lost mission data.

2. Use incorrect input for uplink generation:
   - Damage Potential (M, 2) Disruption to mission operation.
   - Affected Entity (L, 1): Loss of ground resources to recover uplink preparation from incorrect uplink products.

3. Create unwanted or garbage uplink products:
   - Damage Potential (M, 2) Disruption to mission operation.
   - Affected Entity (L, 1): Loss of ground resources to clean up malicious uplink products.

G. Risk Determination

The metrics and calculations determining risk described in this section are used to estimate the likelihood of a successful attack by a threat agent and the effect of that attack on the mission (impact). Such risks to the mission can be calculated using the standard risk formula [3,9]:

Level of Risk = Attack Success Likelihood (ASL) x Mission Impact (MI)

Uplink system risk determination calculated from the Level of Risk formula:

- Tampering with S/C commands:
  - ASL = 3 + 2 + 2 = 7
  - MI = 3 + 3 = 6
  - Level of Risk = 7 x 6 = 42
- Tampering with mission support data
  - ASL = 3 + 2 + 2 = 7
  - MI = 2 + 1 = 3
  - Level of Risk = 7 x 3 = 21
- Unauthorized use of uplink system
  - ASL = 2 + 2 + 2 = 6
  - MI = 2 + 1 = 3
  - Level of Risk = 6 x 3 = 18

Risk Score	Risk Level
1 - 18	Low (L)
19 - 36	Medium (M)
37 - 54	High (H)

IV. CONCLUSION

Concern	Likelihood	Impact	Level of Risk	Mitigation
Tampering with Commands	M to H	H	H	M1
Tampering with Mission Support Data	M to H	M	M	M2
Unauthorized Use of Uplink S/W	M	L to M	L	Acceptable Risk

Recommendations and Migration Strategies:

A. Mitigation #1 (M1):
   - Strengthen perimeter security control to mission and science operation centers by multi-level sign authentication with multi-level security policy enforcement [1].
   - Increase data confidentiality and integrity securities by data encryption and multi-factor security control to command data store [2].
   - Perform forward and reverse command validations.
   - Strengthen commanding process and reviews by cross-examinations.

B. Mitigation #2 (M2):

   - Strengthen perimeter security control to mission and science operation centers by multi-level

sign authentication with multi-level security policy enforcement.
- Increase data confidentiality and integrity securities by data encryption and multi-factor security control to mission data store.
- Perform data verification at each node in uplink process value chain.

In general, MOS should continue to be vigilant to security threats. Establish vigorous process for user credentials management, to avoid account decommissions negligence and duplication of user credential stores. Infuse of new security technologies. Work with FFRDCs NASA centers, and other external organizations in determining cyber security threats and mitigation strategies. Apply cyber security knowledge learned from MOS experience to continuously improve cyber security protection to NASA missions.

The most important recommendation is to include cyber threat risk assessments and security system engineering throughout the MOS development cycle concurrent with system fault protection system design. Otherwise, it is impossible to design a dependable and reliable MOS to meet today's rapid changing cyber threat environment.

Acknowledgments

We would like to acknowledge the many contributions of the participants in the JPL Space Asset Protection task: Jim Rinaldi (JPL Chief Information Officer), Jay Brar (JPL Chief Security Officer), Rich Doyle (Information and Data Science Program Manager), Andy Dowen (Multi-Mission Ground Systems and Services Program Deputy Manager), and Bob Vargo (Ground Systems Engineering Section Manager).

This research described in this paper was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with National Aeronautics and Space Administration (NASA).

References

[1] M. Bishop, Computer Security: Art and Science, December 2002. pp.1-3, pp. 32-38 Addison-Wesley Professional Press.

[2] Andrew Hoog, Android Forensics: Investigation, Analysis, and Mobile Security for Google Android, June 2011, pp.159-169, Syngree Press.

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

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

[5] A. Y. Ko, P. Maldague, D. Lam, T. Bui, and J. McKinney, " The Evovable Advanced Multi-Mission Operations System (AMMOS): Making Systems Interoperable", AIAA SpaceOps 2010, Huntsville Alabama, April 2010.

[6] Kam S. Tso, Michael Pajevski, and Bryan Johnson " Access Control of Web and Java Based Appications", 17th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2011), Pasadena CA, December 2011.

[7] A. Y. Ko, D. Lam, P. Maldague, R. Wiegand, and C. Yeung, "GDS S/W Architecture GSFC-GMSEC and JPL-AMMOS Collaboration", in Quality Mission Software Workshop 2010 CA.

[8] Michael Howard and David LeBlanc, Writing Secure Code, Second Edition, 2003, pp.63-73, Microsoft Press.

[9] Houssein Bidgoli. Handbook of Information Security: Threats, Vulnerabilities, Prevention, Detection, and Management. Published by John Wiley and Sons, 2006 ISBN 0471222011, 9780471222

Author Biographies

Mr. Adans Y. Ko *is a Mission Operations Assurance Manager in Mission Assurance Management Office at JPL. He has published numerous papers in the area of mission operation system and system architecture. Currently, he is the U.S. Rosetta Project and Voyager Mission Operations Assurance Manager, and he was the Ground System software architecture for the current and future Advanced Multi-Mission Operations System (AMMOS) and the system engineer and development manager for the AMMOS Mission Planning and Sequencing Subsystem (MPS) over 10 years. He has in-depth knowledge of the Multi-mission Ground Data System uplink tools, which include mission planning, sequence generation, and sequence flight software. In the private sector, he was a project manager for credit card systems for the Navy at CitiBank Development Center, Los Angeles, CA and a Principle Engineer for e-Commerce Consulting at MarchFirst Consulting Firm, in Los Angeles, CA. He received NASA "Turn a goal to reality" award for his work on technology infusion of AMES planning and scheduling technology to AMMOS planning and sequencing legacy system. He has also received NASA's Exceptional Service Medal for his work on Voyager's Onboard Computer Command Subsystem for missions to Uranus and Neptune. He got his B.S.C.S. degree from Utah State University, Logan, Utah in 1982 and his M.B.A. degree from University of California, Los Angeles in 1993.*

Dr. Kymie M. C. Tan *is a Systems Engineer at the Jet Propulsion Laboratory and adjunct faculty of the Computer Science Department at Carnegie Mellon University. She has authored several papers in the area of cyber security, specifically intrusion detection, and served on a number of program and proposal selection committees (NSF, ARPA). Her research interests include the effective design,*

implementation and deployment of cyber-defensive systems, and the design of effective testing methodologies to evaluate the reliability and performance of cyber-defensive systems within operational environments.

Mr. Ferner Cilloniz-Bicchi *was a Software Security Engineer at JPL.*

Mr. Grant B. Faris *is the Chief Mission Operations Assurance Manager in Mission Assurance Management Office at JPL. Grant has spent his 42 year career in space operations including 13 plus years in the USAF, several years in aerospace industry, and the last 27 years with the Jet Propulsion Laboratory (JPL). His last 14 years have been focused on the formalization of the mission operations assurance program at JPL.*