GSAW2015

A SPACE MISSION CYBER-SECURITY STUDY

CODE: GMV-GSAW2015-PRE-001
DATE: 03/03/2015
VERSION: 1

© 2015 by GMV
Published by The Aerospace Corporation with permission.
CONTEXT
TRENDS

Criticality of space-based services

Battlefield: Cyber-space

DUQU
FLAME
RED OCTOBER
PRISM
THE MASK...
AND IN SPACE?
SUMMARISING II

BUT... IT ISN’T EASY AT ALL

- Several deeply specialised fields converge
- Very complex systems
- Large infrastructures
- Lots of actors
- Dependencies, interconnections,...
REQUIREMENTS

- SIMPLICITY & USABILITY: TOOL SUPPORT
- FLEXIBILITY AND ADAPTABILITY
- COMPLETE
- EASY TO MAINTAIN AND EVOLVE
- INTERNAL CROWDSOURCING
- HOMOGENIZE
- FULL OWNERSHIP TO ESA
SOLUTION CONCEPTS

A PRIORI RISK ASSESSMENT & TREATMENT RECOMMENDATIONS

- MODULARITY CONCEPT:
  - EXPLOIT COMMONALITIES
  - ADAPT TO PARTICULARITIES

FOR DUMMIES AND EXPERTS
METHODOLOGY
METHODOLOGY

- WE WILL TAKE A RECOMMENDED SAFEGUARD AND GO BACKWARDS
SAFEGUARD

“Event Logging” in phase E of a mission

- Can be HIGH or BASIC

- Mitigates vulnerabilities:
  - Directly: removing the vulnerability or the possibility of exploiting it
  - Indirectly: mitigating the consequences of the vulnerability being exploited

- In this case:  
  - Untraceability of User Actions

- **BUT**... it is not the only safeguard required to mitigate the vulnerability...
**VULNERABILITY**

- Is part of a risk (threat-vulnerability pair)
  - It can be exploited by threats

- In our example one threat is:
  - Unauthorized use of rights

- Value based on CVSS:
  - Range
  - Complexity
  - Authentication
  and
  - Impact
**THREAT**

- The risk introduced by a threat is:
  - The Probability of the threat materializing, per,
  - The Impact that it would have if it materializes
THREAT - PROBABILITY

- The probability of a threat materializing depends on the attacker:
  - Means
  - Motivation
  - Opportunity
THREAT – PROBABILITY – MEANS

- Linked with the attacker skills and resources
THREAT – PROBABILITY – MOTIVATION

- Linked with the attacker interests and the mission capacities

For each mission type we have identified groups of attackers, their motivations to attack the mission and the means.
Based on the existence of vulnerabilities which can be exploited by the threat

- Takes the MAX of all exploitable opportunities
THREAT – IMPACT

- Combines:
  - The threat potential damage
  - The degradation allowed by the vulnerability (TOTAL, PARTIAL, NONE)

- Potential damage:
  - Considers the value of each security dimension for the mission
  - Calculated based on impact table
## THREAT – IMPACT

<table>
<thead>
<tr>
<th>Level</th>
<th>Economic Loss (% of budget)</th>
<th>Impact to image/reputation</th>
<th>Legal impact</th>
<th>Impact to Strategic Position</th>
<th>Impact to society</th>
</tr>
</thead>
<tbody>
<tr>
<td>L1</td>
<td>0.1%</td>
<td>Impact to internal image (unsatisfied, unmotivated employees)</td>
<td>Violation of regulations and laws by an employee, but with no legal impact to organization.</td>
<td>Loss of data with strategic value.</td>
<td>Knowledge development</td>
</tr>
<tr>
<td>L2</td>
<td>1%</td>
<td>Impact to technical leadership</td>
<td>Violations of regulations and laws with minor consequences. Minor breaches of contract which result in at most minor contractual penalties.</td>
<td>Strategic service accessible by the enemy.</td>
<td>Impact to non-critical services</td>
</tr>
<tr>
<td>L3</td>
<td>10%</td>
<td>Impact to public opinion (utility of mission)</td>
<td>Violations of regulations and laws with substantial consequences. Major breaches of contract with high contractual penalties.</td>
<td>Strategic service degraded. Data with strategic value corrupted.</td>
<td>Critical services degradation</td>
</tr>
<tr>
<td>L4</td>
<td>100%</td>
<td>Impact to customers</td>
<td>Fundamental violations of regulations and laws. Breaches of contract with ruinous damage liabilities.</td>
<td>Temporal loss of strategic service.</td>
<td>Critical services unavailability</td>
</tr>
<tr>
<td>L5</td>
<td>&gt;100%</td>
<td>Impact to financial credibility of ORG, financial partners relationship</td>
<td>Revocation of the license for space services.</td>
<td>Loss of strategic service.</td>
<td>Safety of life</td>
</tr>
</tbody>
</table>
RECAPITULATING

Launcher missions:
- Potentially interesting for different attackers for several reasons
- Some of them might be motivated and have the means to, among many others, execute an “unauthorised use of rights”
- This threat can exploit “untraceability of user actions”.
- This has a probability which is a combination of Means/Motivation/Opportunity
- The Impact which depends on the potential damage and the degradation allowed by the vulnerability for each dimension.
- The Risk is Threat x Vulnerability
- To reduce that risk we can apply several safeguards among which “Event Logging”
RESULTS
VIDEO SUMMARY