Cyber Defense Lessons for Flight Software

DJ Byrne

Jet Propulsion Laboratory
California Institute of Technology

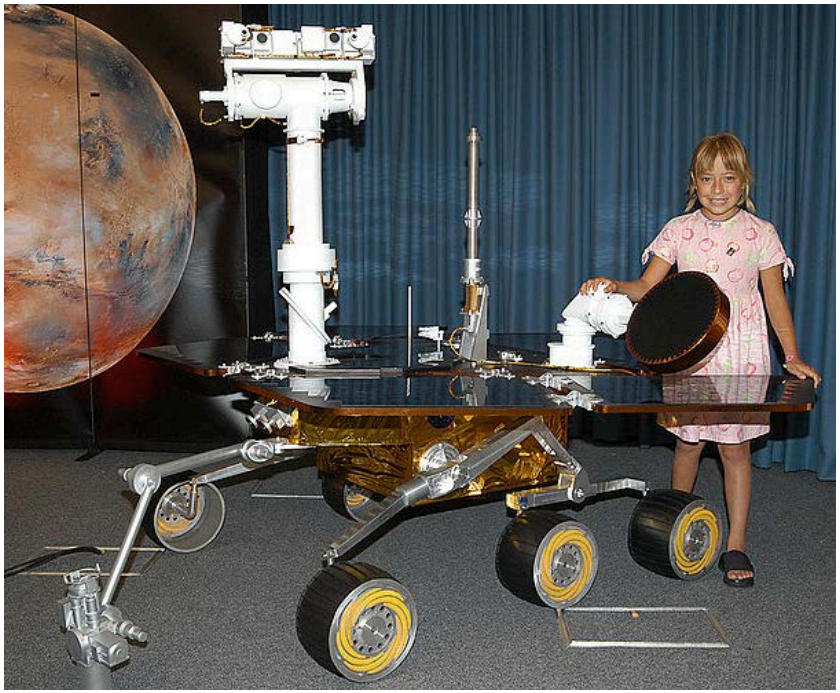
Overview

- *How attackers look at your system*
- Key take-aways
  - It's worth your time
  - It's not that difficult
    - 80/20 rule
  - It's not that expensive
- Lessons by Lifecycle
  - Mission Planning
  - Software Management
  - System Engineering
  - Architecture & Design
  - Implementation
  - Testing
  - Operations

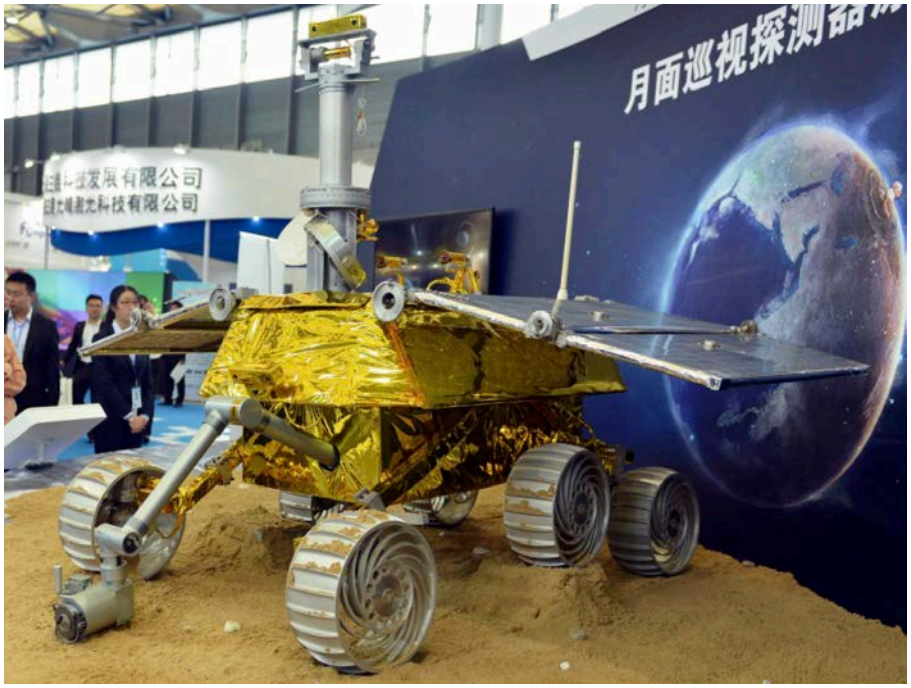
© 2016 California Institute of Technology. Government sponsorship acknowledged.

How Closely Are You Being Watched?

- Spirit/Opportunity
  Mars
  - 2004-01, USA



- Yutu (Jade Rabbit)
  Luna
  - 2013-11, China



© 2016 California Institute of Technology. Government sponsorship acknowledged.

Yesterday's Headlines

Stolen NASA laptop contained space station control codes

Inspector general says theft resulted in 'loss of algorithm'; Chinese intrusions also noted

Friday, March 2, 2012

NASA HACKED AGAIN

Chinese hackers took over NASA's Jet Propulsion Lab, Inspector General reveals

Published March 01, 2012 / FoxNews.com

Sections ☰ The Washington Post

Local

Chinese hack U.S. weather systems, satellite network

Chinese Military Suspected in Hacker Attacks on U.S. Satellites

By Tony Capaccio and Jeff Bliss | Oct 26, 2011 9:01 PM PT | 0 Comments

Hackers had 'full functional control' of Nasa computers

2 March 2012 Last updated at 13:52 ET

Romanian accused of hacking NASA-JPL computers

AP February 9, 2012 9:09 AM

NASA: We've Been Hacked Thousands Of Times Because Of Inadequate IT Infrastructure

Posted Mar 2, 2012 by Devin Coldewey

Tomorrow's Headlines?

The New York Times

Cyber Attack Turns ‘Curiosity’ into Martian Boulder

The Washington Post

Hackivists fry Spitzer Telescope by Pointing at Sun

THE WALL STREET JOURNAL.

‘Juno’ Jupiter Explorer hijacked by Al Qaeda, transmitting anti-U.S. Slurs

Attackers Do Not "Fly As You Test"

- Can I come at you through the weeds?
  - Breadth of attack surface
  - Depth of defenses
- "Test as you fly, fly as you test"
  - Creates coverage gaps by permitting us to avoid, rather than patch, dangerous behavior.
  - If a Bad Thing can happen by chance, it can also happen by intention (e.g. maliciously)
- V'ger 6 was totally pwned...
  - Stardate 7412.6

© 2016 California Institute of Technology. Government sponsorship acknowledged.

Mission Planning

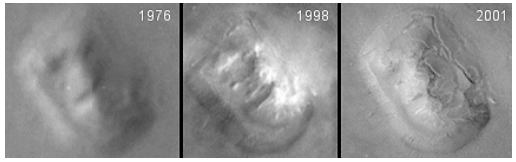
Fortune Favors the Prepared

- Can I attack you unopposed?
- Acknowledge the need, define it, track it
  - Good starting reference: CCSDS Green Book "Security Threats Against Space Missions"
- Threat Agents, Motivations:
  - Nation state – Design Info, Financial Plans
  - Criminals – Money (e.g. RansomWare)
  - Terrorists/activists – Publicity (destruction OK)
  - "Kids" – Thrills, Attention, Experimentation

© 2016 California Institute of Technology. Government sponsorship acknowledged.

Mission Planning, cont

- C-I-A "Security triad"
  - Confidentiality
  - Integrity
  - Availability
- Consequences to Avoid Include
  - Scientific scooping (who publishes first?)
  - Bogus science results (injected)
  - Loss of mission or schedule
  - Loss of reputation, i.e. loss of future business



© 2016 California Institute of Technology. Government sponsorship acknowledged.

Mission Planning, cont

- Some threats FSW <u>could be</u> resilient to
  - Data corruption
  - Ground facility physical attack
  - Interception
  - Jamming
  - Denial-of-Service
  - Masquerade
  - Replay
  - Software threats
  - Unauthorized Access
  - Tainted Hardware Components

© 2016 California Institute of Technology. Government sponsorship acknowledged.

Software Management

Don't start from scratch

- How disciplined are your defenses?
- Governance, controlling authorities you <u>need a story</u> for - starting with:
  - FISMA (Federal Information Security Management Act of 2002)
  - FIPS requirements
    - Federal Information Processing Standard Publication 199, "Standards for Security Categorization of Federal Information and Information Systems"
  - Implementation guidance
    - CNSSI 1253 "Security Categorization and Control Selection for National Security Systems"
      - Attachment 2, Appendix F "Space Platform Overlay"
    - NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations"

© 2016 California Institute of Technology. Government sponsorship acknowledged.

Software Management, cont

Make defenses work for you

- Budgeting for cyber-defense
  - Return on investment from dual-use benefits
    - Screen out accidental behaviors
    - Monitor behavior against expected baseline
    - Fewer subtle dangers available to users
  - Include wedge for sunset, or sustaining fixes

© 2016 California Institute of Technology. Government sponsorship acknowledged.

Software Management, cont

- Training
  - Experience and knowledge matter
  - Defensive coding materials freely available
  - Schedule time for training

- Lifecycle
  - Threats and attacks evolve
  - Include sunset, or sustaining fixes
  - Waterfall vs iterative, agile

© 2016 California Institute of Technology. Government sponsorship acknowledged.

System Engineering

"I can't do that, Dave."

- *Is there <u>one command</u> that would kill your spacecraft, end the mission?*
  - How about a pair of cmds? A sequence?

- Reliability analyses vs Threat Models
  - "It hurts when I do that!" "Then don't do it."
  - Model your environment, including threats
  - Be resilient to ground-system flaws

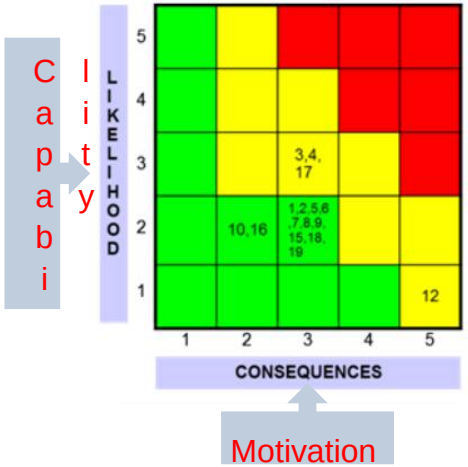
© 2016 California Institute of Technology. Government sponsorship acknowledged.

System Engineering, cont

- *Can I achieve my goal with your system?*
- Risk drivers: adversary capability and motivation
  - If it can happen accidentally, it can happen maliciously. But worse than that...
  - Intentional faults have different characteristics than accidental, or random faults
  - Risks adapt to defeat your counter-measures
  - Think strategic campaign, not single-fault analysis

© 2016 California Institute of Technology. Government sponsorship acknowledged.

System Engineering, cont



- Risk <u>Likelihood</u>
  - Linked with attacker capability
  - Can be driven up from "epsilon / negligible" toward "almost certain"
  - Multiple, coordinated, simultaneous faults

- Risk <u>Consequences</u>
  - Alignment with motives affects the likelihood

© 2016 California Institute of Technology. Government sponsorship acknowledged.

System Engineering, cont

- Can I process your data before you do?
- Can I modify your cmds or telemetry?
- Can I deny your service?
- Requirements for security (C-I-A views)
  - C: Encryption, key mgt,...
  - I: Signatures / hashes, key mgt...
  - A: What is safety-critical?
    - Power, thermal, telecom

© 2016 California Institute of Technology. Government sponsorship acknowledged.

Architecture and Design

Bake it in

- Diagram both use cases and *abuse* cases
- How many users do you design for?
  - Six? Six million?
  - Should it matter?
- Prevent, Detect, Mitigate, Recover

© 2016 California Institute of Technology. Government sponsorship acknowledged.

Architecture and Design - Prevent

- *Can I impersonate a trusted component?*
- Distrust users, instruments, other modules
  - Isolate inputs
    - Validate against unforgiving spec
  - Isolate outputs
  - Digital signatures on code, config, files, data
- When inheriting, can details be modified?
  - Like re-using a combination lock while changing the code (e.g. opcodes)

© 2016 California Institute of Technology. Government sponsorship acknowledged.

Architecture and Design – Prevent, cont

- *Can I taint a trusted component?*
- Chart the full supply chain
  - Compiler, libraries, chips
  - Can these be vetted / analyzed?
    - ...or isolated?
  - Is there malware inside already?

© 2016 California Institute of Technology. Government sponsorship acknowledged.

Architecture and Design - Detect

- *Can I jam an interface? Replay cmds?*
- Build in visibility
  - Avoid "no news is good news"
    - Does silence mean all is well, or alarm's been cut?
    - "...A 16-inch pipeline ruptures under Whatcom Falls Park and releases about 237,000 gallons of unleaded gasoline into Whatcom Creek, *unknown to anyone*."
  - Hashes / signatures / checksums on data
  - Heartbeats with timetags
  - Invalid data marked and returned, not dropped

© 2016 California Institute of Technology. Government sponsorship acknowledged.

Architecture and Design - Mitigate

- *Can I gain unauthorized access?*
  - *And do untraceable things?*
- Survive the attack
- Notice the attack, characterize it
- Call for help
- Shed complexity
  - Strip down to minimal critical functions

© 2016 California Institute of Technology. Government sponsorship acknowledged.

Architecture and Design - Recover

- *Can I persist after being noticed?*
- Fail-safe fallback of minimum complexity
- Checkpoint and restore to last-known-good state
- Redundant but non-identical components

© 2016 California Institute of Technology. Government sponsorship acknowledged.

Implementation

Bugs == Exploits

- *Can I inject my code to a running image?*
- Use everything your mother taught you about maintainable design
  - Few if any globals, etc
  - Anticipate buffer overflow attempts
  - Memory segmentation
- Code analysis is an unalloyed win
  - Dev process should have analysis baked-in

© 2016 California Institute of Technology. Government sponsorship acknowledged.

Implementation, cont

- *Can I modify artifacts in your CM (Configuration Management) System?*
  - *Circumventing your reviews*
- How often does this happen?
  - PROM image sent by email
  - Firmware image salvaged from old laptop
  - Parameter files from USB drive
  - "As-run" test data mis-labeled when retrieved
- Archive checksums separate from artifact they protect; compare them out-of-band

© 2016 California Institute of Technology. Government sponsorship acknowledged.

Testing

More reliable too!

- *Can I make the unexpected work for me?*
- Seeing goat paths as highways
  - "It can be made to work"
  - ...vs "Can it be made to fail?"
- Independent testers who use software in unintended ways, configs, and combinations
  - Fuzzing inputs
- Code coverage (looking for trojans)

© 2016 California Institute of Technology. Government sponsorship acknowledged.

Operations

- *Can I upload my own software patch?*
- *Can I re-normalize your baseline?*
- Flight rules and restrictions vs code fixes
- Constant patch vs fly-as-you-test
- Continuous Monitoring
  - Establish a baseline and track against it
  - Command counter?
  - Time-powered-on counter?

© 2016 California Institute of Technology. Government sponsorship acknowledged.

Summary: Necessary But Not Sufficient

Look for gaps in coverage

- Current cyber-security designs
  - Single-layer; blind to multi-layer actions
  - Fault Containment intended along Dev/Test/Ops lifecycle boundaries, but not strictly maintained
  - Gaps in coverage between layers

© 2016 California Institute of Technology. Government sponsorship acknowledged.

Questions?

- Key take-aways
  - It's worth your time
  - It's not that difficult
    - 80/20 rule
  - It's not that expensive

"I can't do that, Dave."

Fortune Favors the Prepared

Look for gaps in coverage

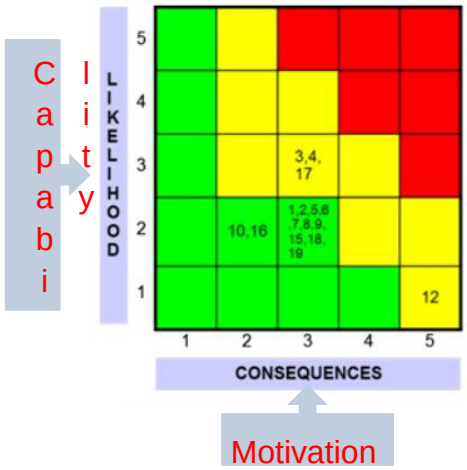
Bake it in

More reliable too!

Make defenses work for you

Don't start from scratch

Bugs == Exploits



References

- CCSDS Green Book "Security Threats Against Space Missions"
  - https://public.ccsds.org/Pubs/350x1g2.pdf
- NASA IV&V Secure Coding portal
  - https://nen.nasa.gov/web/coding
- Build Security In - best practice articles
  - https://www.us-cert.gov/bsi
- Common Weakness Enumeration
  - https://cwe.mitre.org/

© 2016 California Institute of Technology. Government sponsorship acknowledged.

References, cont

- Satellites interfered with
  - 2011 Report to Congress of the U.S.-China Economic and Security Review Commission (page 216)
  - http://origin.www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf
- "Hacking Curiosity" article
  - http://www.pcmag.com/article2/0,2817,2408295,00.asp

© 2016 California Institute of Technology. Government sponsorship acknowledged.

References, cont

- 2012-02-29, NASA OIG to Congress
  - http://oig.nasa.gov/congressional/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf
- NASA OIG Semiannual report, April 1 – Sept 30, 2012
  - http://oig.nasa.gov/SAR/sar0912.pdf
  - http://oig.nasa.gov/press/pr2012-E.pdf
- "Exposing One of China's Cyber Espionage Units"
  - https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

© 2016 California Institute of Technology. Government sponsorship acknowledged.

References, cont

- "Chinese hack U.S. weather systems, satellite network"
  - https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html
- "Chinese hackers took over NASA's Jet Propulsion Lab, Inspector General reveals"
  - http://www.foxnews.com/tech/2012/03/01/chinese-hackers-nasa-jpl-lab.html

© 2016 California Institute of Technology. Government sponsorship acknowledged.

Jet Propulsion Laboratory
California Institute of Technology

jpl.nasa.gov