MSL CYBER SECURITY IMPLEMENTATION GSAW 2013

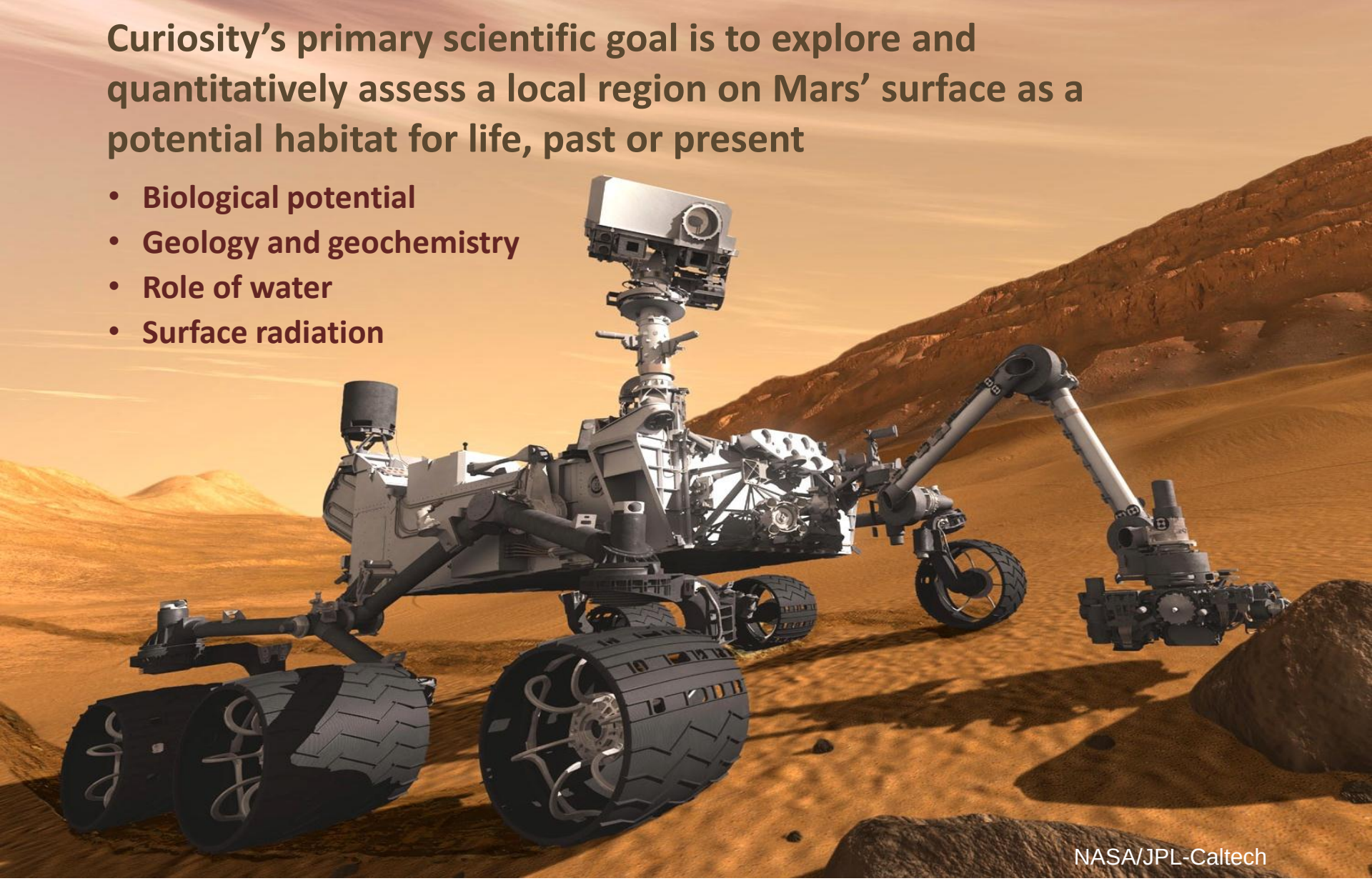
Presenters:

Glen Elliott and Bryan Johnson

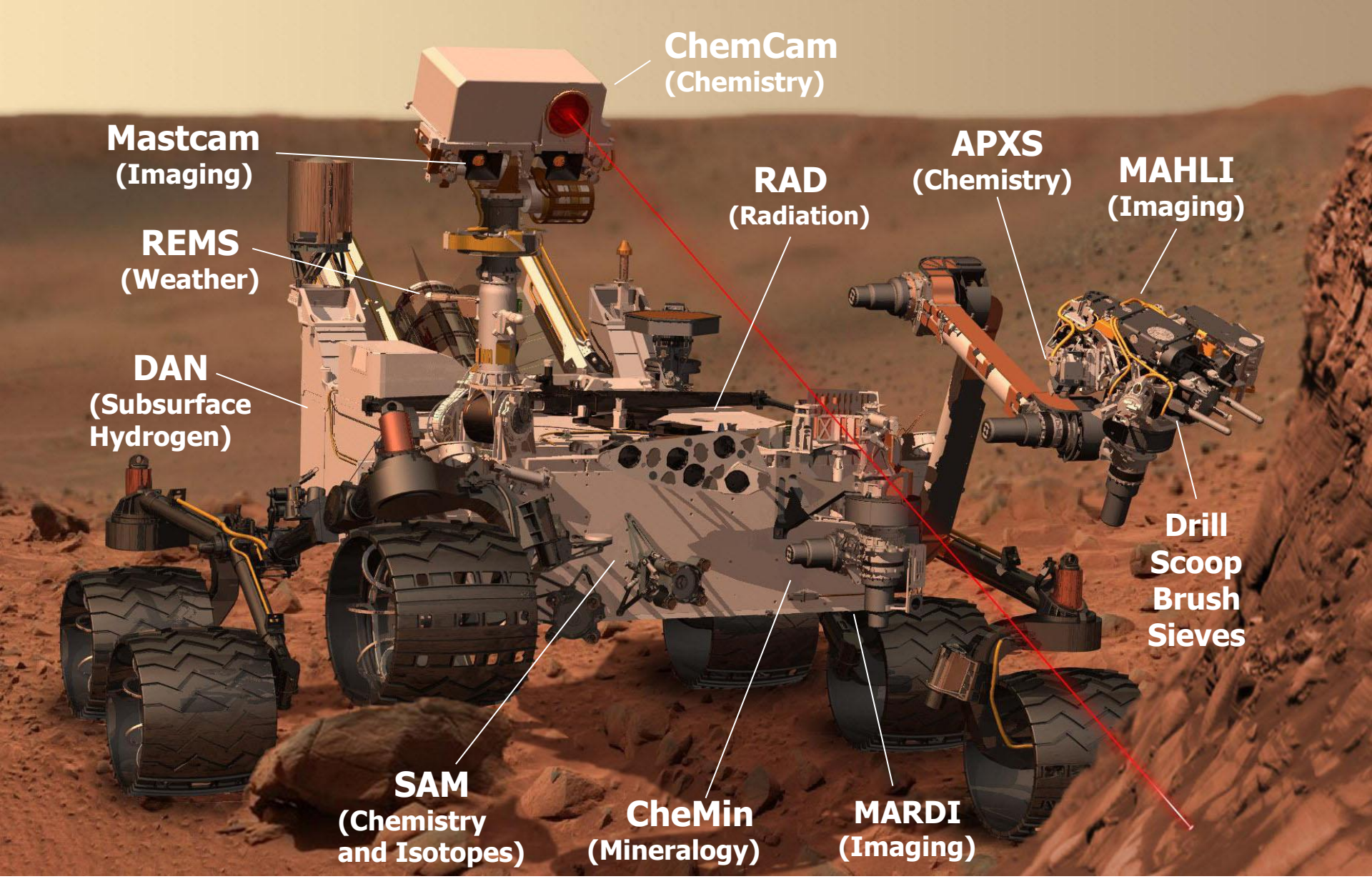
Jet Propulsion Laboratory, California Institute of Technology

Curiosity's primary scientific goal is to explore and quantitatively assess a local region on Mars' surface as a potential habitat for life, past or present

- Biological potential
- Geology and geochemistry
- Role of water
- Surface radiation



NASA/JPL-Caltech



How it started….

- We were hacked!.....

FOX NEWS .com Fair & Balanced

Search

ON AIR NOW › 11a et Happening Now WATCH LIVE

Home | Video | Politics | U.S. | Opinion | Entertainment | Tech | Science | Health | Travel

Science Home | Archaeology | Dinosaurs | Planet Earth | Wild Nature | Air & Space | Natural Science

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

Published March 01, 2012 / FoxNews.com

An artist's conception of NASA's next Martian rover, called Curiosity, one of many U.S. missions to the Red Planet run by the Jet Propulsion Lab. (NASA/JPL)

Print
Email
Share
0 Comments

Chinese hackers gained control over NASA's Jet Propulsion Laboratory (JPL) in November, which could have allowed them delete sensitive files, add user accounts to mission-critical systems, upload hacking tools, and more -- all at a central repository of U.S. space technology, according to a report released Wednesday afternoon by the Office of the Inspector General.

What we did about it….

- Previous to the intrusion all flight project relied upon the Office of the Chief Information Officer (OCIO) to provide all aspects of cyber-security
- Since MSL was identified as a “national treasure” and NASA project of great importance the project senior management approved a proposal to staff a cyber-security position to implement a list of implementations that would either retire or reduce identified risks.
- The risk list, with identified improvements, was provided to the project by Bryan Johnson
- The implementer of the improvements was Glen Elliott
- The implementations were worked in close concert with the JPL OCIO, project SAs, and other selected personnel

Standards Applied to MSL Cyber-Security

- The Federal Information Security Management Act (FISMA)
- NIST SP800-30 Guide for Conducting Risk Assessments: Information Security

Standards Controls Implemented

- The controls as listed on the previous URL with those MSL are currently implementing, or have been implemented already listed in Green.

- Risk Assessment;
- Certification, Accreditation and Security Assessments;
- System Services and Acquisition;
- Security Planning;
- Configuration Management;
- System and Communications Protection;
- Personnel Security;
- Awareness and Training;
- Physical and Environmental Protection;
- Media Protection;
- Contingency Planning;
- Maintenance;
- System and Information Integrity;
- Incident Response;
- Identification and Authentication;
- Access Control;
- Accountability and Audit

Cruise/EDL Security Implementation Options

Threats	Risks	Pre-EDL Mitigations
MSL command dictionary deployment process assumed compromised	Unauthorized users could access and possibly exploit MSL command dictionary	Correct web based upload process Restrict access to smallest possible group – as small as 2
JPL usernames and passwords assumed compromised	Unauthorized access to project systems and data	Implement two-factor authentication
JPL internal systems assumed compromised Undetected malware	Indirect monitoring of project activity Data manipulation Code manipulation	Implementation if VLAN for all MSL critical assets Implement secure software deployment pattern
Assume MSL account list allows non-MSL personnel to access MSL resources	Exploitation of MSL resources by non-MSL personnel	Decrement MSL access list to maintain currency with actual MSL project personnel
An attack directed at MSA computers CloudBurst	Denial of service - Inconsistency across operations environment Installation of malware VM Host computer compromised	Implement network filtering measures Harden authentication and authorization mechanisms Identify decision authority in accordance with IRP – based on attack impact on project Implement a log collection system
An attack directed at Storage NFS exploits	Denial of service - Loss of continuity of operations Project data disclosure, manipulation or loss	Isolate points of privileged access Improve security measures for admin access Implement file hashing algorithm
An attack directed at Databases SQL injection	Denial of service - Delay in post-pass spacecraft analysis Project data disclosure, manipulation or loss	Isolate points of privileged access Verify accounts / account management Implement data recovery

Surface Security Implementation

Threats	Risks	Surface Mitigations
Assumed that MSL Ground System architecture has vulnerabilities	MSL ground system architecture vulnerabilities can lead to compromised operations Loss of planning cycles, GDS capabilities supporting critical roles needed for completion of daily operations	Review and analyze the architecture to identify vulnerabilities and remediation with an outside consultant Review critical operations roles and the software that supports that role
Unknown and un-needed software and components attacked Buffer overflows, command injection	Aging and non-supported software, and other apps can lead to exploitable vulnerabilities leading to data disclosure, manipulation, or loss	Establish and maintain complete list of required software Implement new software and components that are up to date, supported, and securitized on a schedule that allows for continuity and non-interruption of MSL operations
JPL internal systems assumed compromised Undetected malware	Exploitable vulnerabilities could compromise operations Compromised systems used to conduct surveillance	Coordinate with MSL Security Group to scan for known vulnerabilities Remote logging and Log Reporting being enhanced
Unauthorized addition of software to the desktop standard build for software systems Includes trojans, viruses, command and control	Direct monitoring of project activity via malware Planning data manipulation Compromised developer systems exploited to commit malware to code repositories Unintentional introduction of malware through non-scanned and vetted desktops connected to guest networks	Conduct periodic desktop system checks for malware and rootkits Coordinate enhanced security controls for all developer systems Implement static code analysis as a pre-delivery requirement
An attack directed at externally facing application resources SQL injection, buffer overflows, cmd execution	Denial of service – Loss of planning cycle Project data disclosure, manipulation or loss	Segment applications to protected zones Improve security logging and alerting measures for externally facing applications Limit or eliminate direct privilege data access
An attack directed at Web resources Cross-site scripting	Denial of service – Loss of planning cycle Project data disclosure, manipulation or loss	Investigate NASA IG recommendations based on the November 2011 attacks Coordinate implementation of OWASP rules
Compromise of user credentials – unauthorized user uses compromised user's credentials	Allows non-credentialed user access to MSL resources	Conduct training classes for users to remind them of the shared security environment and responsibilities Establish baseline patterns for trending of user account usage Develop reporting mechanism for errant patterns in authentication

MSL Cyber Security Implementations

- Creation of Incident Response Plan with senior MSL project management and the JPL Security Operations Center
  - Test and training of personnel in procedures
- Improved Anomaly Detection
  - Use of network and system logs to identify common, or nominal, activities as well off nominal activities
- Improved User Authentication
  - Use of Two Factor Authentication (TFA)
  - User base of over 500 users, including Foreign Persons, that needed to be setup and trained
  - All MSL environments needed to be updated for TFA
- Network configuration segregation to VLANs
- Network and user segregation of dictionary access
- User access list decrement

MSL Cyber Security Implementations

- Improved data integrity and data accountability
  - NIST approved programs utilized
- Improved vulnerability and audit scans across all MSL assets
- Update security patches regularly and maintain currency
- Decrement Third Party Software inventory rigorously

Results of all that work….

- The MSL project has successfully fulfilled the mandate to land a rover on Mars and operate that rover, >190 Sols to date
  - Without a cyber-security incident impacting operations….