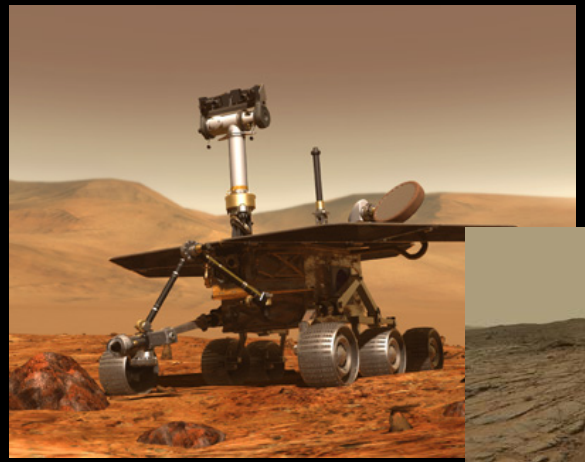
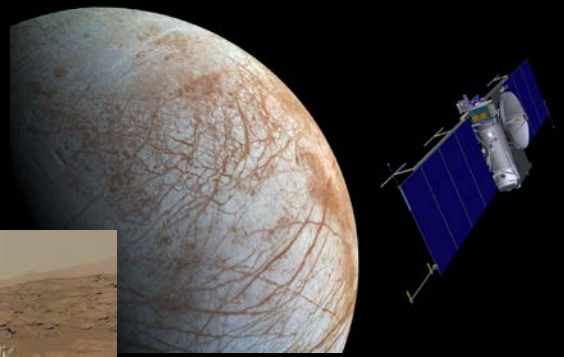
Protecting Space in Cyber Space: When the Aliens are Hackers

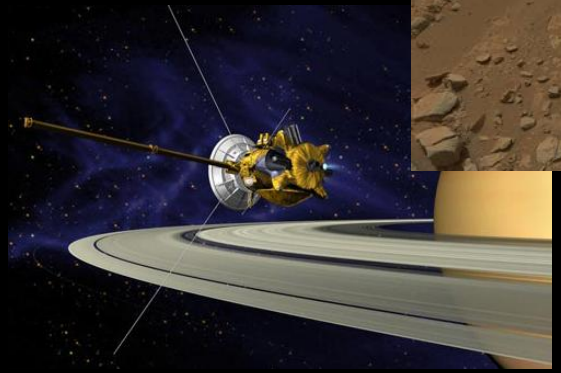
Suzanne Stathatos, Cyber Defense Engineer

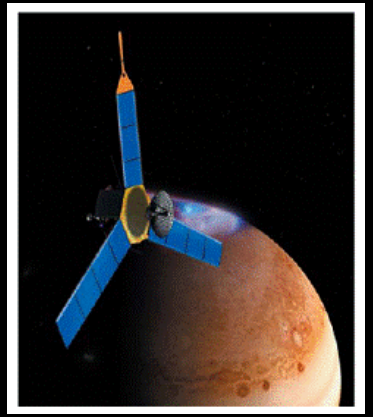
Jet Propulsion Laboratory
California Institute of Technology

JPL Builds Cool Stuff!









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

But ...

HACKERS ALLEGEDLY HIJACK DRONE AFTER MASSIVE BREACH AT NASA

Hackers release 631 aircraft and radar videos, 2,143 flight logs and data on 2,414 employees

Mikael Thalen | Infowars.com - JANUARY 31, 2016 720 Comments

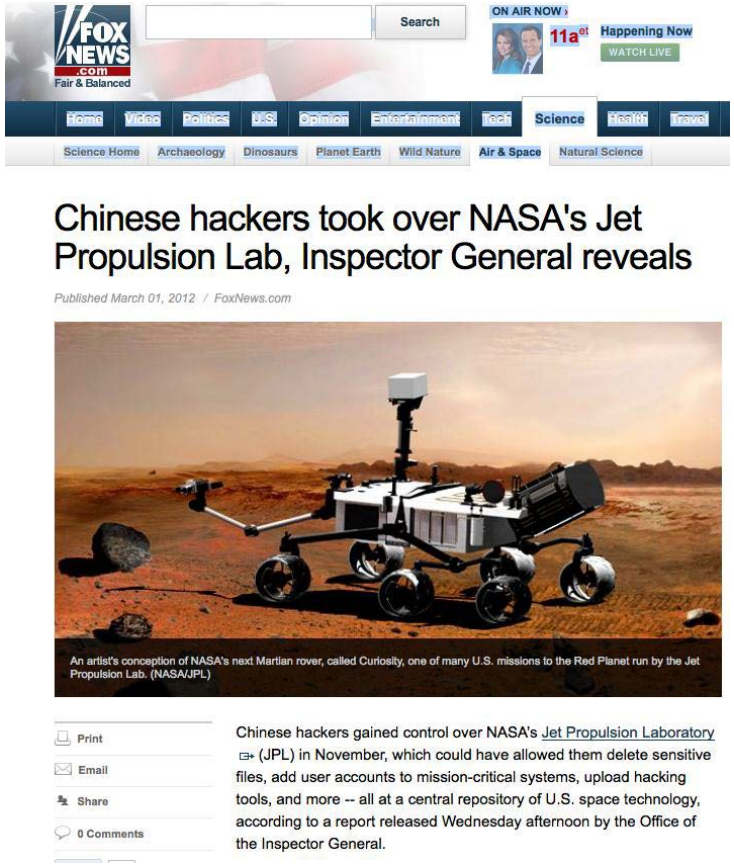
Hackers had 'full functional control' of Nasa computers

2 March 2012 Last updated at 13:52 ET

Romanian accused of hacking NASA-JPL computers

AP February 9, 2012 9:09 AM

JPL Real-World Example



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.

Unique Cyber Security Challenges @ JPL

Mission-critical Systems

Legacy Systems

Cyber-physical Systems

Heterogeneous Cyber Systems

Many collaborators, different collaboration profiles

Sensitive Operational Environments (low tolerance for uncertainty)

(Very) Remote High Value Assets

CDER Focus and Research Thrusts

Survivability – operational resilience through attacks

Automated detection, diagnosis and remediation

Design and deployment of anomaly detectors

APTs and Supply Chain Attack Detection

Cyber Situational Awareness

Design of Security Metrics

Rigorous evaluation of cyber defenses in mission-critical environments

Threat and Vulnerability Assessments

Some Current Projects

Mission-centric Cyber Risk Assessment for JPL Missions

Sensor Mesh for Cyber Situational Awareness

Cyber Defense Test Lab

Smart Grid Cyber Security (non-NASA funded)

Machine learning techniques to make sense of cyber data from missions

Cyber Security for Petroleum and Oil Infrastructures (non-NASA funded)

Calibration of Cyber Sensors (NSA funded / yet to begin)

Some Current Projects

Mission-centric Cyber Risk Assessment for JPL Missions

Sensor Mesh for Cyber Situational Awareness

Cyber Defense Test Lab

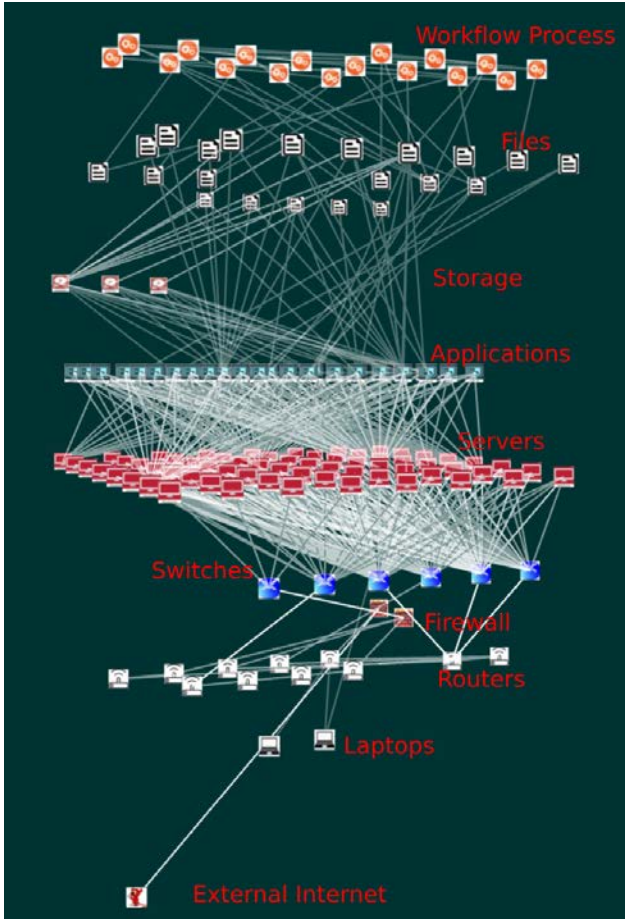
Smart Grid Cyber Security (non-NASA funded)

Machine learning techniques to make sense of cyber data from missions

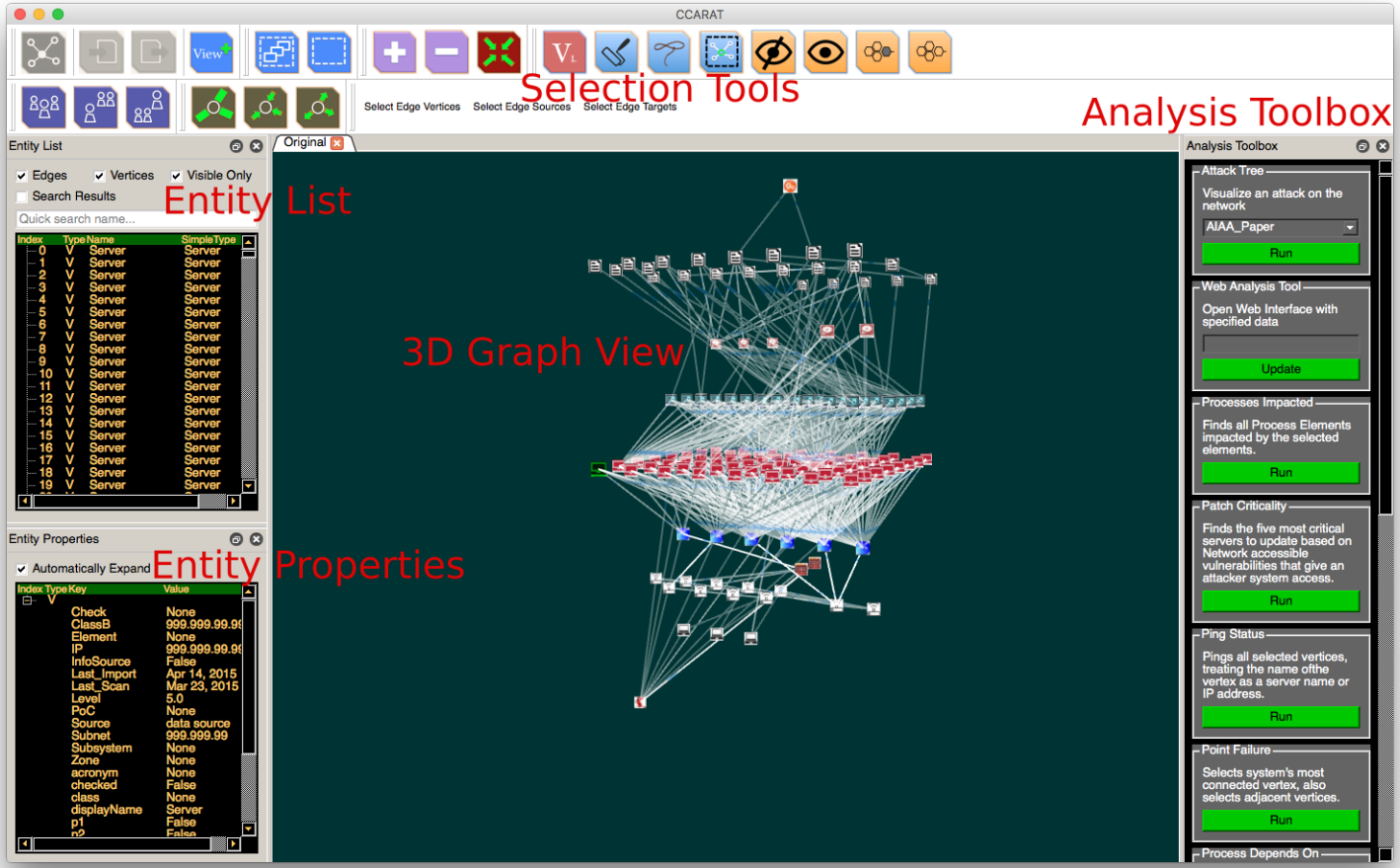
Cyber Security for Petroleum and Oil Infrastructures (non-NASA funded)

Calibration of Cyber Sensors (NSA funded / yet to begin)

Mission-centric Cyber Risk Assessment for JPL Missions



Cyber Analysis Visualization Environment (CAVE)



Some Current Projects

Mission-centric Cyber Risk Assessment for JPL Missions

Sensor Mesh for Cyber Situational Awareness

Cyber Defense Test Lab

Smart Grid Cyber Security (non-NASA funded)

Machine learning techniques to make sense of cyber data from missions

Cyber Security for Petroleum and Oil Infrastructures (non-NASA funded)

Calibration of Cyber Sensors (NSA funded / yet to begin)

Machine learning techniques to make sense of cyber data from missions

- Anomaly detection for Cyber Security
  - Detect anomalous network connections from/to mission system
    - E.g. Detect botnet communicating to command and control system
  - Detect anomalous user activity on a critical machine
    - E.g. authentication failures
  - Detect anomalous processes on critical machines
    - E.g. detect rootkit infection
  - Detect anomalous system usage
    - E.g. abnormal process usage, memory usage
  - Detect anomalies in network protocols, application protocol usage

Challenges for Anomaly Detection in Cyber

- Lots of research, not much operational deployment
  - Baselining nominal
    - System behavior evolves over time, requires continuous re-training of models.
  - Accurate characterization of anomalies and attacks
    - Anomalies often manifest differently based on system context
  - Interpretation/explanation anomaly detection alerts
    - Explain why something was detected? Or not?
  - Environmental/operational factors
    - Changes in environment can cause attack signal to manifest differently.
  - Adversarial evasion (hiding within normal)
    - Adversaries can make attacks hide within legitimate traffic.
  - Impact of adversary-induced noise (changing the normal)
    - For example, conditioning of network traffic to maliciously train anomaly detectors
  - Detection of anomaly vs. an attack
    - Not all anomalies are attacks

Our Approach

- Generate traffic in an isolated test lab
- Make nominal model
- Inject anomalous behavior (malware, botnets, bad authentications, etc.)
- Develop algorithms to detect cyber-anomalies in dynamic environment
- Refine and Repeat

CDER Group

Dr. Kymie Tan (Research Lead, CMU alum)
Bryan Johnson (Group Supervisor)

- CS / Math PhDs
- System Administrators
- System Programmers / Software Engineers
- Hardware Security Engineer

Questions?

- Email me!
  - Suzanne.C.Stathatos@jpl.nasa.gov

End

Some Current Projects

Mission-centric Cyber Risk Assessment for JPL Missions

Sensor Mesh for Cyber Situational Awareness

Cyber Defense Test Lab

Smart Grid Cyber Security (non-NASA funded)

Machine learning techniques to make sense of cyber data from missions

Cyber Security for Petroleum and Oil Infrastructures (non-NASA funded)

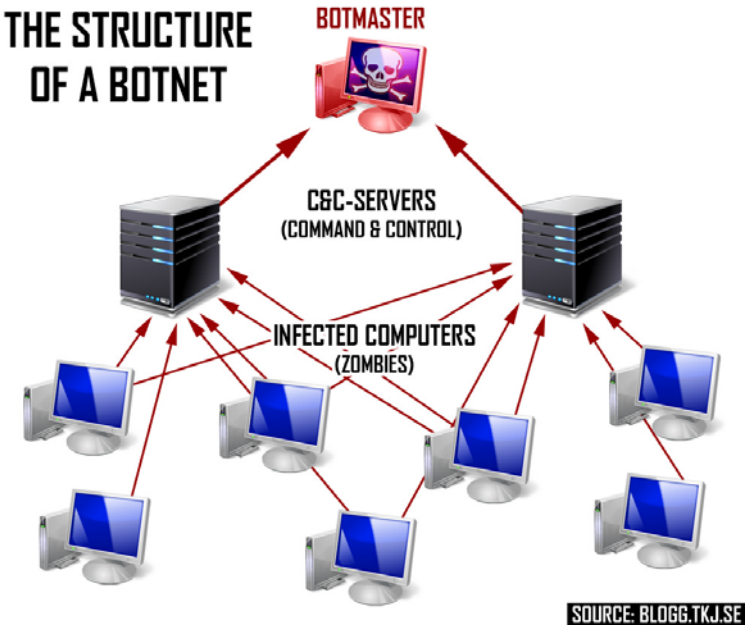
Calibration of Cyber Sensors (NSA funded / yet to begin)

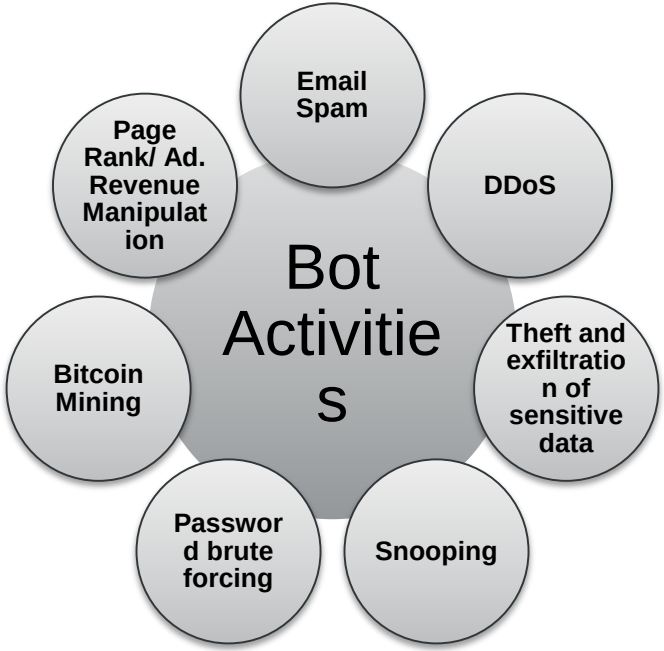
Cyber Defense Test Lab

- Validating Performance and system impacts of security measures
- Isolatable Environment on which to analyze malware and new attacks/faults
- Testing effectiveness of cyber security measures

What is a botnet?

Interconnected network of malware infected computers controlled by cybercriminals.





Threat Modeling

- Threat modeling is used to
  - understand the attacker goals
  - characterize the attackers
  - calculate likelihood of certain attacks
  - understand security assumptions when designing a system

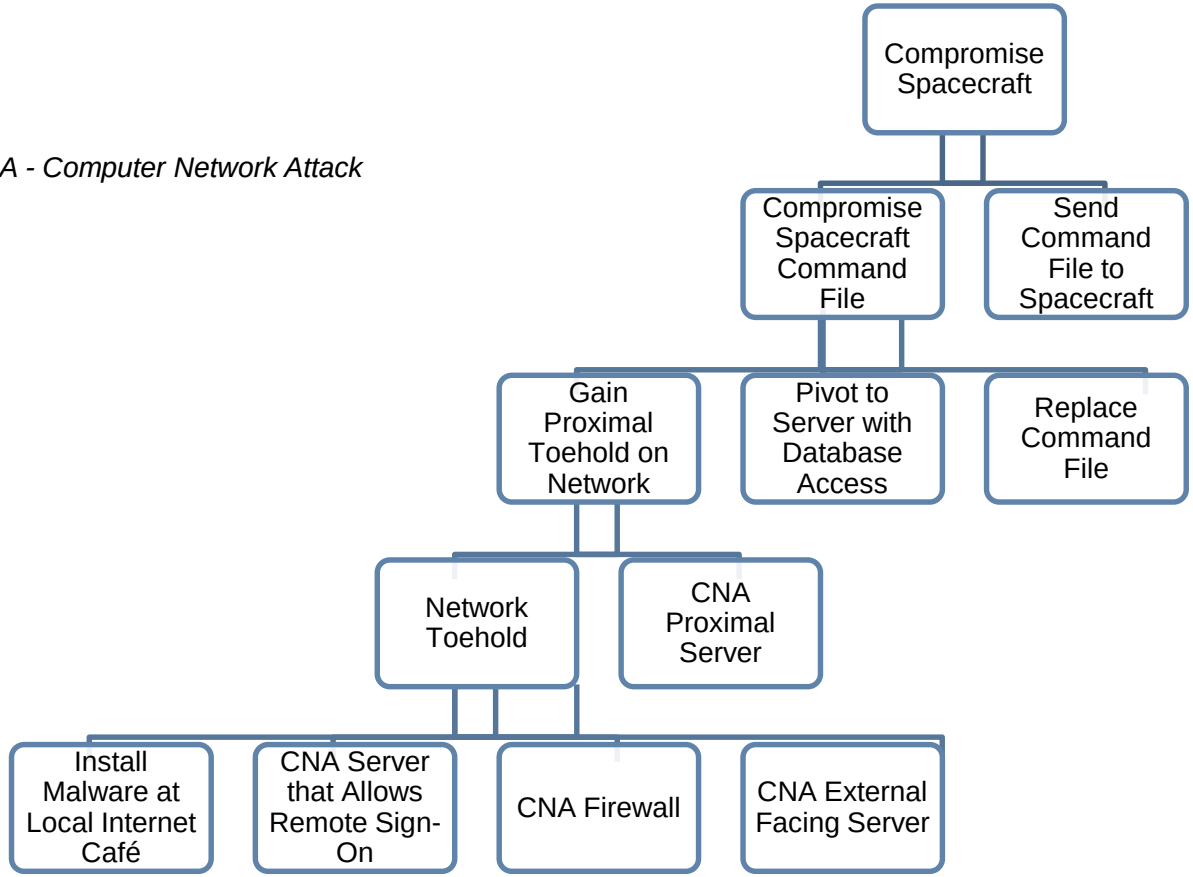
- Attack Trees are one such way to model threats

Attack Trees

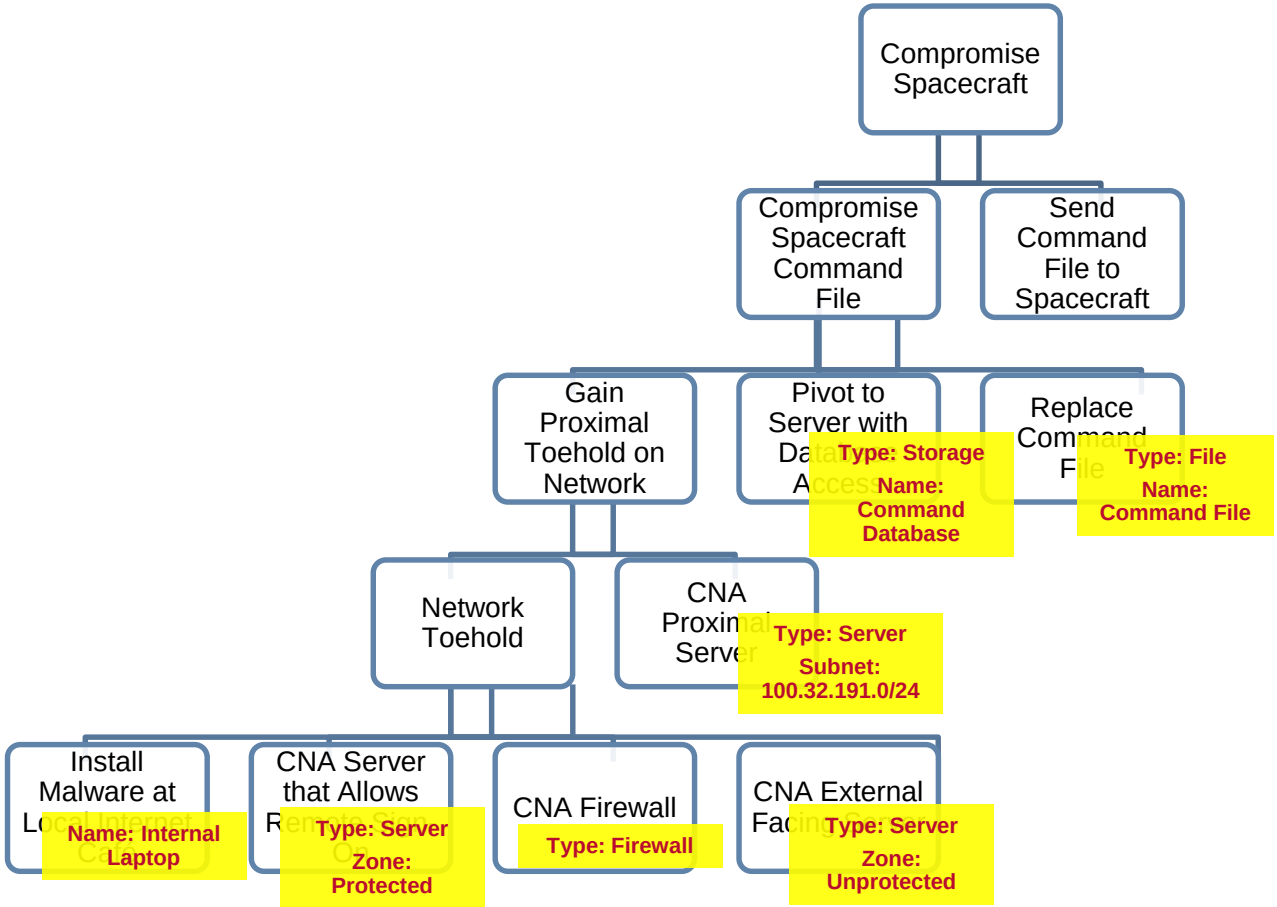
- Multilevel diagrams representing the steps an adversary needs to take to achieve a goal
  - Consist of a single objective (root node)
  - Several children nodes (intermediate steps)
  - Edge between two nodes, A and B, if B must be executed immediately before A.
  - Entry nodes (leaf nodes), from which an attacker can begin an attack path to the root node
- Typically constructed via a Cyber Subject Matter expert.
- Annotate the attack tree to link nodes of the attack tree with nodes in the system model

Attack Tree Example

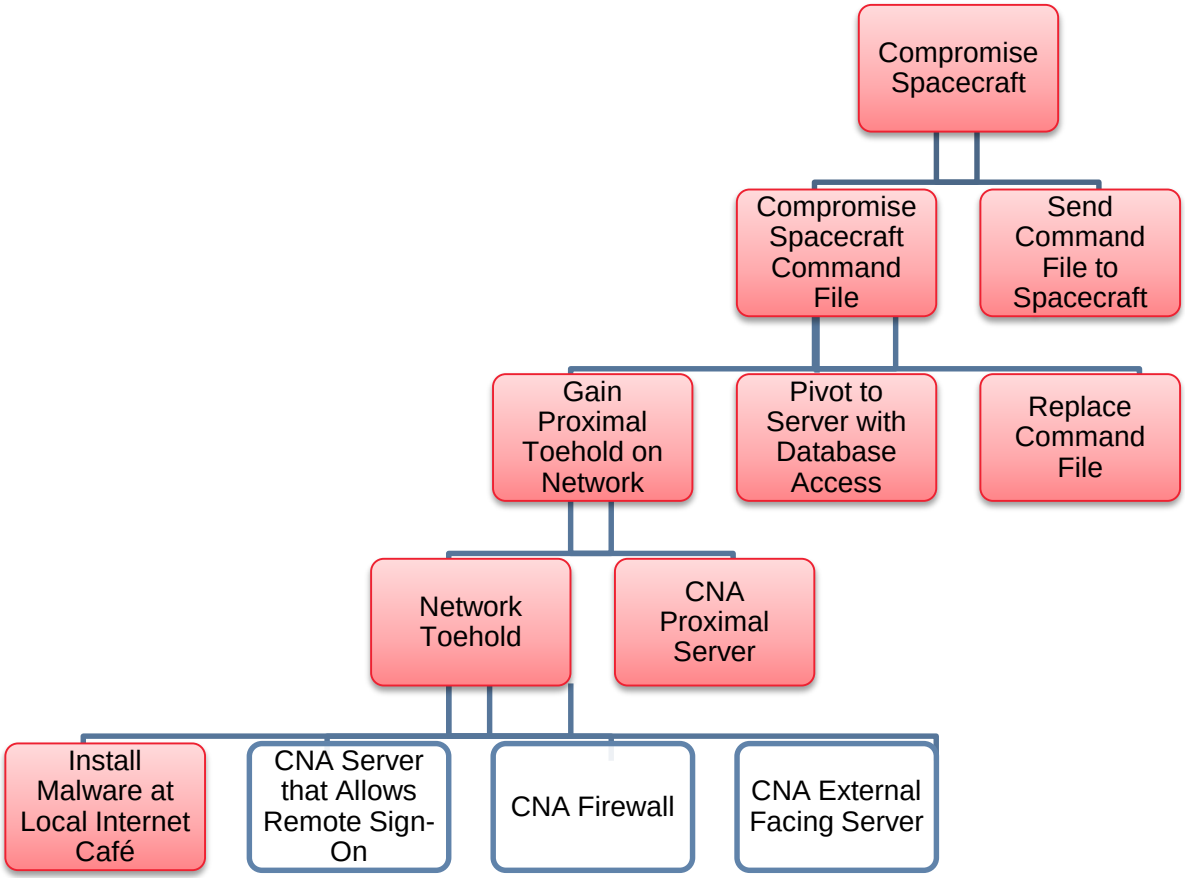
CNA - Computer Network Attack



Attack Tree Example



Path in the Attack Tree

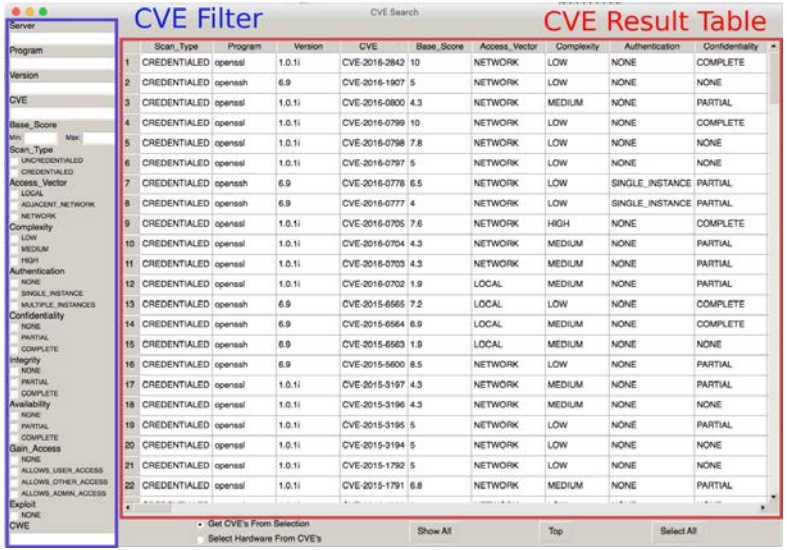


Analytical Capabilities in CAVE

- Programmatic interface to develop custom-analysis scripts
  - Based on graph semantics
    - Shortest path between nodes
    - Paths based on semantics of different layers
    - Adjacent vertices
    - Patching prioritization based on number of CVES
    - Eigenvector centrality
    - Most connected node
  - Analysis results are displayed on 3D Graph View

Analytical Capabilities in CAVE

- CVE Database Interface
  - List interface to view vulnerabilities for a network model
    - Can easily filter/search based on CVE properties
  - Connected to system model with selection
    - View vulnerable hardware in network model based on selected CVEs



	Scan_Type	Program	Version	CVE	Base_Score	Access_Vector	Complexity	Authentication	Confidentiality
1	CREDENTIALED	openssl	1.0.1i	CVE-2016-2842	10	NETWORK	LOW	NONE	COMPLETE
2	CREDENTIALED	openssh	6.9	CVE-2016-1907	5	NETWORK	LOW	NONE	NONE
3	CREDENTIALED	openssl	1.0.1i	CVE-2016-0800	4.3	NETWORK	MEDIUM	NONE	PARTIAL
4	CREDENTIALED	openssl	1.0.1i	CVE-2016-0799	10	NETWORK	LOW	NONE	COMPLETE
5	CREDENTIALED	openssl	1.0.1i	CVE-2016-0798	7.8	NETWORK	LOW	NONE	NONE
6	CREDENTIALED	openssl	1.0.1i	CVE-2016-0797	5	NETWORK	LOW	NONE	NONE
7	CREDENTIALED	openssh	6.9	CVE-2016-0778	6.5	NETWORK	LOW	SINGLE_INSTANCE	PARTIAL
8	CREDENTIALED	openssh	6.9	CVE-2016-0777	4	NETWORK	LOW	SINGLE_INSTANCE	PARTIAL
9	CREDENTIALED	openssl	1.0.1i	CVE-2016-0705	7.6	NETWORK	HIGH	NONE	COMPLETE
10	CREDENTIALED	openssl	1.0.1i	CVE-2016-0704	4.3	NETWORK	MEDIUM	NONE	PARTIAL
11	CREDENTIALED	openssl	1.0.1i	CVE-2016-0703	4.3	NETWORK	MEDIUM	NONE	PARTIAL
12	CREDENTIALED	openssl	1.0.1i	CVE-2016-0702	1.9	LOCAL	MEDIUM	NONE	PARTIAL
13	CREDENTIALED	openssh	6.9	CVE-2015-6565	7.2	LOCAL	LOW	NONE	COMPLETE
14	CREDENTIALED	openssh	6.9	CVE-2015-6564	6.9	LOCAL	MEDIUM	NONE	COMPLETE
15	CREDENTIALED	openssh	6.9	CVE-2015-6563	1.9	LOCAL	MEDIUM	NONE	NONE
16	CREDENTIALED	openssh	6.9	CVE-2015-5600	8.5	NETWORK	LOW	NONE	PARTIAL
17	CREDENTIALED	openssl	1.0.1i	CVE-2015-3197	4.3	NETWORK	MEDIUM	NONE	PARTIAL
18	CREDENTIALED	openssl	1.0.1i	CVE-2015-3196	4.3	NETWORK	MEDIUM	NONE	NONE
19	CREDENTIALED	openssl	1.0.1i	CVE-2015-3195	5	NETWORK	LOW	NONE	PARTIAL
20	CREDENTIALED	openssl	1.0.1i	CVE-2015-3194	5	NETWORK	LOW	NONE	NONE
21	CREDENTIALED	openssl	1.0.1i	CVE-2015-1792	5	NETWORK	LOW	NONE	NONE
22	CREDENTIALED	openssl	1.0.1i	CVE-2015-1791	6.8	NETWORK	MEDIUM	NONE	PARTIAL

Traversing through the Network Model

- A user selects an entry node of the attack tree.
  - This selection gives an attack path in the tree.

- The algorithm selects nodes in the system model based on the annotation of the attack tree nodes.
  - `*Install malware at local internet café'* equates to (**type=Laptop, Name=Internal Laptop**)

- The User then proceeds through the attack path pivoting in the system model to the selected nodes if possible.