Mission-Centric Cyber Security Assessment of Critical Systems

Jeremy Pecharich, Suzanne Stathatos, Brian Wright, Arun Viswanathan, Kymie Tan
Jet Propulsion Laboratory, Pasadena, CA
AIAA Space 2016, Long Beach, CA

Jet Propulsion Laboratory
California Institute of Technology

- Introduction
- System Model
- Threat Modeling
- Cyber Analysis Visualization Environment
- Impact Assessment with CAVE
- Conclusion and Future Work

Introduction

The Threat Landscape

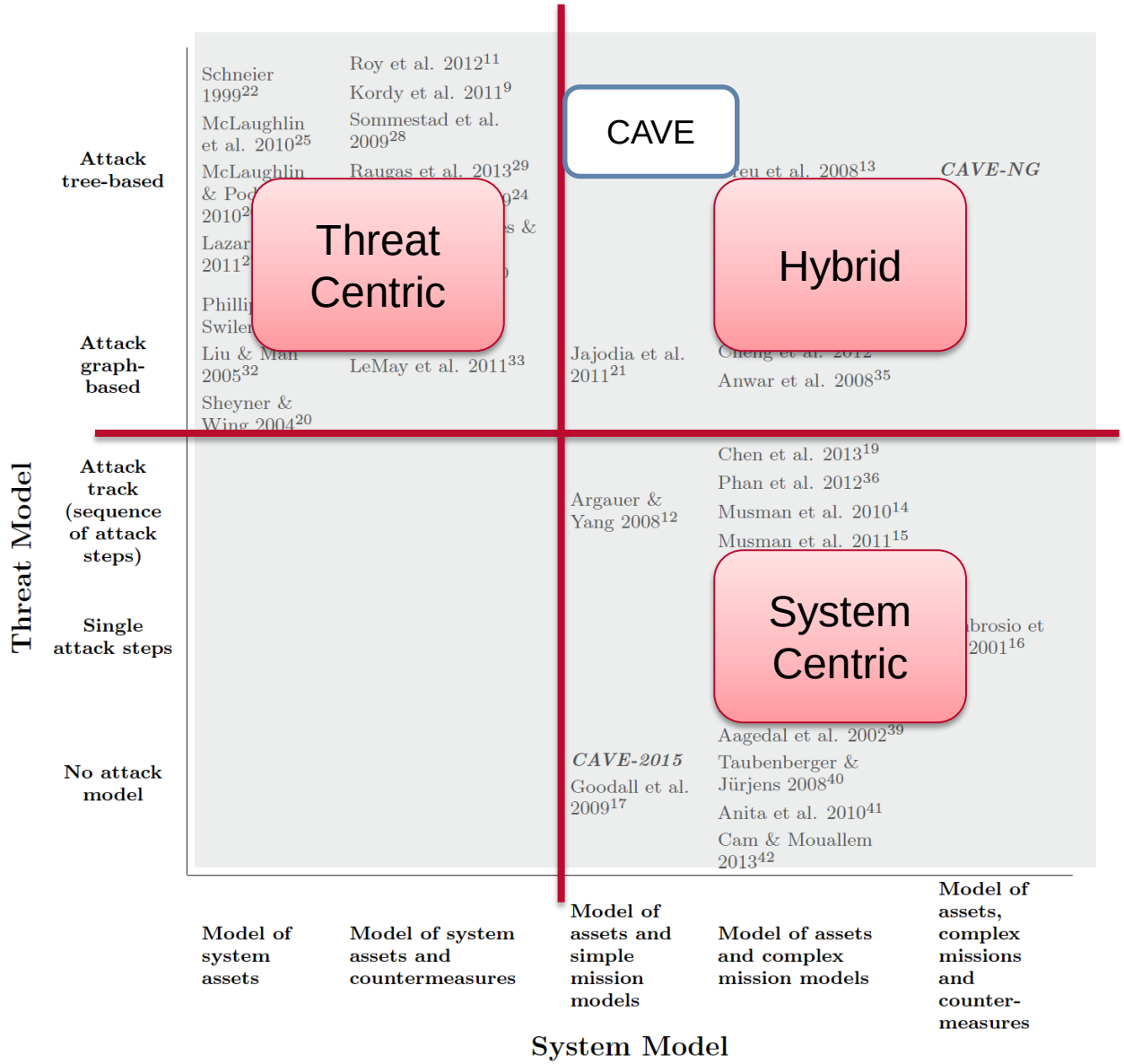
Past Incidents against Space Systems

- **January, 2016** – GSFC, GRC, and AFRC. Drone data and command authority hack
- **September, 2014** – National Oceanic and Atmospheric Administration (NOAA) – Chinese hackers breached computer networks to distort operational data coming from U.S. satellites
- **November, 2011** – Chinese hackers took over NASA's Jet Propulsion Lab, Inspector General reveals
- **May, 2011** – Goddard Earth Observation System – a hacker gained access to information contained on servers for the satellite-based Earth observation system
- **June, 2011** – Lockheed Martin was attacked using data obtained from the March RSA attack, unclear what was lost from Lockheed
- **2009** – Johns Hopkins University Applied Physics Laboratory – the lab was removed from all external network connections for a month due to the detection of hidden malware and stolen data
- **2007** – NASA Kennedy Space Center – a rogue program penetrated KSC networks, surreptitiously gathered data from computers in the Vehicle Assembly Building, and removed that data through covert channels

Lay of the Land

Threat Model \ System Model	Model of system assets	Model of system assets and countermeasures	Model of assets and simple mission models	Model of assets and complex mission models	Model of assets, complex missions and counter-measures
Attack tree-based	Schneier 1999[22] McLaughlin et al. 2010[25] McLaughlin & Podkuiko 2010[26] Lazarus et al. 2011[27]	Roy et al. 2012[11] Kordy et al. 2011[9] Sommestad et al. 2009[28] Raugas et al. 2013[29] Zonouz et al. 2009[24] Piètre-Cambacédès & Bouissou 2010[23] Edge et al. 2007[30]	***CAVE-2016***	Breu et al. 2008[13]	***CAVE-NG***
Attack graph-based	Phillips & Swiler 1998[31] Liu & Man 2005[32] Sheyner & Wing 2004[20]	LeMay et al. 2011[33]	Jajodia et al. 2011[21]	Cheng et al. 2012[34] Anwar et al. 2008[35]	
Attack track (sequence of attack steps)			Argauer & Yang 2008[12]	Chen et al. 2013[19] Phan et al. 2012[36] Musman et al. 2010[14] Musman et al. 2011[15]	
Single attack steps				Vigna 2011[18] Jakobson et al. 2011[37]	Ambrosio et al. 2001[16]
No attack model			***CAVE-2015*** Goodall et al. 2009[17]	Barreto et al. 2012[38] Aagedal et al. 2002[39] Taubenberger & Jürjens 2008[40] Anita et al. 2010[41] Cam & Mouallem 2013[42]	

Lay of the Land



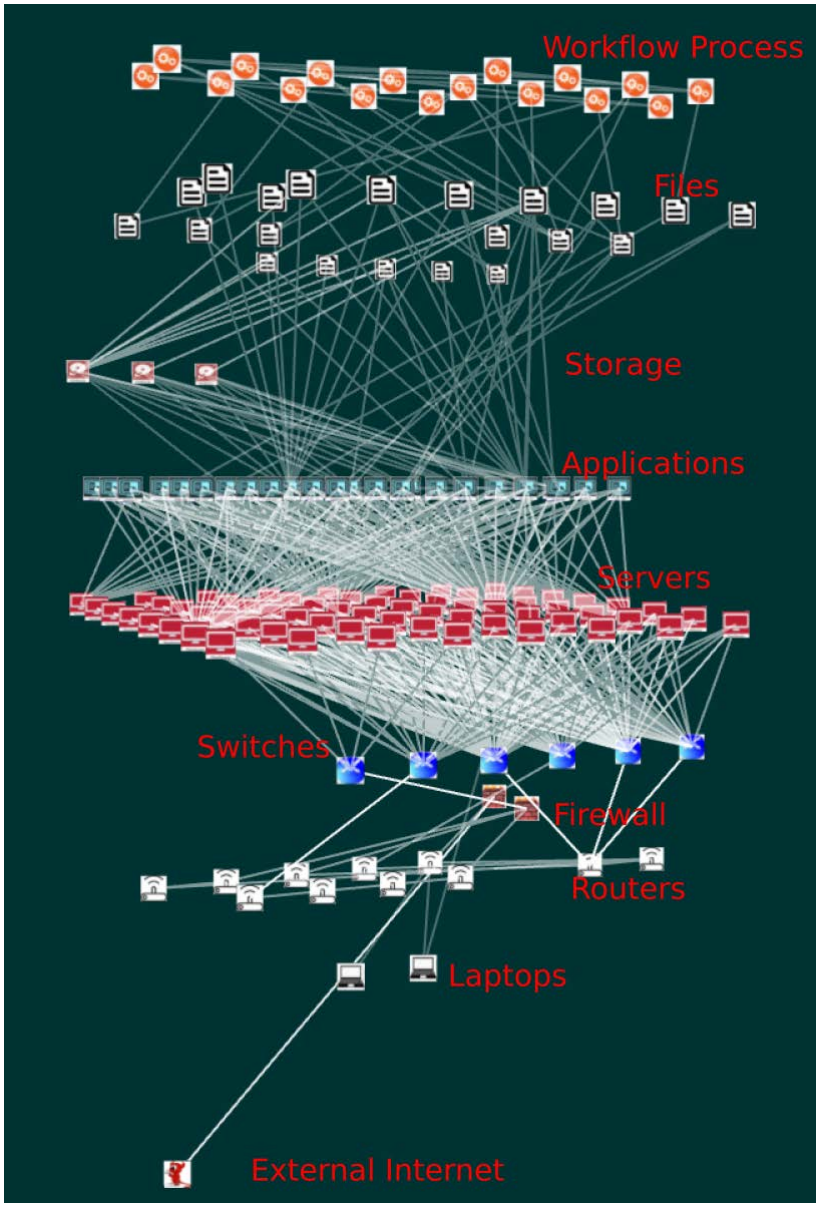
System Model

System Modeling

- Represent the Enterprise Network as graph.
  - Vertices consist of:
    - Hardware
      - (Servers, Firewalls, Routers, Switches, etc.),
    - Mission Software, Files, and Workflow Process (Higher Level Mission Tasks).
  - Edges are relationships between the different vertices
    - Software running on a server
    - File that can be accessed using software.

- Attached to the vertices are system attributes
  - OS, IP Groups, Users, Third-Party Software

Multilayer Network Model



Threat Modeling

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

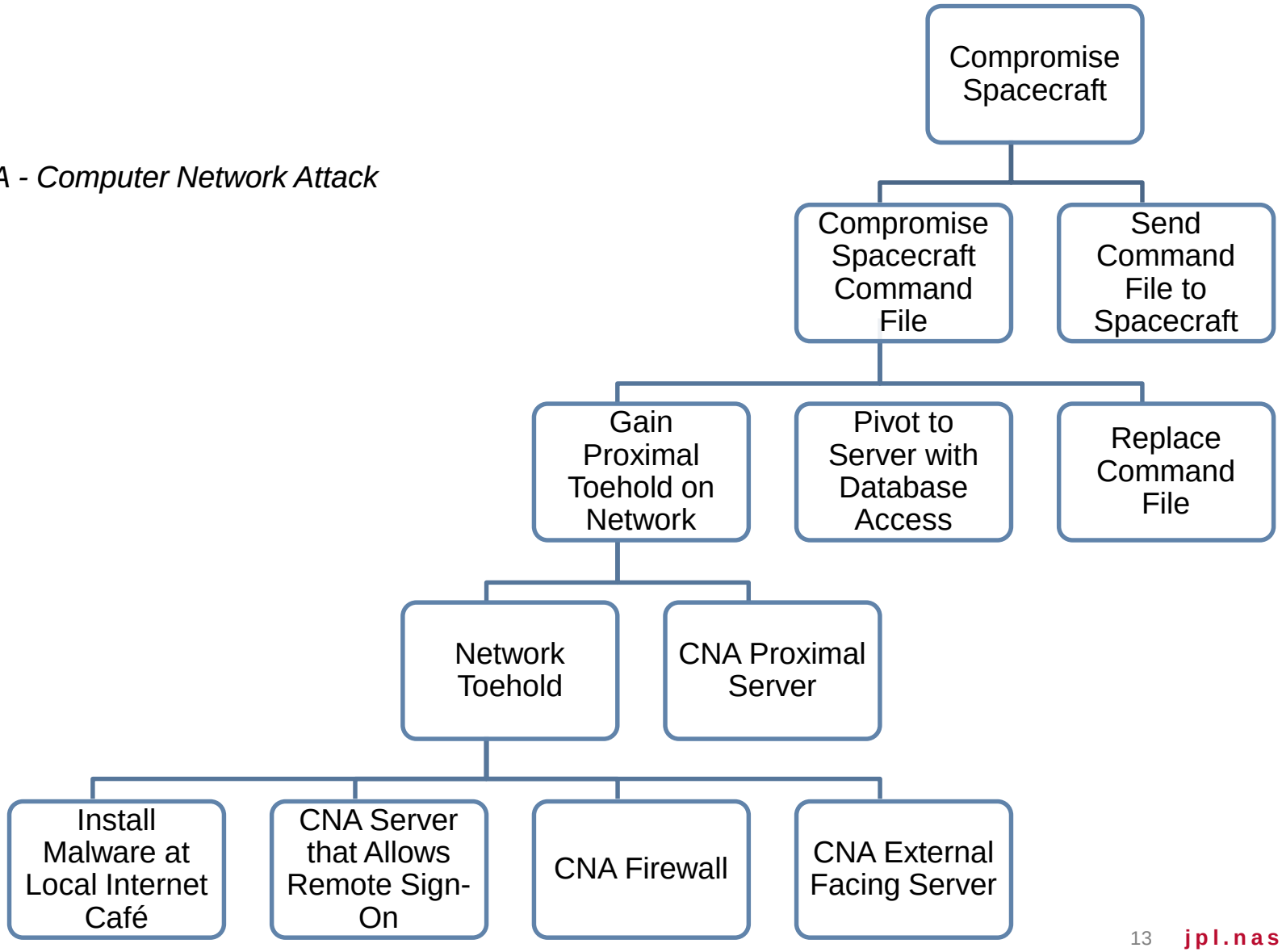
- Attack Trees are one such way to model threats

Attack Trees

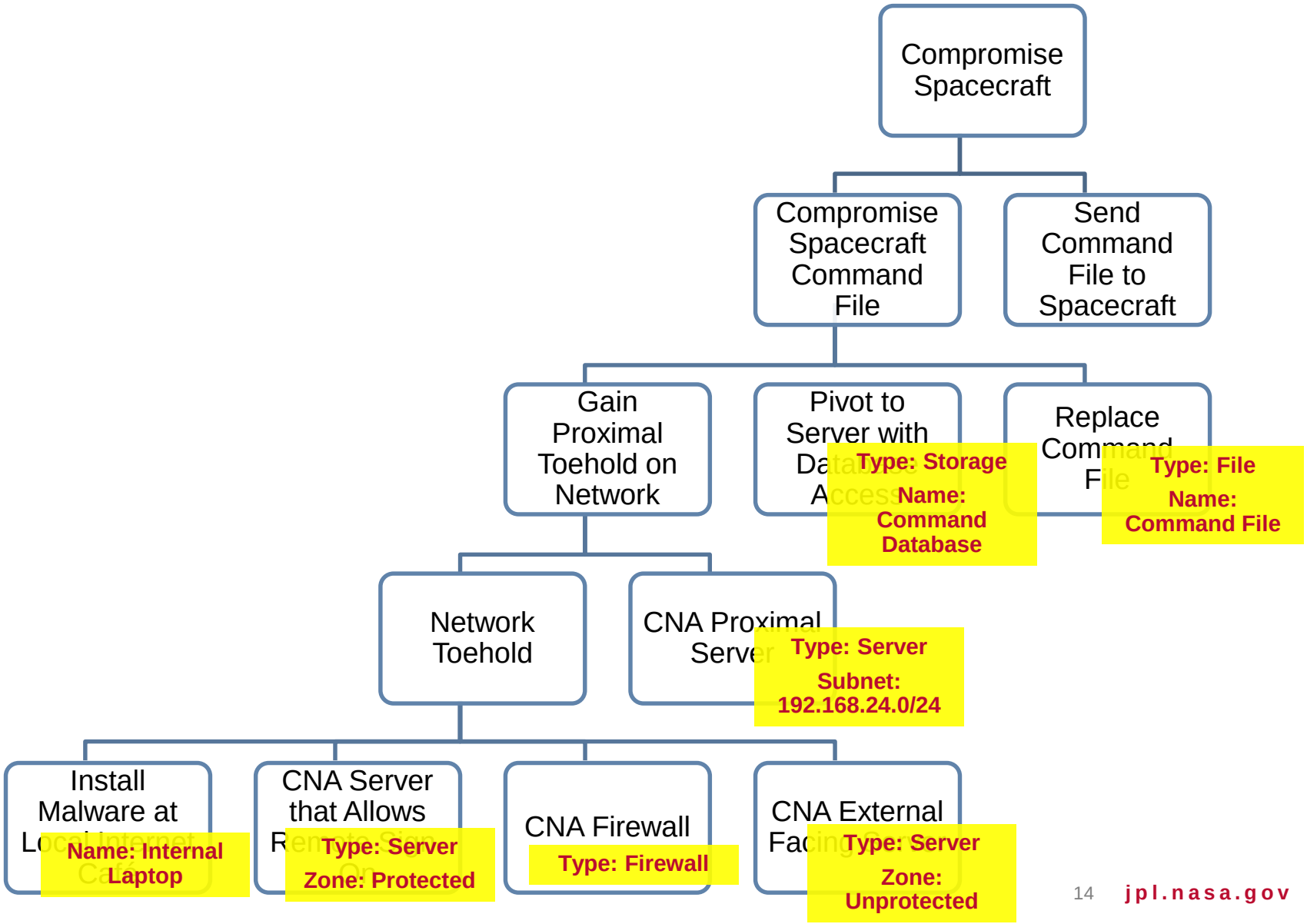
- Multilevel diagrams representing the steps an adversary needs to take to achieve a goal
  - Consist of a single objective (root node)
  - Several children nodes (intermediate steps)
  - Edge between two nodes, A and B, if B must be executed immediately before A.
  - Entry nodes (leaf nodes), from which 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

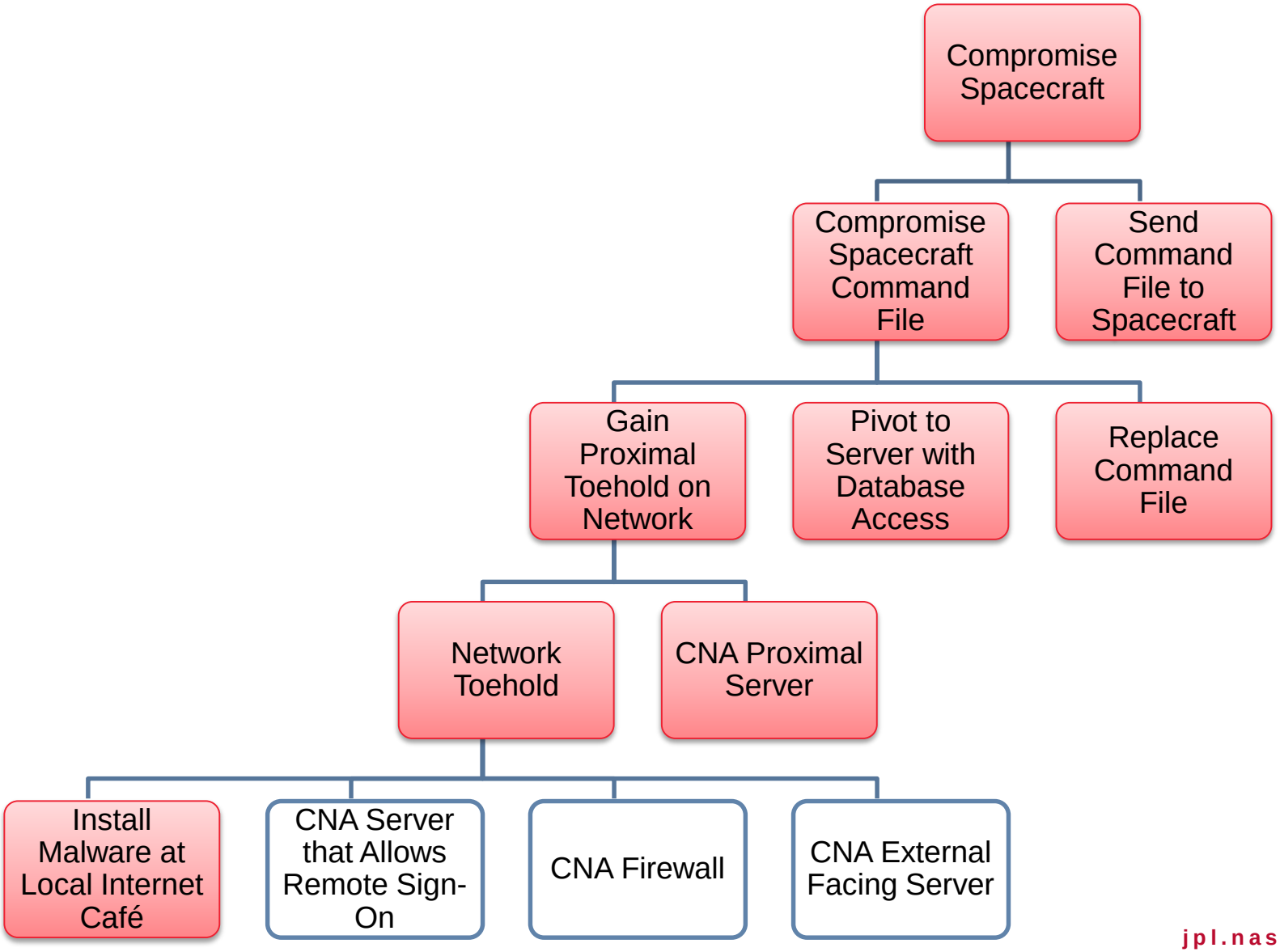


Algorithm for Paths from Entry Nodes to Root of Attack Tree

- Get all paths to root node:
  - Recursive traversal from root node to entry node
    - Check whether node's parent has condition AND or OR
      - If OR: node will be added to the path without its individual siblings
      - If AND: node will be added to path along with its siblings and their subtrees
  - Algorithm terminates when all paths are added from all entry nodes to root node

- Prune list of all paths for those starting with the entry node that the user selected

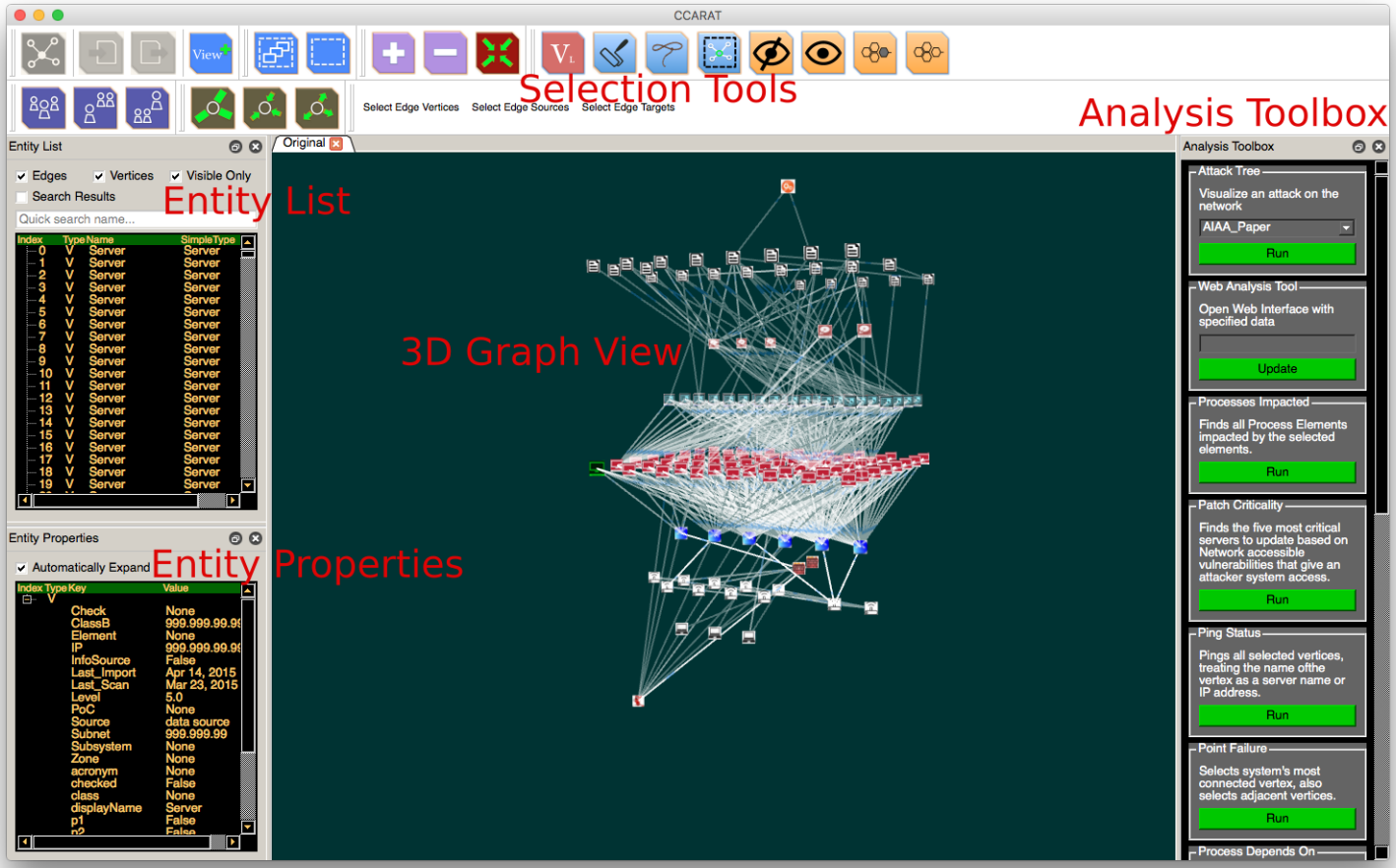
Path in the Attack Tree



Cyber Analysis Visualization Environment (CAVE)

Cyber Analysis Visualization Environment (CAVE)

- CAVE provides a user-interface to interact with the system-model network graph.

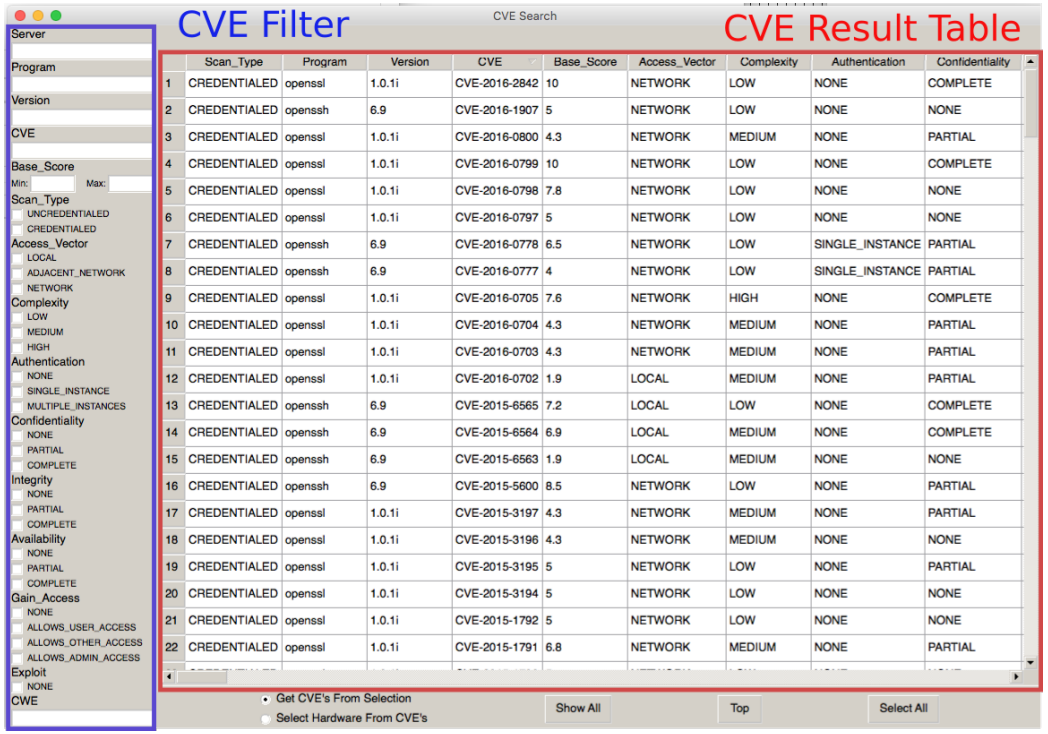


Analytical Capabilities of CAVE

- 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 of 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

Impact Assessment with CAVE

Traversing through the Network Model

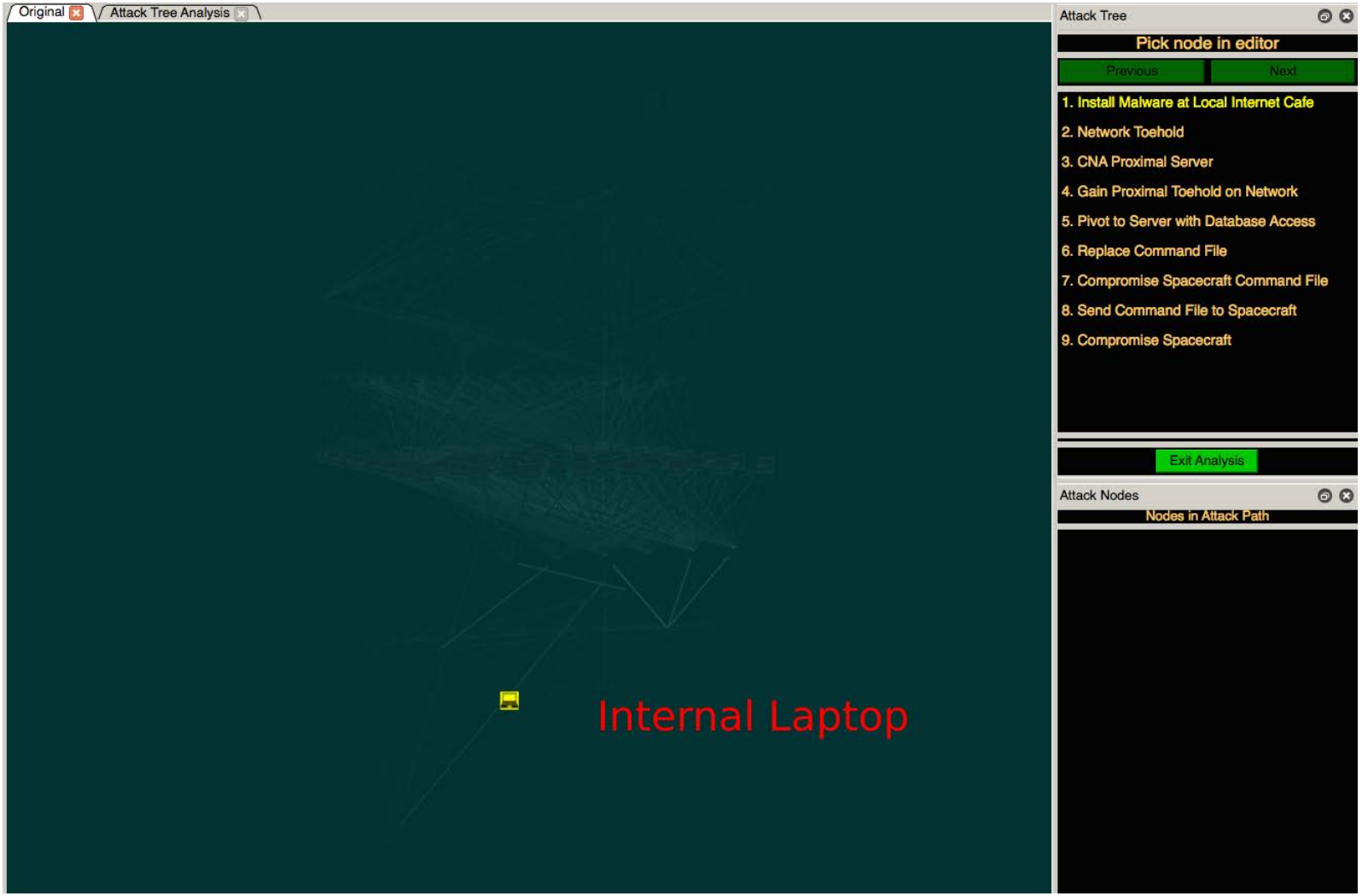
- A user selects an entry node of the attack tree.
  - This selection gives an attack path in the tree.

- 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**)

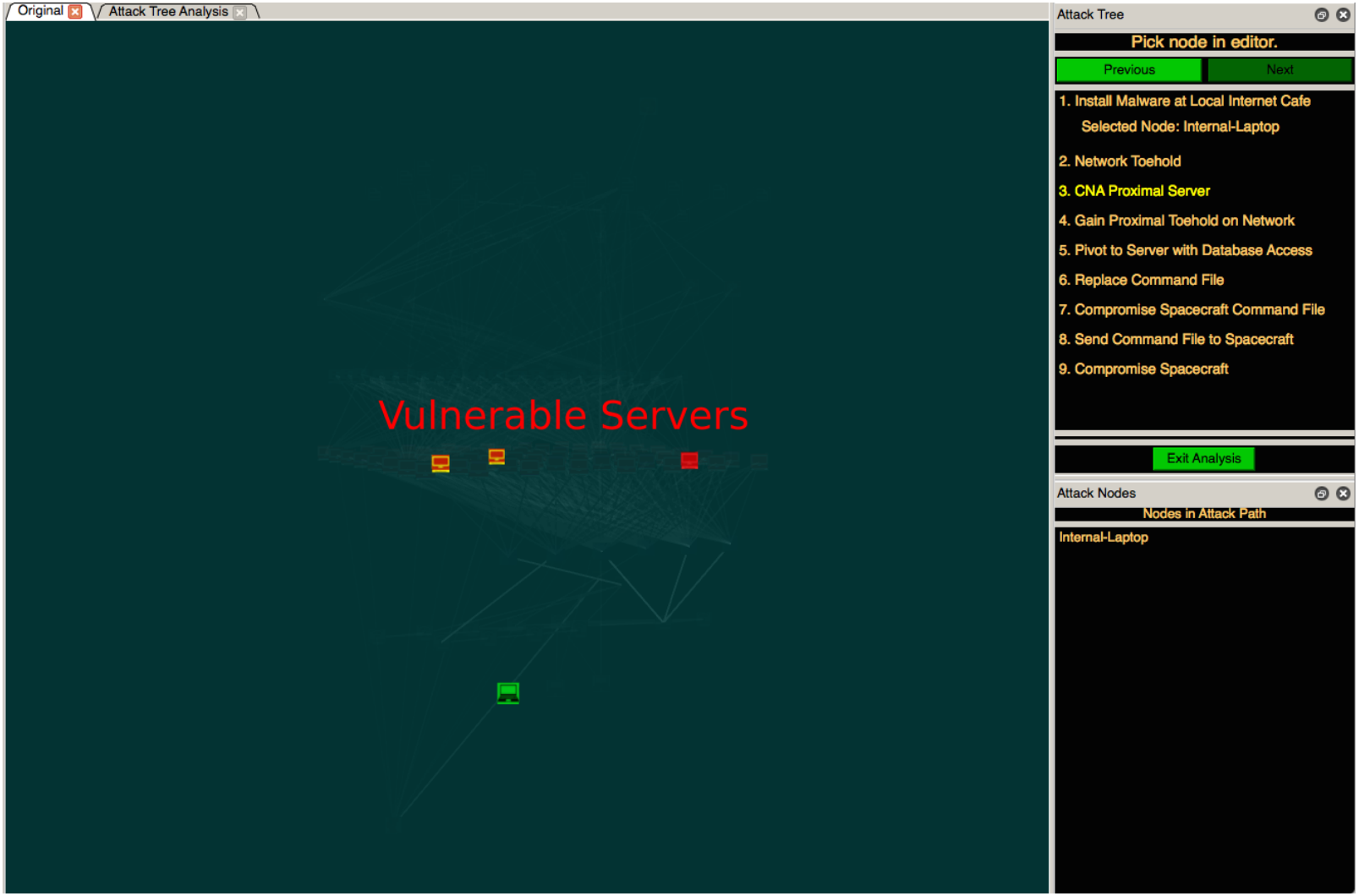
- The User then proceeds through the attack path pivoting in the system model to the selected nodes if possible.

Demo

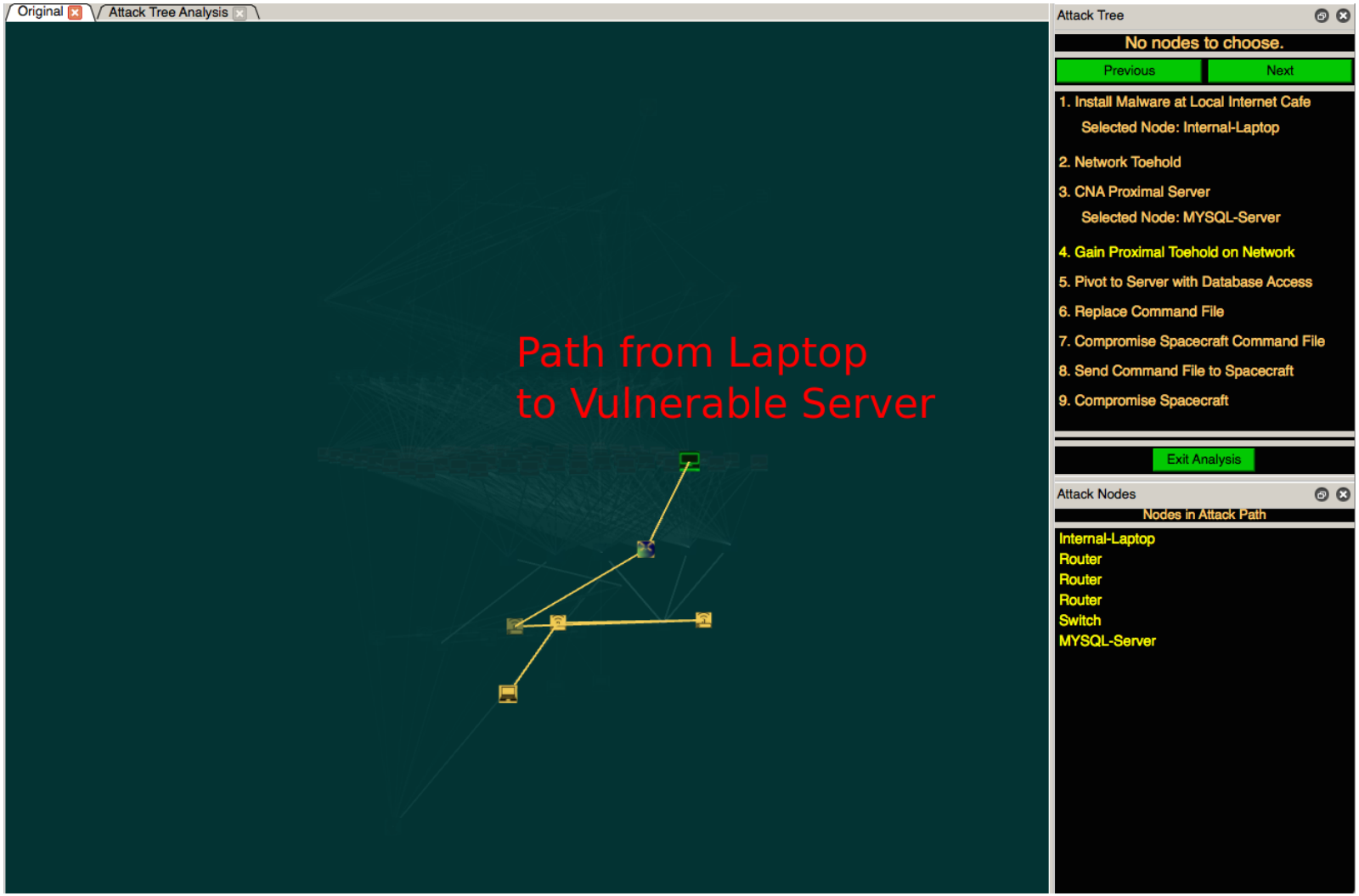
Impact Assessment Example



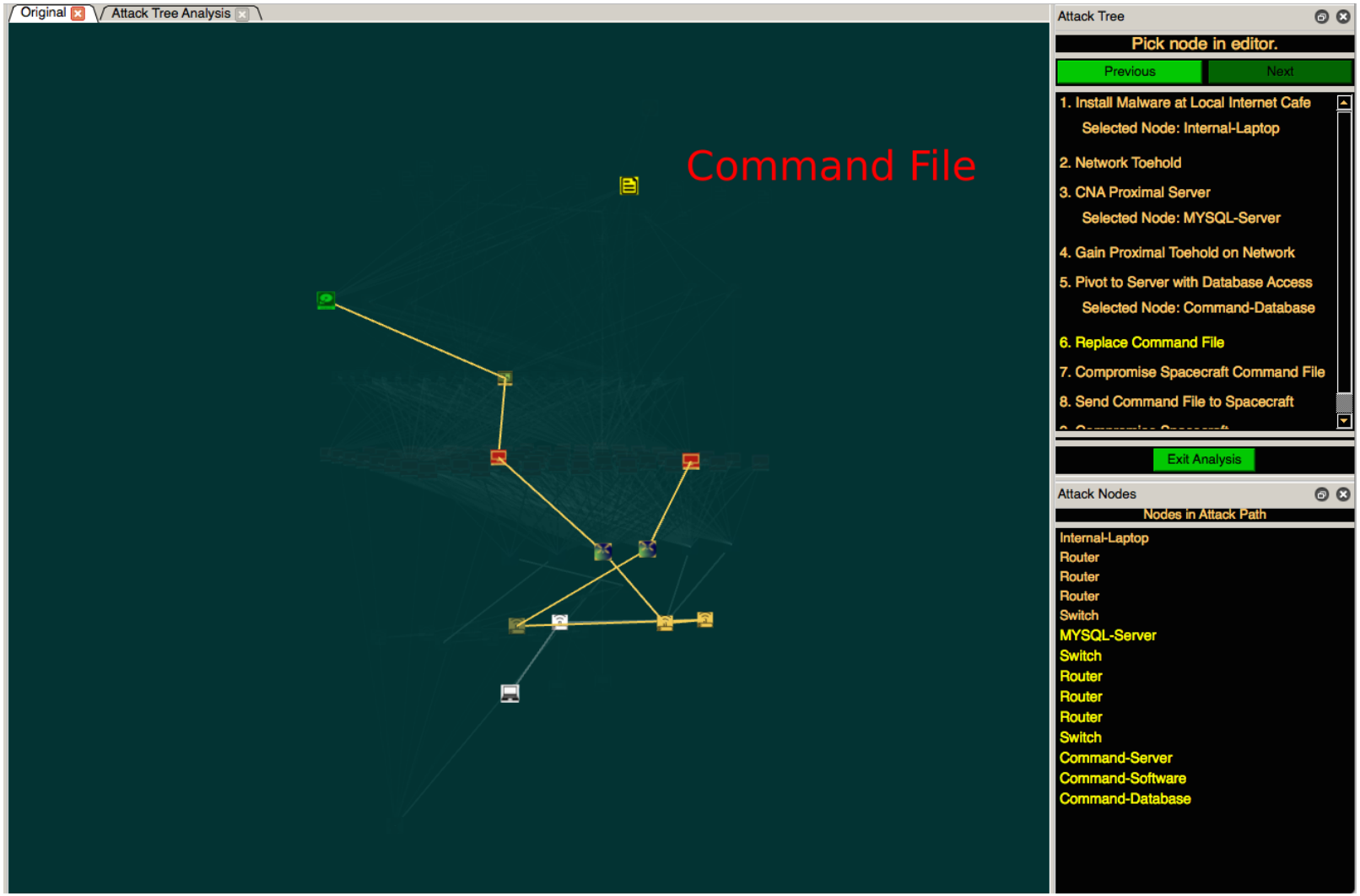
Impact Assessment Example



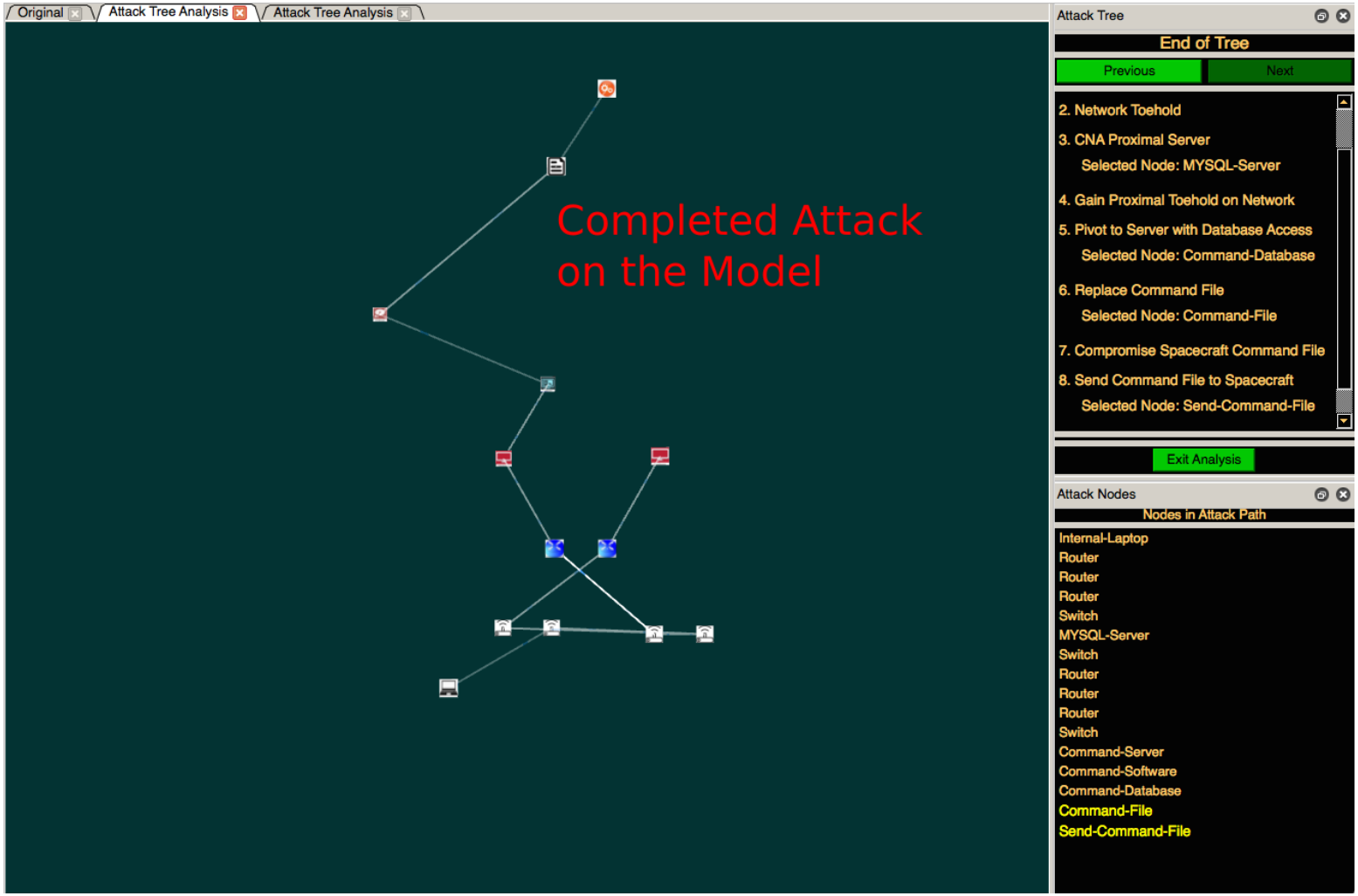
Impact Assessment Example



Impact Assessment Example



Impact Assessment Example



Conclusion and Future Work

Contributions

- Hybrid methodology for cyber risk assessment based on attack tree threat models.
- Simple, pragmatic approach to annotating attack trees.
- Algorithm to execute annotated attack trees on a multi-layered model.
- Visual perspective to better enable visualization of a multi-layered network.

Conclusion

- Created a way for a cyber-SME to quickly assess the impact of low-level cyber events on high-level mission objectives.

- Interactive visualization environment enabling an SME to visualize the propagation of an attack.

Future Work

- Probabilistic Attack Trees
  - Attach Probability of attack/success to the nodes of the attack trees
  - Gives the most likely path an attacker will take
- Automated Parsing of Attack Trees
  - Parse the written language in order to speed up annotation
- Inclusion of Countermeasure
  - Allows an SME to plan defensive measures to stop an attack

Jet Propulsion Laboratory
California Institute of Technology

jpl.nasa.gov

The Threat Landscape

- January, 2016 – GSFC, GRC, and AFRC. Drone data and command authority hack
  http://www.infowars.com/hackers-allegedly-hijack-drone-after-massive-breach-at-nasa/
- September, 2014 – National Oceanic and Atmospheric Administration (NOAA) – Chinese hackers breached computer networks to distort operational data coming from U.S. satellites
  https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html
- November, 2011 – 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
- May, 2011 – Goddard Earth Observation System – a hacker gained access to information contained on servers for the satellite-based Earth observation system
  http://threatpost.com/en_us/blogs/hack-targets-nasas-earth-observation-system-051711
- June, 2011 – Lockheed Martin was attacked using data obtained from the March RSA attack, unclear what was lost from Lockheed
  http://www.pcmag.com/article2/0,2817,2386512,00.asp
- **2009 – Johns Hopkins University Applied Physics Laboratory – the lab was removed from all external network connections for a month due to the detection of hidden malware and stolen data**
  http://weblogs.baltimoresun.com/news/technology/2009/06/johns_hopkins_apl_site_hacked.html
- **2008 (reported Oct. 2011) - Terra and Landsat 7 – spacecraft compromised from ground systems**
  http://www.bloomberg.com/news/2011-10-27/chinese-military-suspected-in-hacker-attacks-on-u-s-satellites.html
- 2007 – NASA Kennedy Space Center – a rogue program penetrated KSC networks, surreptitiously gathered data from computers in the Vehicle Assembly Building, and removed that data through covert channels
  http://www.kepstein.com/2008/11/20/network-security-breaches-plague-nasa/

Features of CAVE

- System Model represented by a 3D Graph View
  - 3D Camera System to easily change perspective towards model
- Multiple Graph layout algorithms
  - 2D and 3D layouts
- Searching based on name and type of entities in model.
- Selection of entities to navigate model and view properties of a given entity
  - Is performed by:
    - Mouse Clicks
    - Selection Tools: lasso, rectangle, and paint selection
    - Graph Semantics
      - ie: Select all neighbors, Select incident edges, etc