Visualizing Attack Graphs, Reachability, and Trust Relationships with NAVIGATOR*

Matthew Chu, Kyle Ingols, Richard Lippmann,

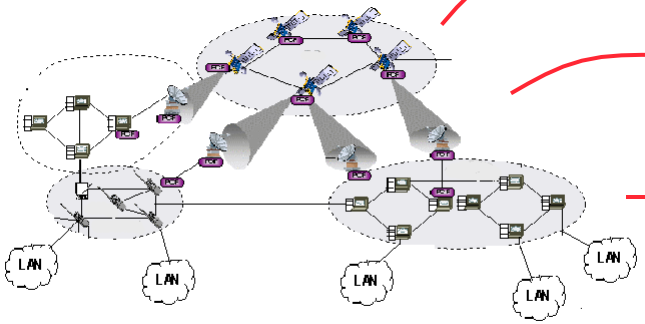
Seth Webster, Stephen Boyer

MIT Lincoln Laboratory

14 September 2010

*This work is sponsored by the United States Air Force under Air Force Contract FA8721-05-C-0002. Opinions, interpretations, conclusions and recommendations are those of the authors and are not necessarily endorsed by the United States Government

A Defender's Primary Advantage is Detailed Network Knowledge – This Needs to Be Used Effectively!



CISCO

SIDEWINDER G2 SECURITY APPLIANCE

eEye Digital Security®

Nessus

OVAL oval.mitre.org

CVE cve.mitre.org

Specify Asset Values and Adversary

Infer Network Topology From Infrastructure Rules

Discover Vulnerabilities

Define Vulnerability Requirements/Effects

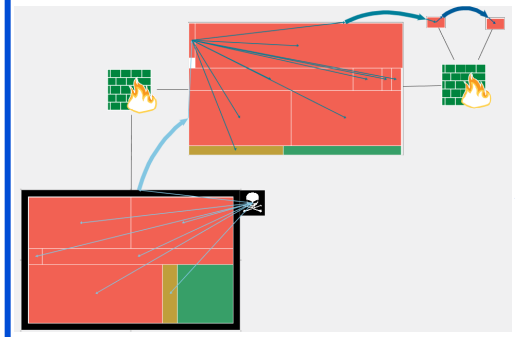
A Tool Named NetSPA Integrates This Data and Supports "What If" Experiments

Infer Network Topology

Construct Network Model

Compute Host-to-Host Reachability

Attack Graph



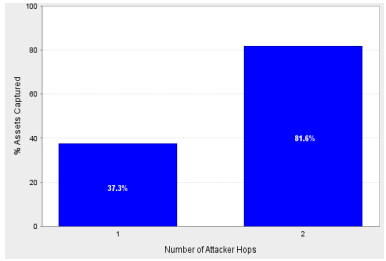
What If ?

Adversary

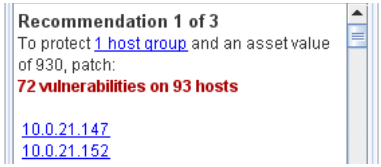
Defenses

Host Asset Values

Metrics



Recommendations

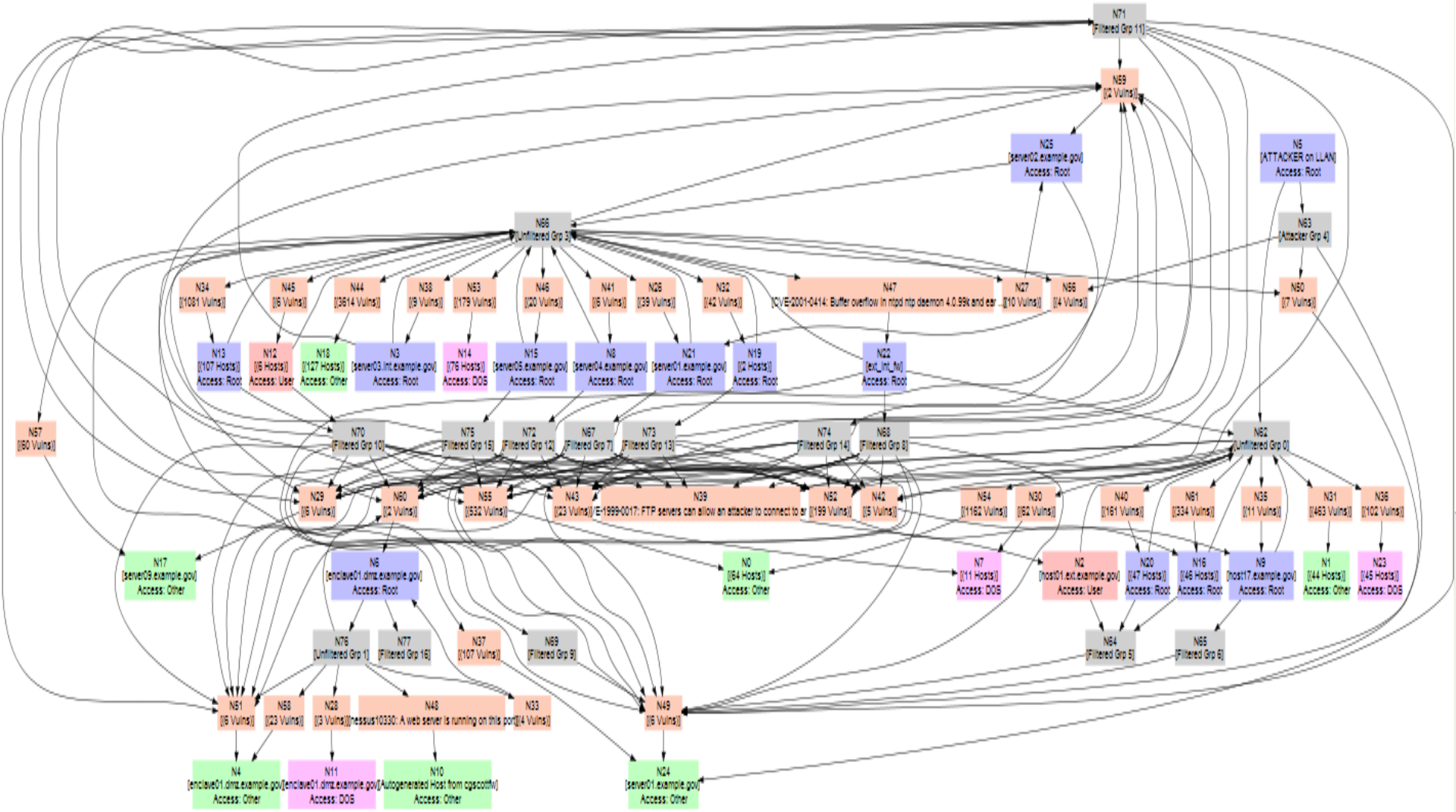


CISCO

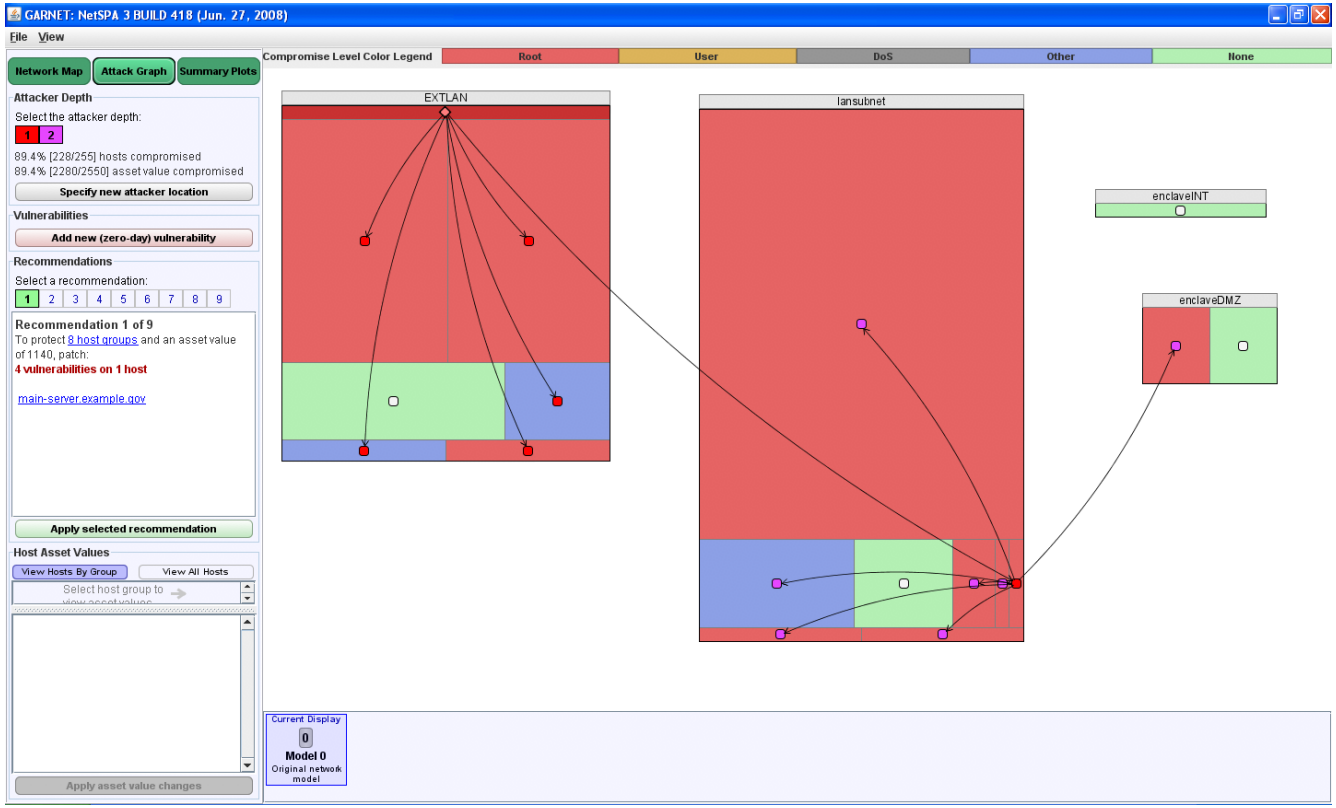
Nessus

NVD

Attack Graphs Can Be Difficult to Understand

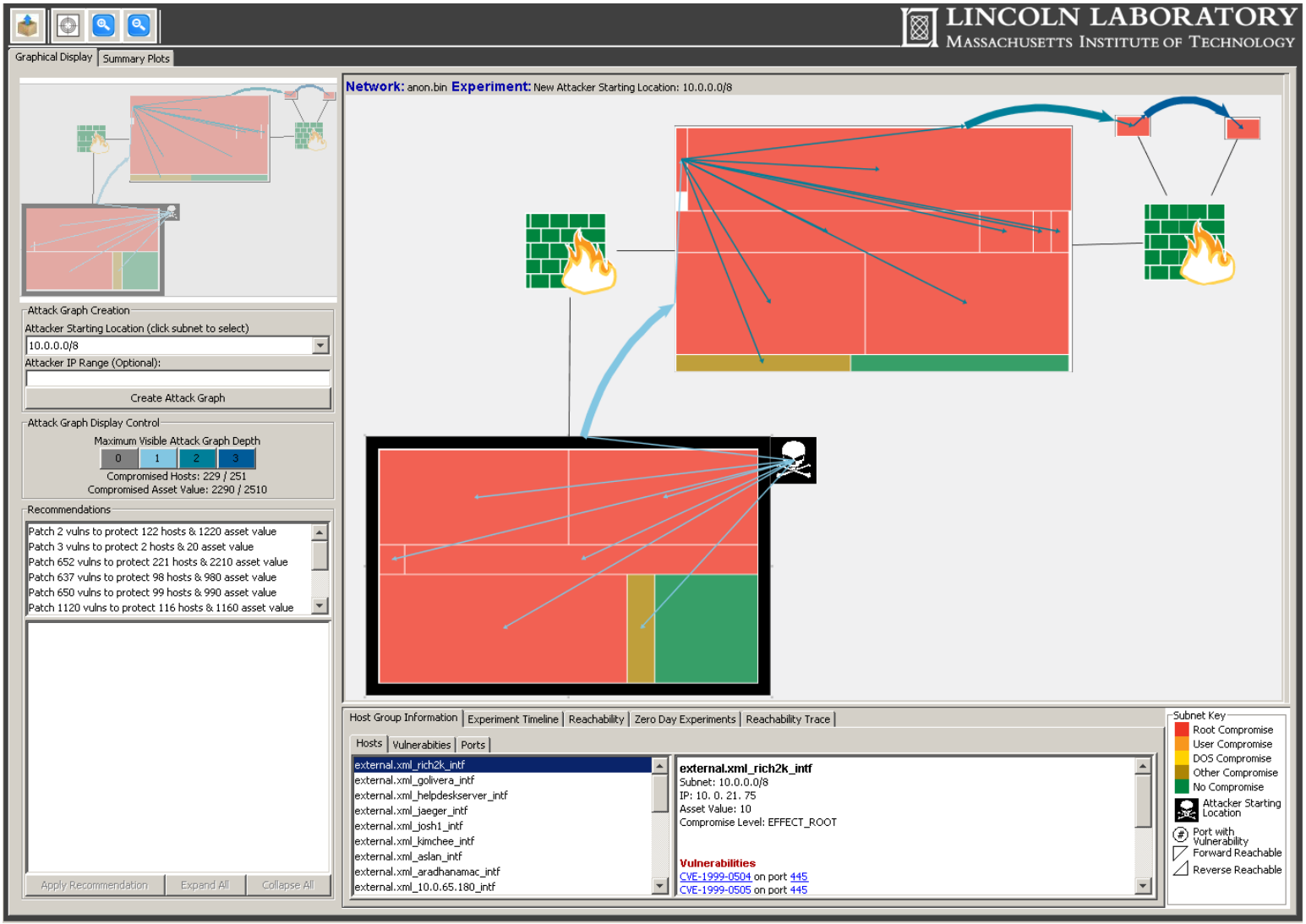


Previous NetSPA GUI: GARNET



- Many of its key features have been kept intact
  - Ability to perform "What-If" experiments
  - Network level metrics
- Major shortcomings have been addressed

NAVIGATOR


LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
Graphical Display
Summary Plots
Network: anon.bin Experiment: New Attacker Starting Location: 10.0.0.0/8
Attack Graph Creation
Attacker Starting Location (click subnet to select)
10.0.0.0/8
Attacker IP Range (Optional):
Create Attack Graph
Attack Graph Display Control
Maximum Visible Attack Graph Depth
0 1 2 3
Compromised Hosts: 229 / 251
Compromised Asset Value: 2290 / 2510
Recommendations
Patch 2 vulns to protect 122 hosts & 1220 asset value
Patch 3 vulns to protect 2 hosts & 20 asset value
Patch 652 vulns to protect 221 hosts & 2210 asset value
Patch 637 vulns to protect 98 hosts & 980 asset value
Patch 650 vulns to protect 99 hosts & 990 asset value
Patch 1120 vulns to protect 116 hosts & 1160 asset value
Apply Recommendation
Expand All
Collapse All
Host Group Information
Experiment Timeline
Reachability
Zero Day Experiments
Reachability Trace
Hosts
Vulnerabilities
Ports
external.xml_rich2k_intf
external.xml_golivera_intf
external.xml_helpdeskserver_intf
external.xml_jaeger_intf
external.xml_josh1_intf
external.xml_kimchee_intf
external.xml_aslan_intf
external.xml_aradhanamac_intf
external.xml_10.0.65.180_intf
external.xml_rich2k_intf
Subnet: 10.0.0.0/8
IP: 10. 0. 21. 75
Asset Value: 10
Compromise Level: EFFECT_ROOT
Vulnerabilities
CVE-1999-0504 on port 445
CVE-1999-0505 on port 445
Subnet Key
Root Compromise
User Compromise
DOS Compromise
Other Compromise
No Compromise
Attacker Starting Location
Port with Vulnerability
Forward Reachable
Reverse Reachable

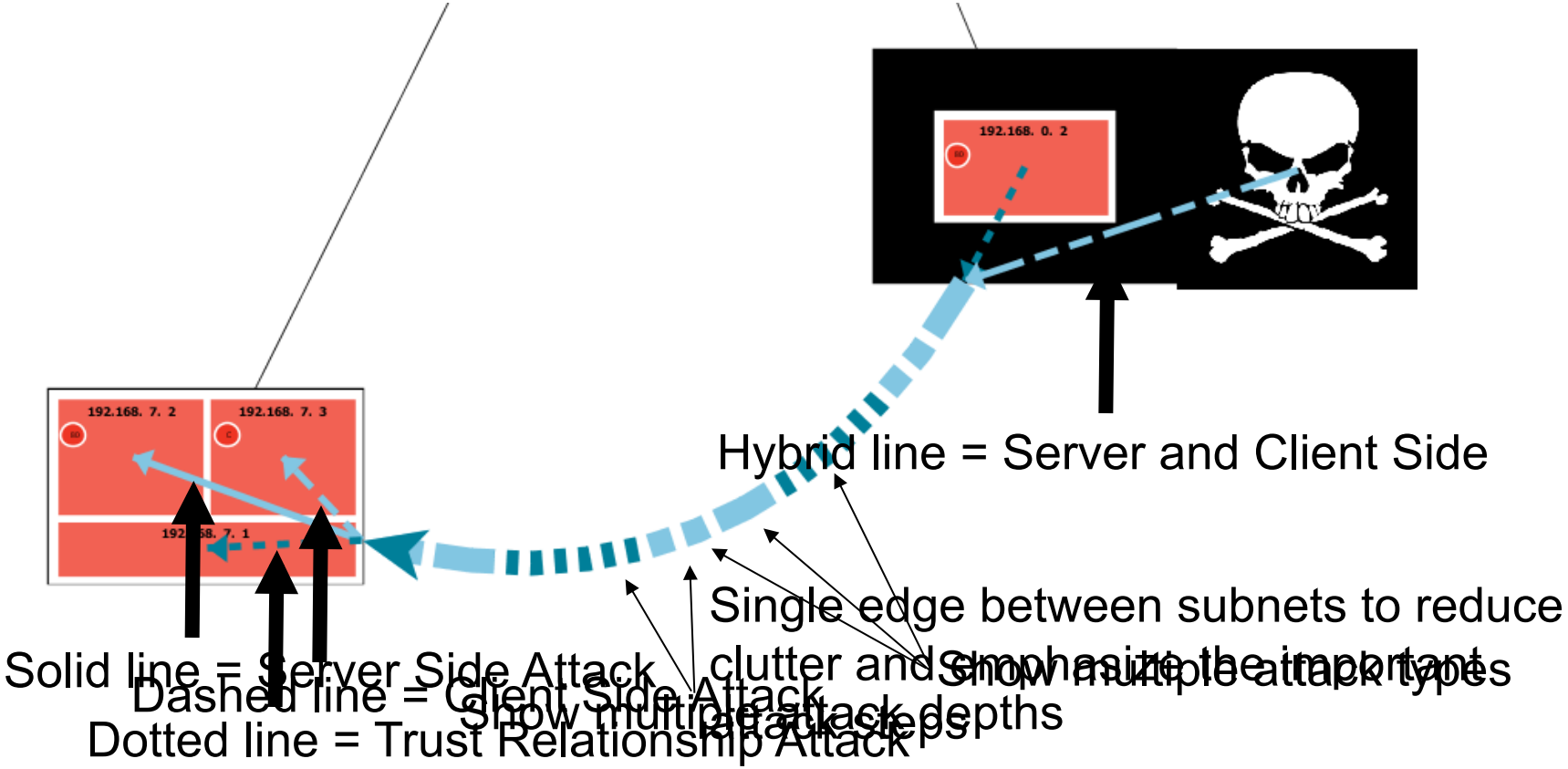
Outline

- Introduction
- **New Features**
  - Client side vulnerabilities and trust relationships
  - Network infrastructure
  - Host level zooming
- **Enhancements**
- **Conclusion**

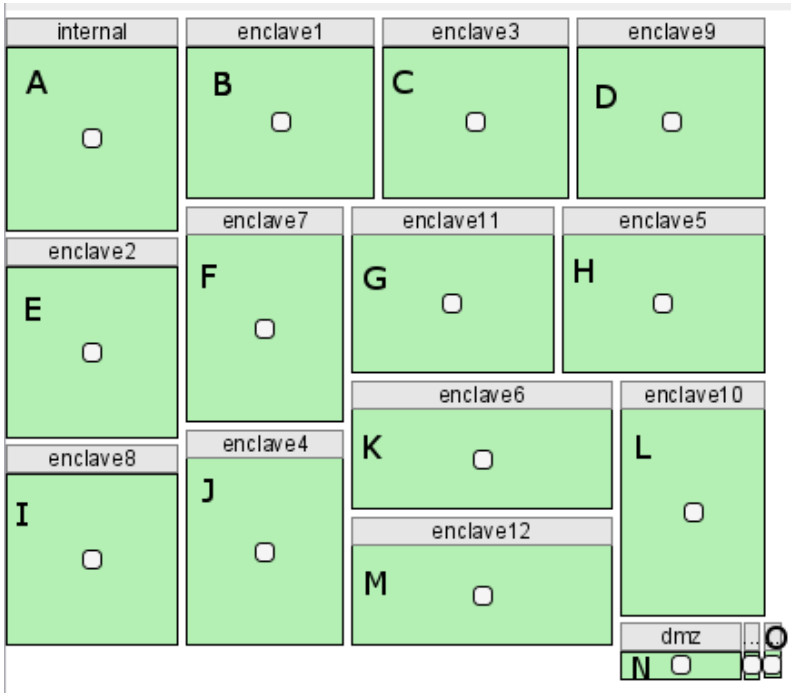
Client-side Attacks and Trust Relationships

- Client-side attacks are an increasingly common attack vector that rely on vulnerable client software connecting to a malicious server
- Attackers also exploit trust relationships, where certain machines are given high level privileges on other machines without passwords or other verification
- Differentiating between server-side, client-side, and trust relationship attacks is important because their respective countermeasures vary greatly

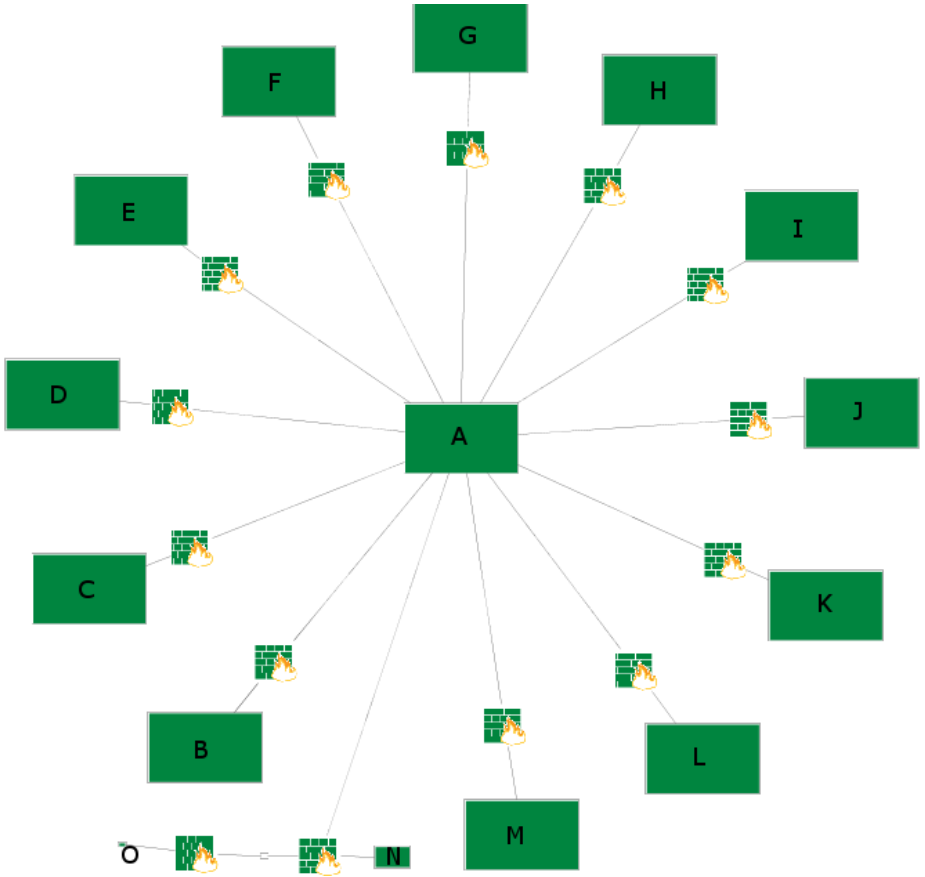
Differentiating Between Attack Types



Show Infrastructure

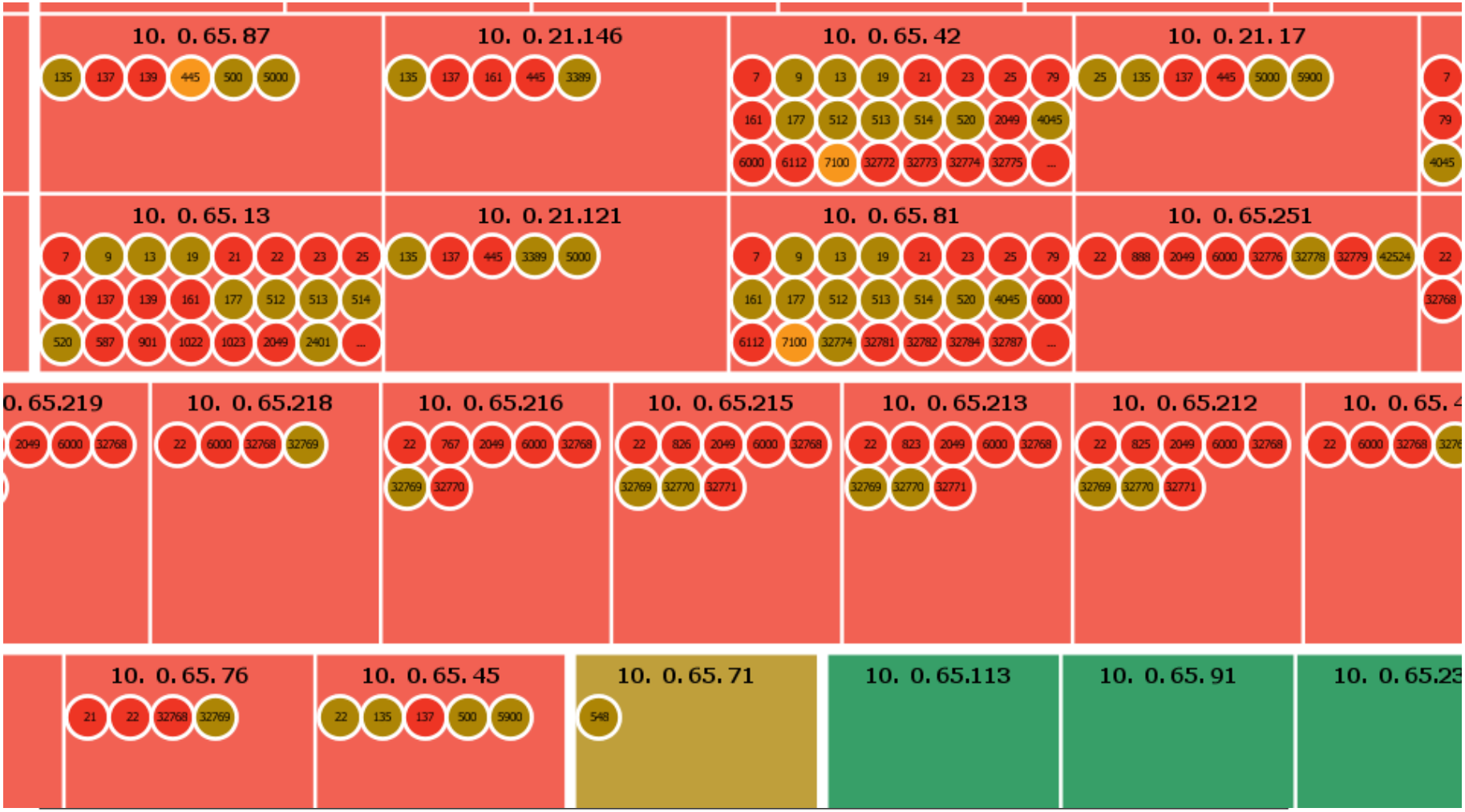


GARNET's view



NAVIGATOR's view

Allow Zooming to the Host Level



Outline

- Introduction
- New Features
- **Enhancements**
  - **Host Group Visualization**
  - **Reachability**
  - **Speed**
- **Conclusion**

Host Group Visualization

- GARNET's method: the strip treemap algorithm
  - Did not take into account asset values
  - Gives no guarantees about aspect ratios

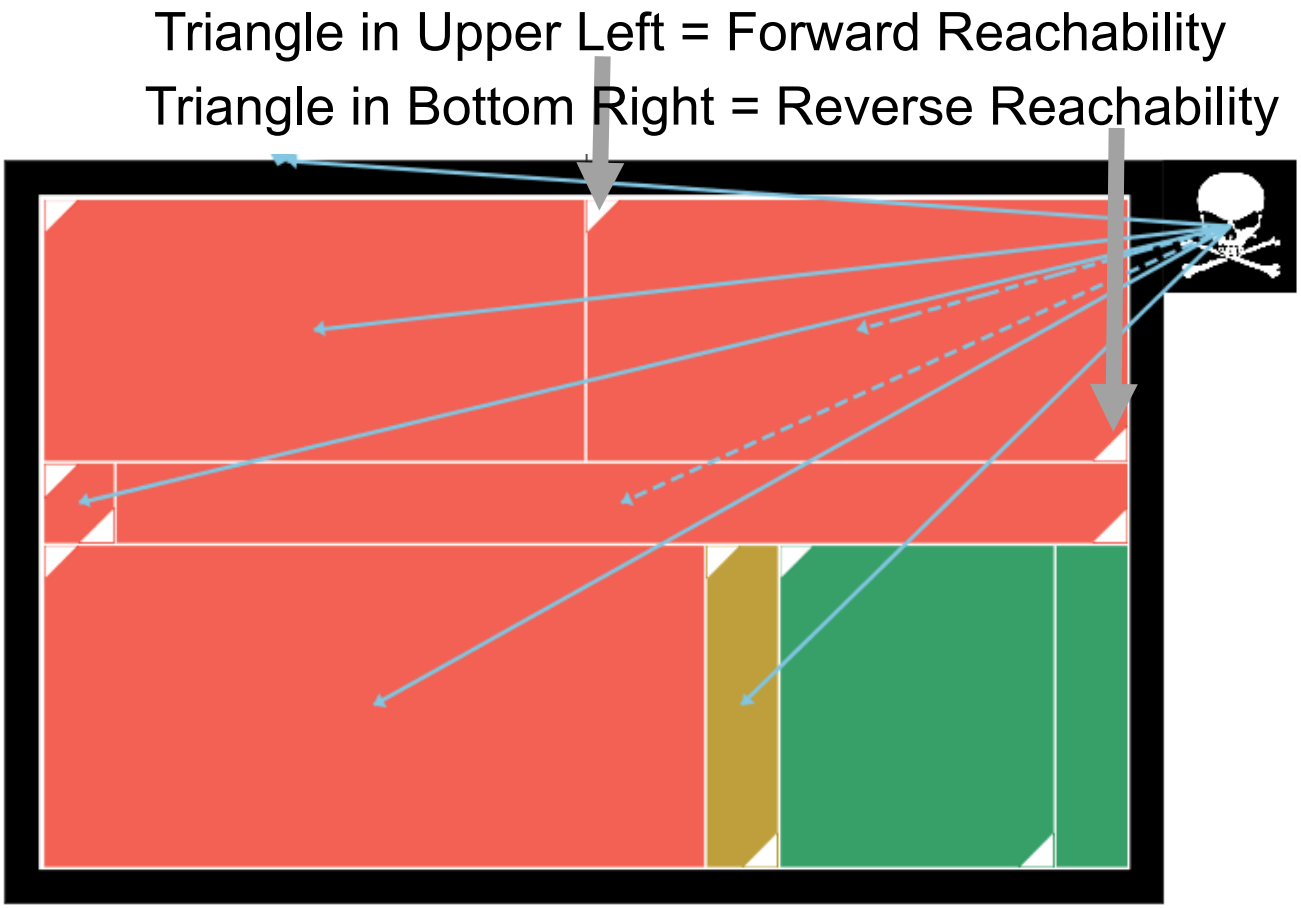
- Criteria for choosing NAVIGATOR's approach
  - Handle multiple asset values
  - Only a small amount of wasted space
  - Rectangular shapes
  - Maintain order

Solution: Modified Strip Treemap Algorithm

- Guarantees minimum dimension for all rectangles by altering their dimensions when placed
- Cost of this modification is some wasted space

Improved Visualization of Reachability

- **Uses symbols instead of arrows to reduce clutter**
- **Shows reachability and attack graph edges at the same time to identify latent threats**



Improved System Speed

- NetSPA is capable of analyzing the large, complex networks often found in the government or large corporations
- Because of preloading, GARNET was slow on some of the more data intensive operations
- NAVIGATOR loads information on demand
  - Engine is often fast enough that user cannot distinguish between preloading and on demand loading
  - For other situations, information is shown as it is calculated
  - On a network of 20,000 hosts spread over 100 subnets, NAVIGATOR loaded in 1 second but GARNET took over 90 seconds
- New backend graph format specifically designed for visualization allows faster analysis

Outline

- Introduction
- New Features
- Enhancements
- **Conclusion**

Conclusion

- NAVIGATOR visualizes attack graphs and network reachability
- First attack graph visualization tool to display effect of client-side, trust-based, and credential-based attacks
- Greatly improves NetSPA's previous GUI, GARNET
  - Displays infrastructure devices
  - Displays host-level data
  - Improved visualization of host groups and reachability
  - Improved overall system speed