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!

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

- Recommendation 1 of 3
  To protect 1 hostgroup and an asset value of 930, patch:
  72 vulnerabilities on 93 hosts
  10.0.21.147
  10.0.21.152

NVD

CISCO

Nessus

MIT Lincoln Laboratory
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
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

Solid line = Server Side Attack
Dashed line = Client Side Attack
Dotted line = Trust Relationship Attack

Hybrid line = Server and Client Side

Single edge between subnets to reduce clutter and emphasize the important attack steps.
Show multiple attack types
Show multiple attack depths
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

Triangle in Upper Left = Forward Reachability
Triangle in Bottom Right = Reverse Reachability
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