ENGINEERING AT ILLINOIS

CSL: COORDINATED SCIENCE LAB

NP-View: Automatic Analysis of Process Control Network Firewall Configurations

Bill Sanders

University of Illinois

with Robin Berthier, David Nicol, Edmond Rogers, Mouna Seri, and Sankalp Singh

The Challenge: Providing Trustworthy Smart Grid Operation in Possibly Hostile Environments

- **Trustworthy**
  - A system which does what is supposed to do, and nothing else
  - Availability, Security, Safety, …
- **Hostile Environment**
  - Accidental Failures
  - Design Flaws
  - Malicious Attacks
- **Cyber Physical**
  - Must make the whole system trustworthy, including both physical & cyber components, and their interaction.

TCIPG Vision and Research Focus

Vision: Create technologies which improve the design of a resilient and trustworthy cyber infrastructure for today's and tomorrow's power grid, so that it operates through attacks

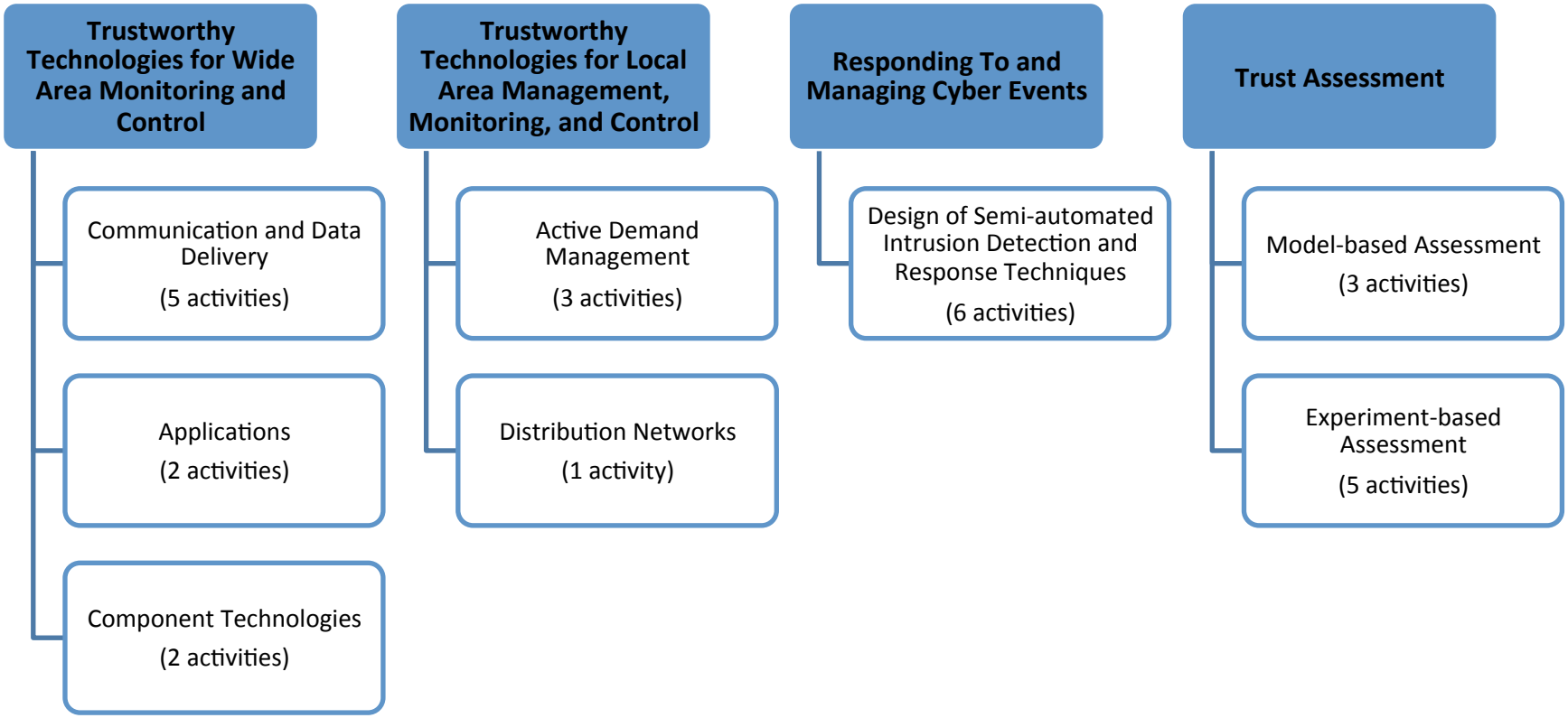
Research focus: Resilient and Secure Smart Grid Systems

- Protecting the cyber infrastructure
- Making use of cyber and physical state information to detect, respond, and recover from attacks
- Supporting greatly increased throughput and timeliness requirements for next generation energy applications and architectures
- Quantifying security and resilience

TCIPG Statistics

- Builds upon $7.5M NSF TCIP CyberTrust Center 2005-2010
- $18.8M over 5 years ($3.8M cost share)
- Funded by Department of Energy, Office of Electricity and Department of Homeland Security, Cyber Security Division, HSARPA, Office of Science and Technology
- 4 Universities
  - Dartmouth College
  - University of California at Davis
  - University of Illinois at Urbana-Champaign
  - Washington State University
- 23 Faculty, 17 Technical Staff, 38 Graduate Students, 9 Ugrad Students, 2 Admin Staff worked on the project in FY 2013

TCIPG Technical Clusters and Threads



Power and Energy applets

32,000 visits in the past year

1000 CD's distributed

Tesla Town for the iPad and Android

5500 iTunes downloads

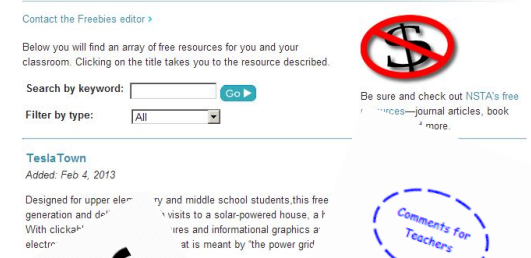
Available in Google play store

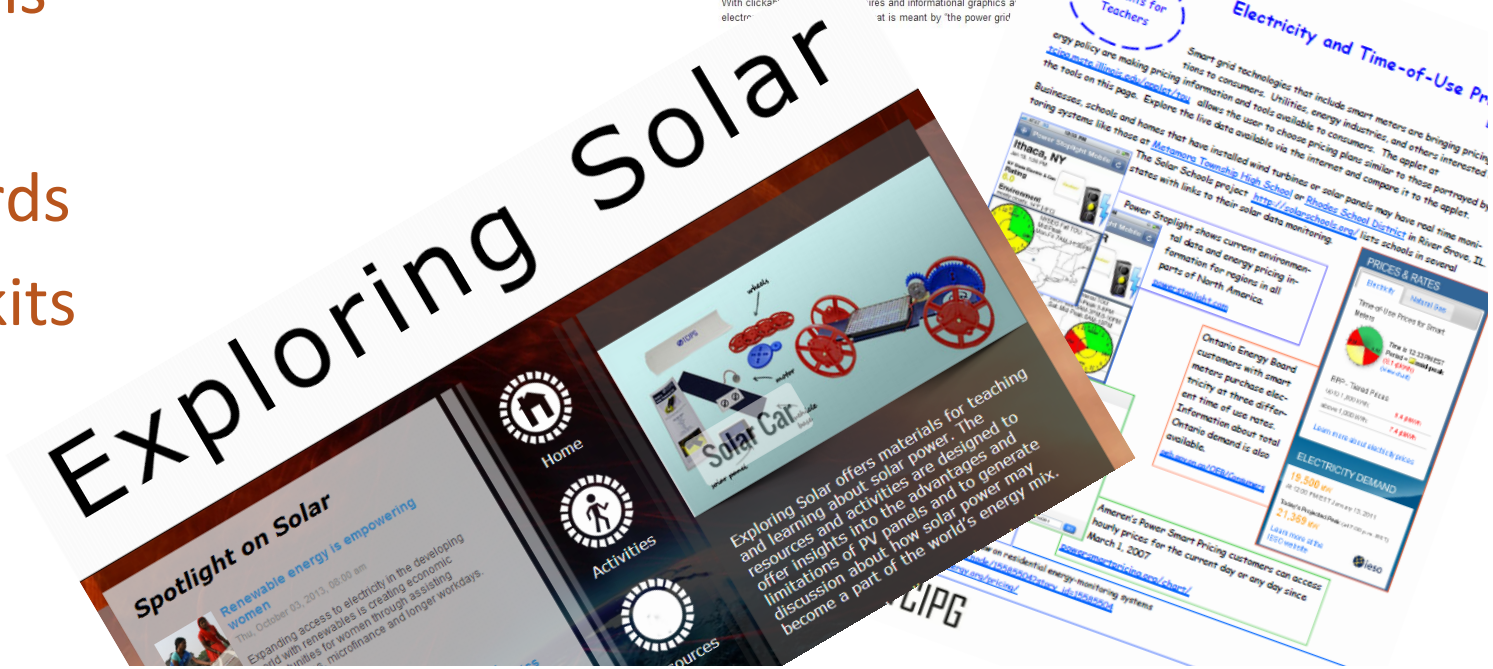
Lesson plans

Posters

Trading cards

Hands-on kits





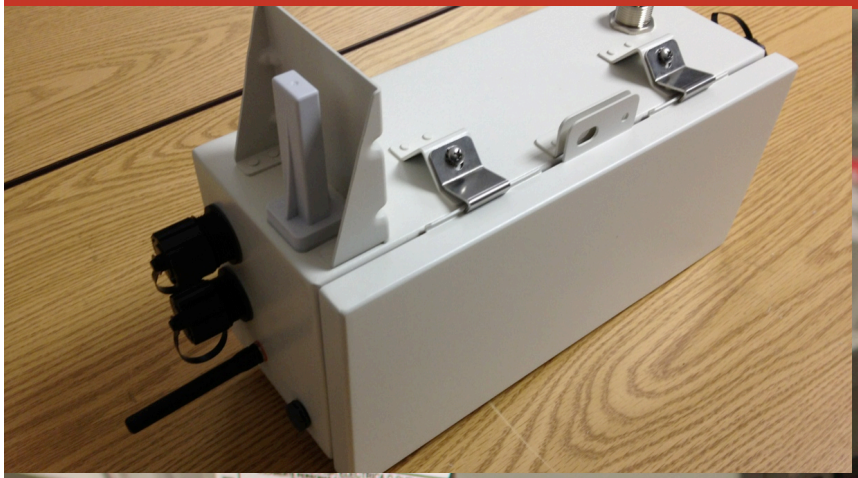
TCIPG Testbed

- A lab-contained but true-to-reality implementation of critical infrastructure
- Leverages over $6.5 million worth of hardware and software (much of which is donated)
- Brings together power system equipment, emulation, and simulation
  - Supports cutting-edge research on grid topics from generation to consumption
- Automated for efficient and effective provisioning of power and cyber assets per experiment
- Used for internal TCIPG research, collaboration with national labs, and projects with industry


CSL: COORDINATED SCIENCE LAB
Rack 1
Rack 2
Rack 3
Rack 4
Mu Dynamics
DELL

CSL: COORDINATED SCIENCE LAB

CSL: COORDINATED SCIENCE LAB



CSL: COORDINATED SCIENCE LAB

TCIPG Collaborators and Event Attendence

Process Control Network Security Assessment Needs

-
-
-
-

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REDACTED FROM THIS PUBLIC VERSION

October 31, 2012

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

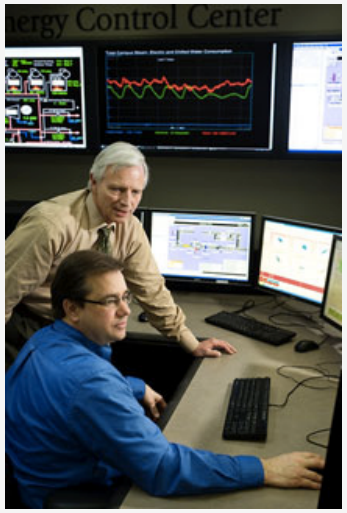
Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req.	VRF	Total Penalty
Reliability*First* Corporation	URE1	1448	RFC201100957	CIP-002-1	R1	Medium[5]	$725,000
Reliability*First* Corporation	URE1	1448	RFC201100958	CIP-002-1	R2	High[6]	

http://www.nerc.com/filez/enforcement/Public_FinalFiled_NOP_NOC-1448.pdf

what we learned

Interview count: 30

Energy Utilities

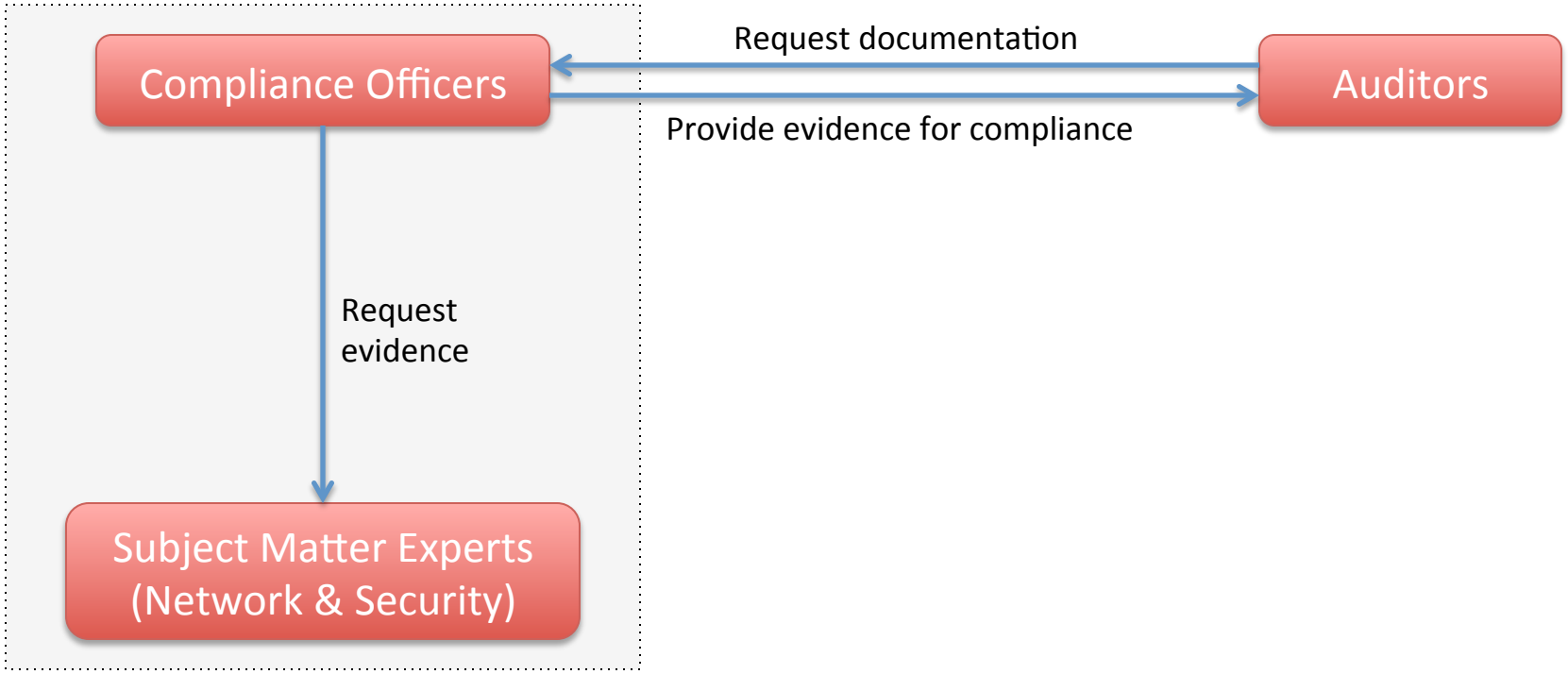


Audit

Auditors

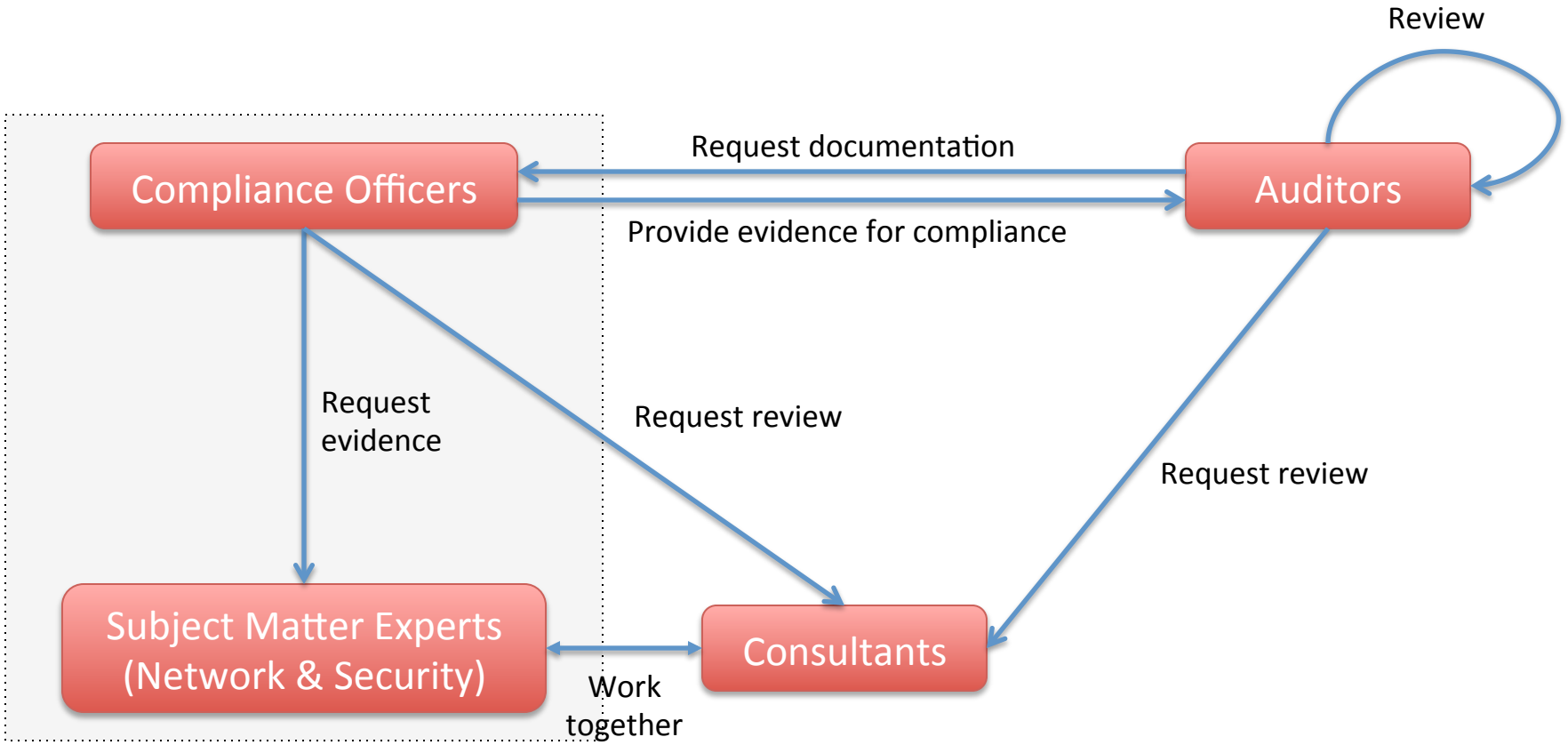
what we learned

Interview count: 40



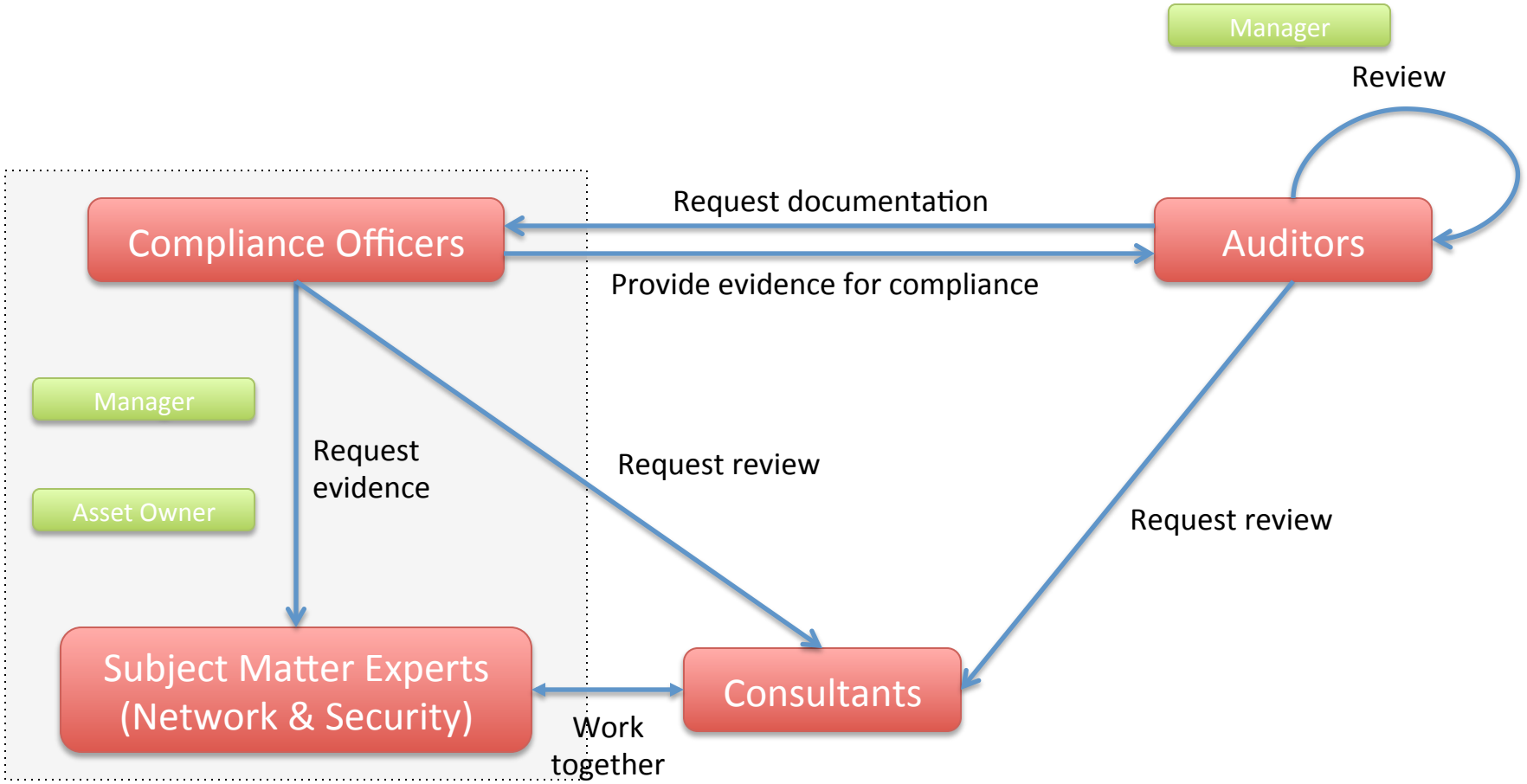
what we learned

Interview count: 50



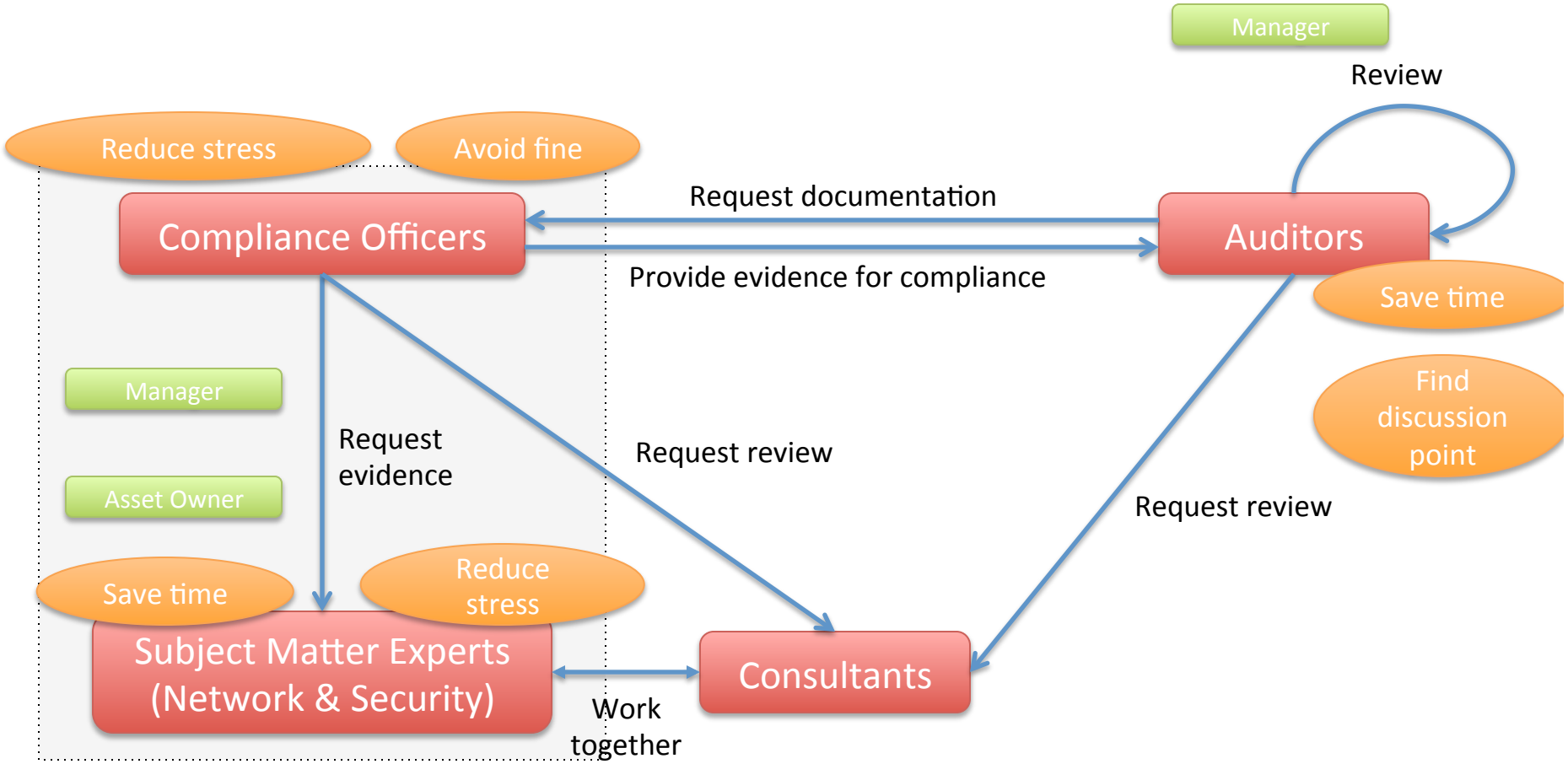
what we learned

Interview count: 60



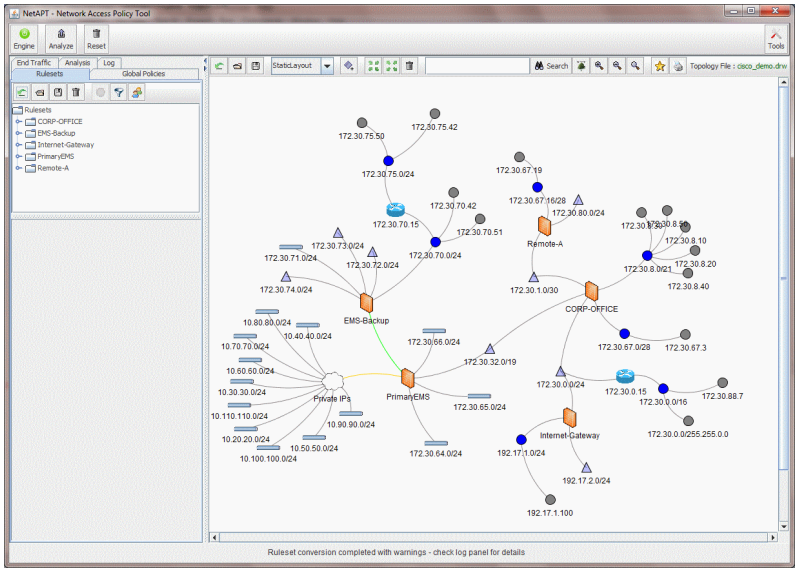
what we learned

Interview count: 70



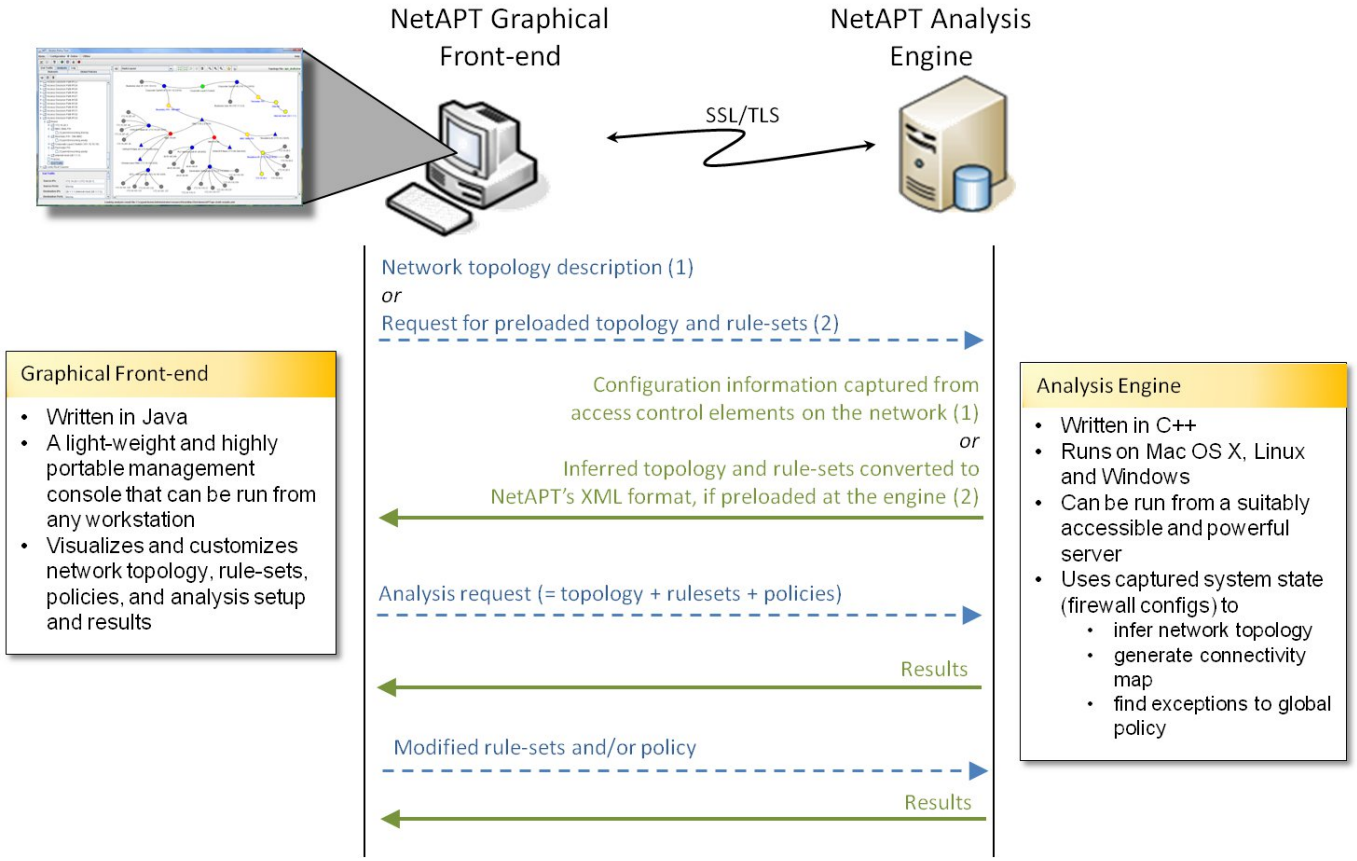
Approach

- The NP-View tool performs a comprehensive security policy analysis
  - Solve complex interactions in a system where multiple firewalls are deployed
  - Access policy implementation misconfiguration of security mechanisms is a major source of security vulnerability
- Highly-usable GUI with network mapping and exploration capabilities
- Automate most of the reporting process required during an audit



Key Features

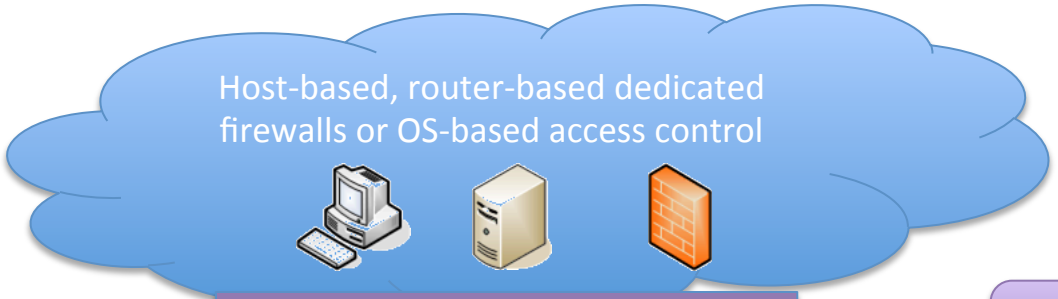
- Automated topology inference, even for complex configurations
- Scalable and complete state space exploration to identify network access violations exhaustively in few minutes, even for very large networks
- Patent issued in June 2012 on core engine algorithm (US 8209 738 B2)



Benefits

- Significantly reduces resources needed to comply with CIP regulations
  - Cut firewall rule analysis time
- Improves accuracy of security analysis
  - Reduces attack surface and mitigates human errors
  - Automates documentation effort
  - Reduces likelihood of getting fined
- Provides metrics to assess vulnerabilities and optimize network changes
  - Describe the network's defensive posture (reachability metrics)
  - Facilitate audit process (IP and service usage metrics)

Framework Overview

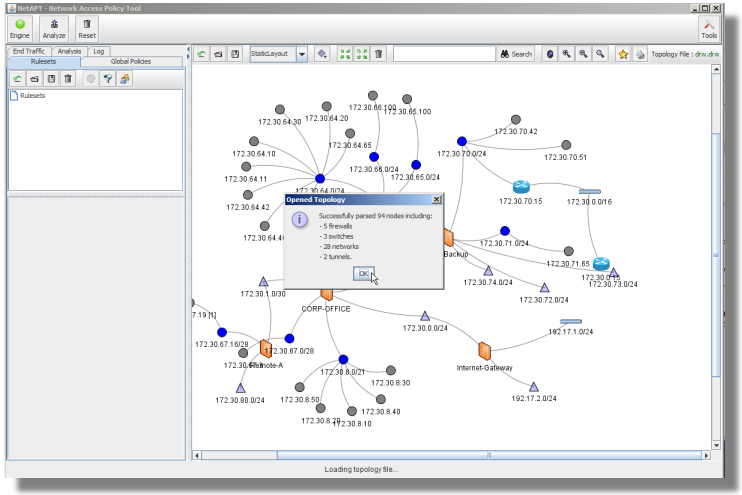


Securely import rule-sets

1. Parse Native Configuration Files

2. Infer topology:
- Inspecting routes
- Creating primary networks
- Marking VPN networks
- Creating nodes from group definitions
- Building border cloud of unmapped IP
- Saving results to XML files

3. Load model into engine:
- Looking up dynamic IP addresses
- Creating data structures to store rules
- Generating graph to store topology



Path Analysis

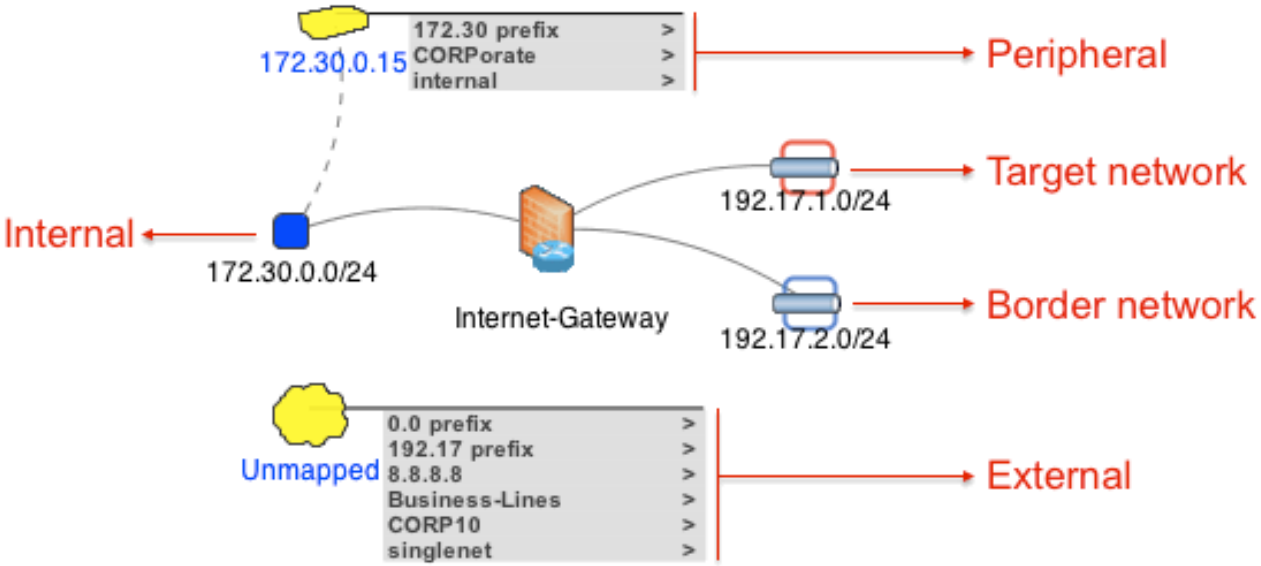
Queries can be sent from the GUI towards the engine

The engine keeps a model of the network in memory

Type of path analysis queries:

- **Exhaustive** path analysis
  - Return all possible paths in the network
  - Prone to scalability issues for large networks
- **End point** (a network or a host)
  - Return all possible paths originating or ending at the selected end point
- **Firewall**
  - Return all possible paths permitted by a selected firewall
  - Can be refined for a specific ACL and a specific rule
- **Tunnel**
  - Return all possible paths that go through a selected tunnel
- **Pair analysis**
  - Return all possible paths going from a selected source to a selected destination
  - Provide a "path halt" mode to troubleshoot why a path doesn't reach its destination

End Point Classification

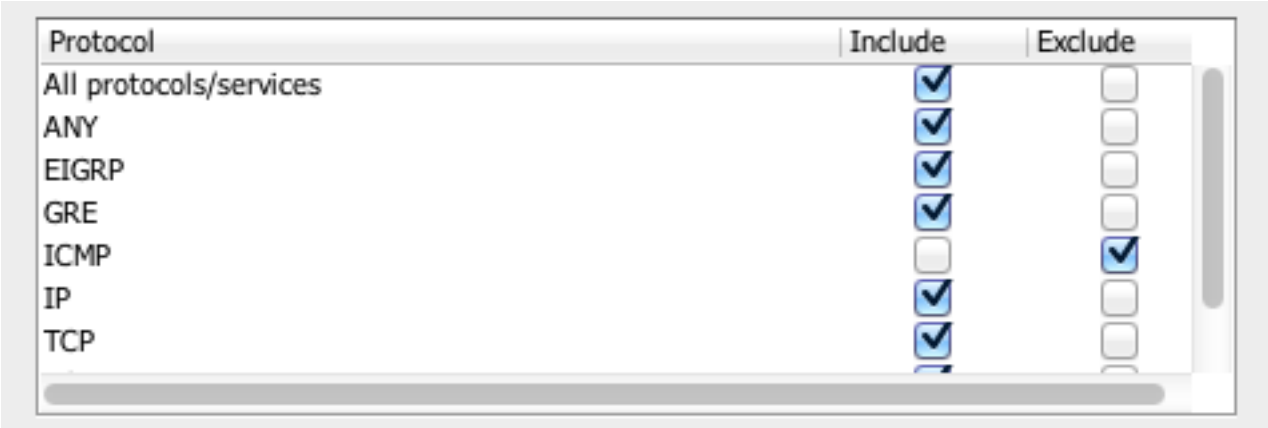


- Users can refine the analysis by selecting/deselecting categories of end points:
  - **Internal** networks and hosts are directly connected to a primary device
  - **External** networks and hosts are not directly connected to a primary device
  - **Peripheral** networks and hosts are mentioned in route tables and connected through a gateway
  - Networks can be marked as "**target**" and "**border**" for further refinement

Additional Analysis Options

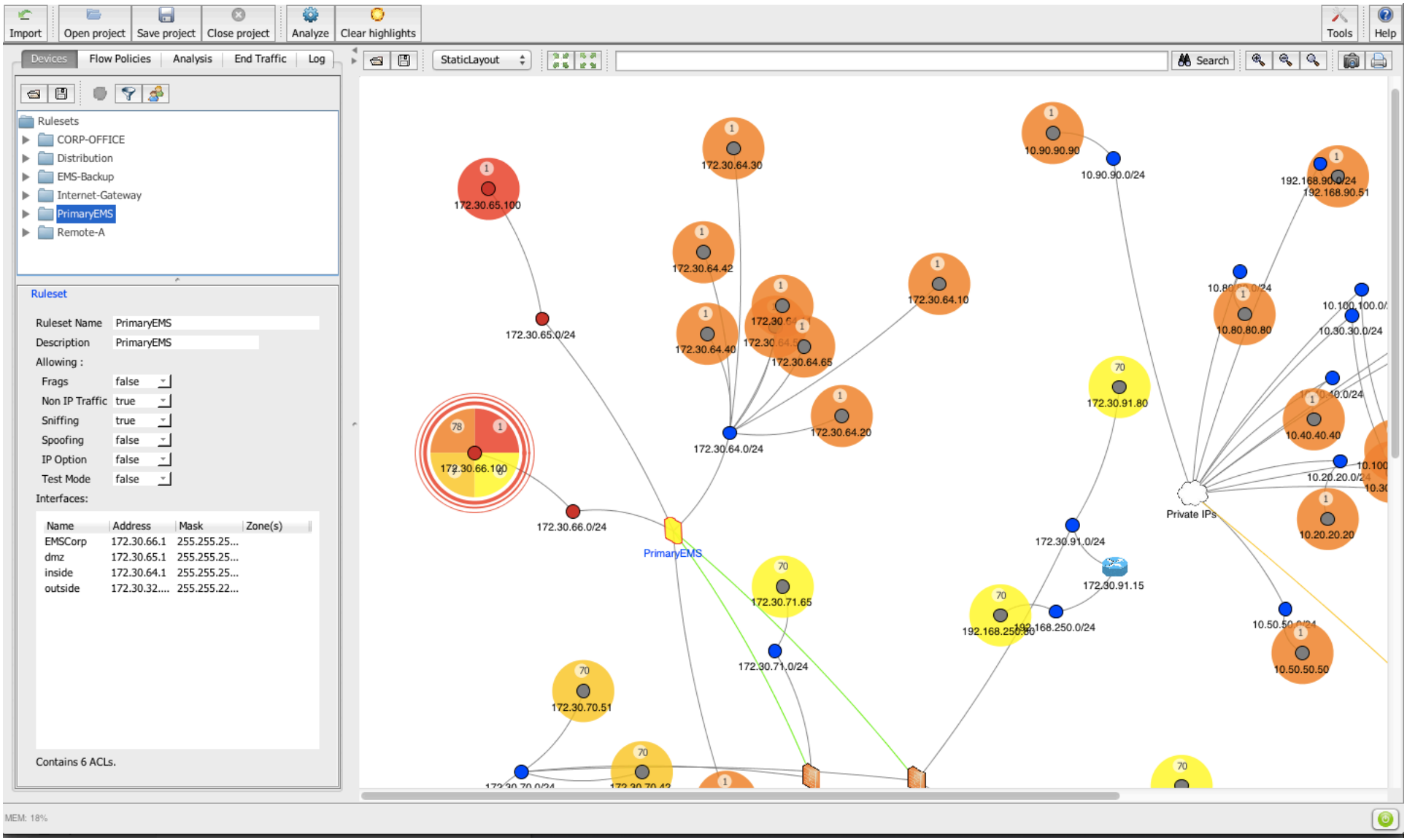
- **Fast** paths
  - Only explore network-to-network paths
  - Stops analyzing a pair of networks as soon as a path is found between them

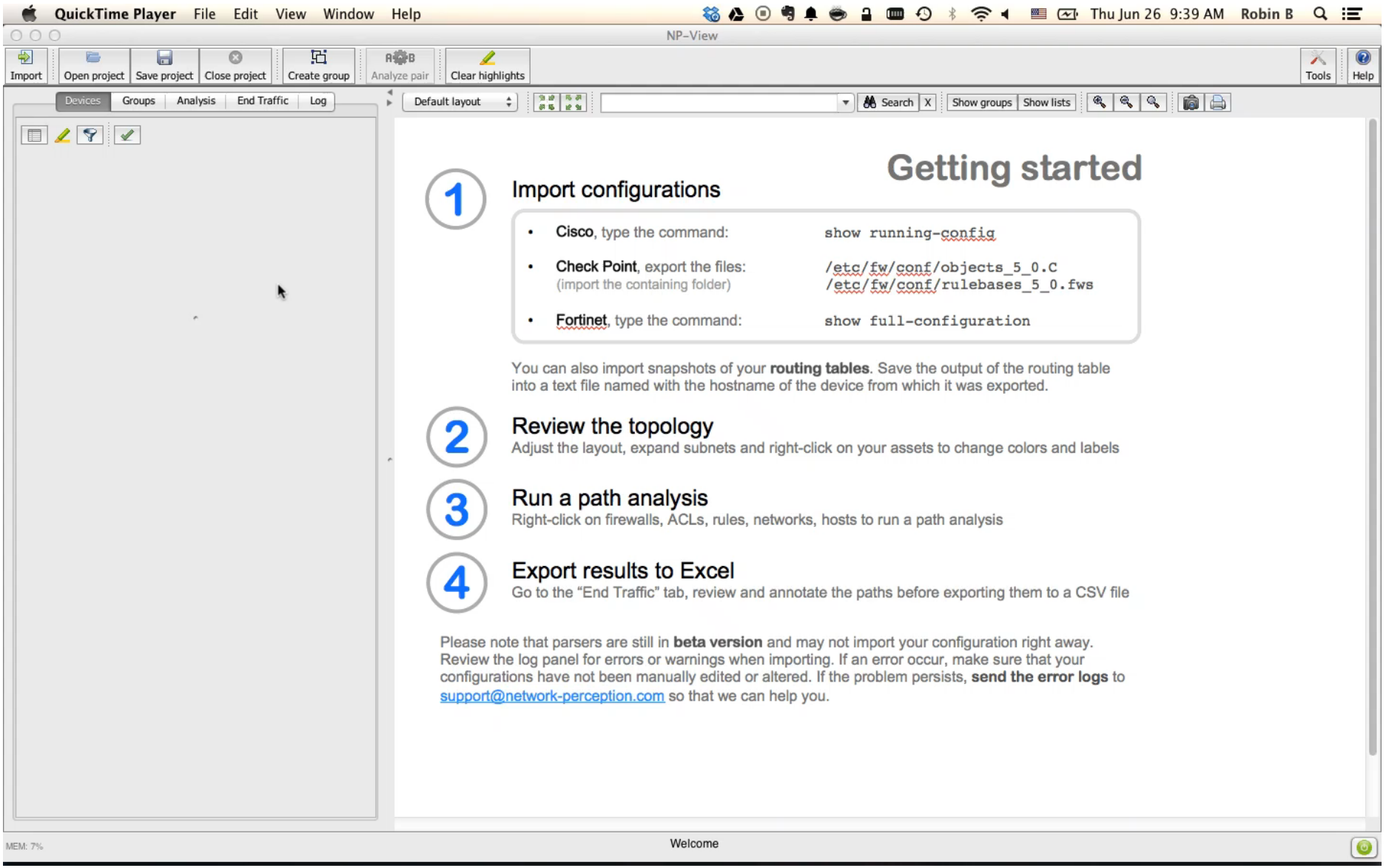
- **Protocol** filtering
  - Can include/exclude protocols taken into account



CSL: COORDINATED SCIENCE LAB

Network Vulnerability Analysis




QuickTime Player File Edit View Window Help
Thu Jun 26 9:39 AM Robin B
NP-View
Import
Open project
Save project
Close project
Create group
Analyze pair
Clear highlights
Tools
Help
Devices
Groups
Analysis
End Traffic
Log
Default layout
Search
X
Show groups
Show lists
Getting started
1
Import configurations
Cisco, type the command: show running-config
Check Point, export the files: /etc/fw/conf/objects_5_0.C
(import the containing folder) /etc/fw/conf/rulebases_5_0.fws
Fortinet, type the command: show full-configuration
You can also import snapshots of your routing tables. Save the output of the routing table into a text file named with the hostname of the device from which it was exported.
2
Review the topology
Adjust the layout, expand subnets and right-click on your assets to change colors and labels
3
Run a path analysis
Right-click on firewalls, ACLs, rules, networks, hosts to run a path analysis
4
Export results to Excel
Go to the "End Traffic" tab, review and annotate the paths before exporting them to a CSV file
Please note that parsers are still in beta version and may not import your configuration right away. Review the log panel for errors or warnings when importing. If an error occur, make sure that your configurations have not been manually edited or altered. If the problem persists, send the error logs to support@network-perception.com so that we can help you.
MEM: 7%
Welcome

Network Perception Startup Incorporation

- Support from the University research park
  - Grant to cover initial legal and accounting costs
  - Entrepreneur mentor
  - Resources for logo and website design
  - Assistance to find funding (e.g., SBIRs)

np network perception

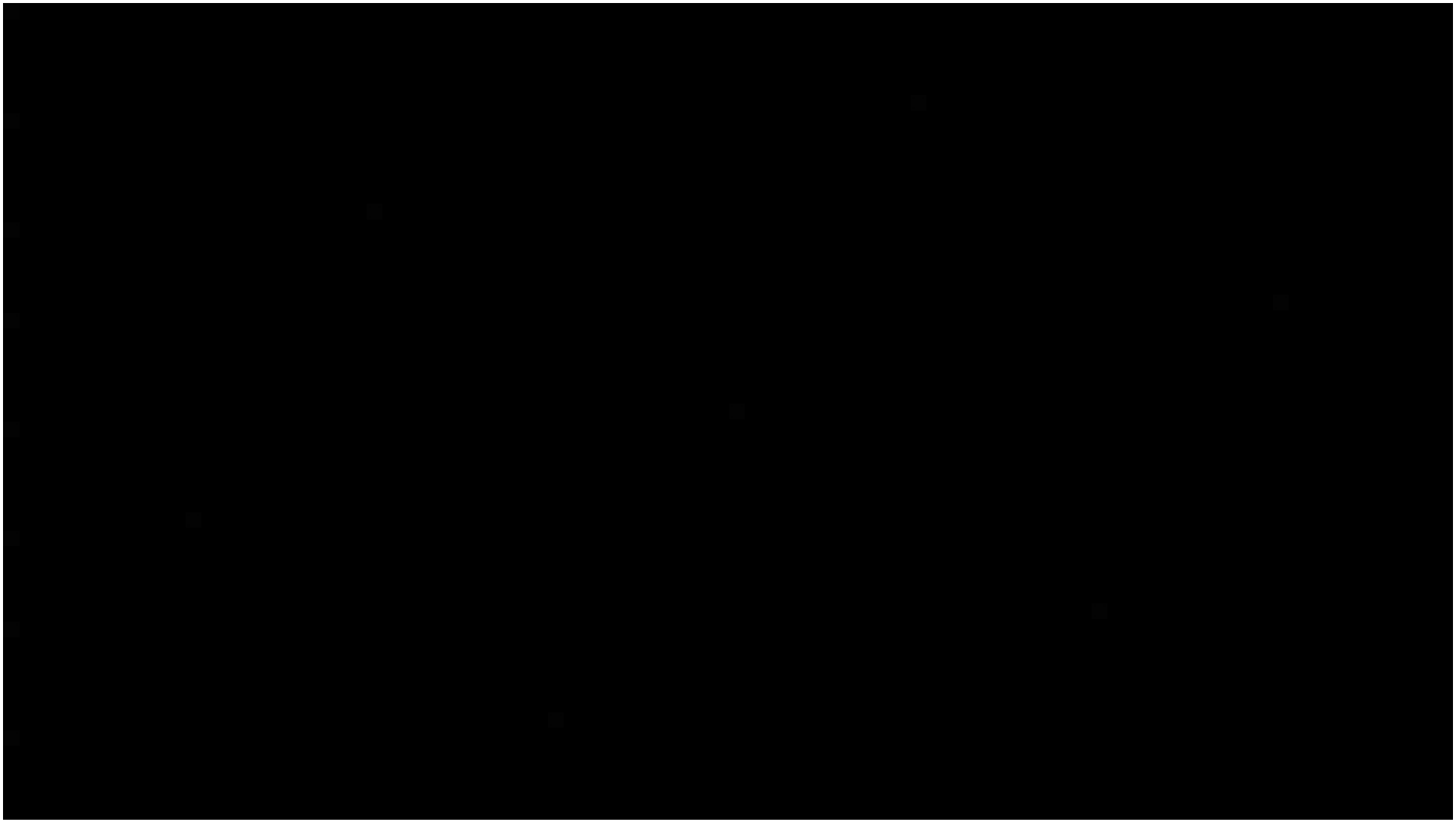
Product Refinement

- Accepted in NSF Innovation Corps program
  - http://www.nsf.gov/news/special_reports/i-corps/

Intense 1 week session in San Francisco in January 2014

100+ potential customer interviews

Refinement of tool focus



Publications

Patent

- S. Singh, D. M. Nicol, W. H. Sanders, and M. Seri. Analysis of Distributed Policy Rule-Sets for Compliance with Global Policy. *Provisional Patent Application* in TF070703, BHGL 10322-99, Serial Number 60/941, 132, June 2007.

Papers

- D. M. Nicol, W. H. Sanders, S. Singh, and M. Seri. Usable Global Network Access Policy for PCS. *IEEE Security and Privacy*, 6(6), November-December, 2008, pp. 30-36.
- D. M. Nicol, W. H. Sanders, S. Singh, and M. Seri. Experiences Validating the Access Policy Tool in Industrial Settings. In *Proceedings of the 43rd Annual Hawai'i International Conference on System Sciences (HICSS)*, Koloa, Kauai, Hawaii, January 5-8, 2010, pp. 1-8.
- R. K. Cunningham, S. Cheung, M. Fong, U. Lindqvist, D. M. Nicol, R. Pawlowski, E. Robinson, W. H. Sanders, S. Singh, A. Valdes, B. Woodworth, and M. Zhivich. Securing Process Control Systems of Today and Tomorrow. In *Proceedings of the IFIP WG 11.10 International Conference on Critical Infrastructure Protection*, Hanover, NH, March 2007.
- S. Singh, D. M. Nicol, W. H. Sanders, and M. Seri. Verifying SCADA Network Access Control Policy Implementations Using the Access Policy Tool. In *Proceedings of the IFIP WG 11.10 International Conference on Critical Infrastructure Protection,* Hanover, NH, March 2007.

To Learn More about TCIPG

- www.tcipg.org
- Bill Sanders whs@illinois.edu
- Request to be on our mailing list
- Attend Monthly Public Webinars
- Attend our Industry Workshop Nov. 12-13, 2014
- Attend the TCIPG Summer School June 15-19, 2015