CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS'

A Tool for Compliance and Depth of Defense Metrics

University of Illinois at Urbana-Champaign

David M. Nicol

September 16-18, 2013

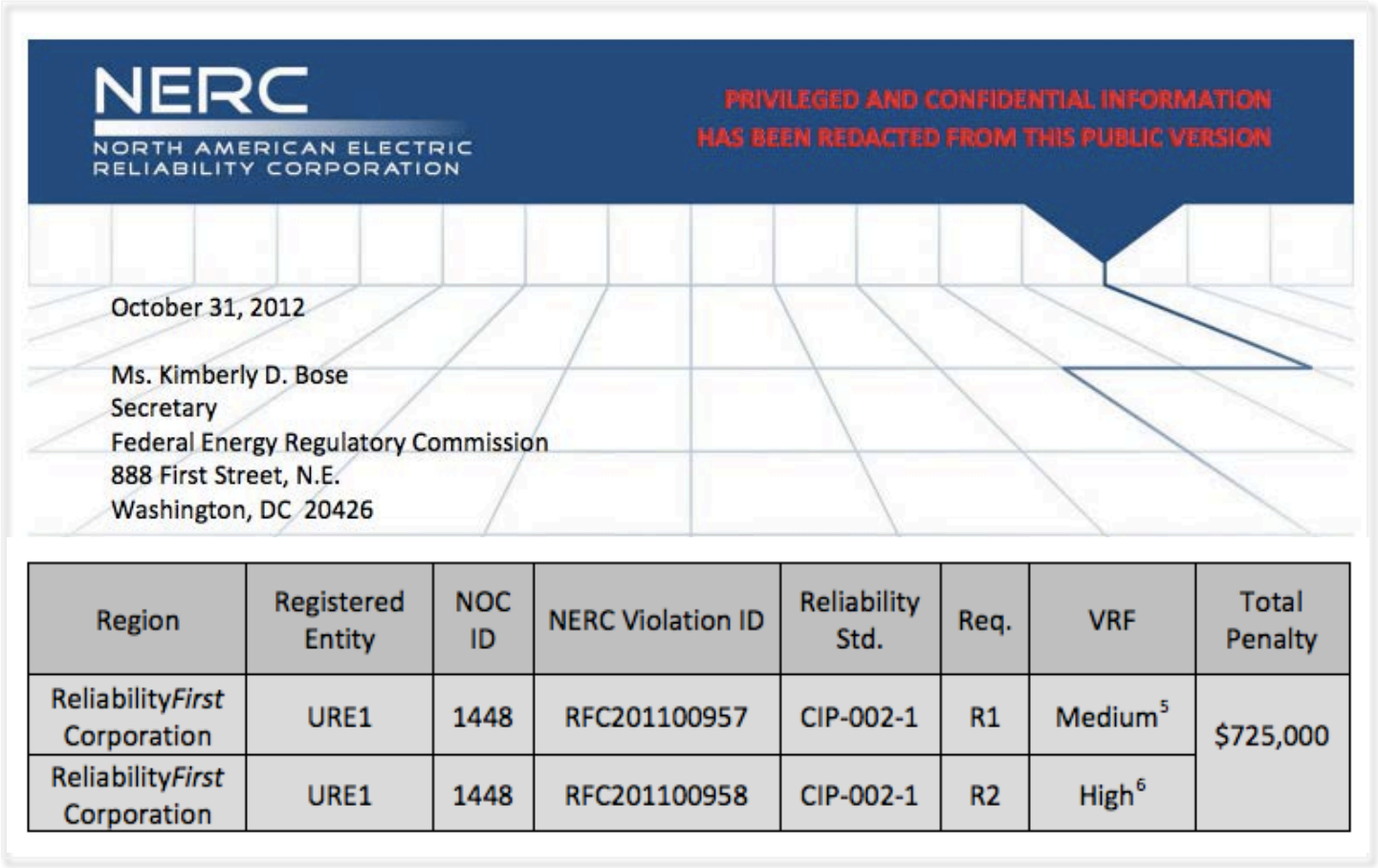
Homeland Security

Science and Technology

Team Profile

- Prof. **David M. Nicol**, PI
  - Director of Information Trust Institute (1.5 years) and professor in ECE and CS departments (25 years)
- Prof. **William H. Sanders**, co-PI
  - Director of Coordinated Science Laboratory (2 years) and professor in ECE and CS departments (24 years)
- Dr. **Robin Berthier**, Research Scientist
  - Researcher on cyber security for critical infrastructure at UIUC (3 years)
- **Edmond Rogers**, Security Engineer
  - Security analyst for large energy utilities and critical infrastructure (20 years) and researcher at UIUC (1 year)
- **Mouna Bamba**, Lead Developer
  - Lead developer of NetAPT (6 years)

NERC-CIP Violation Fines Motivate Electric Utilities



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

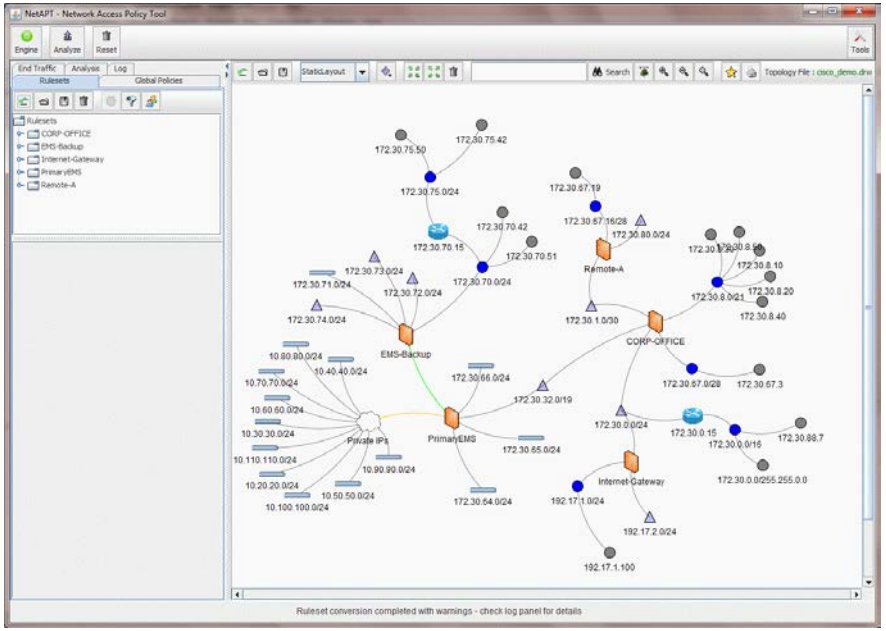
Customer Need

- Complexity of network infrastructures is growing every day
  - Security policies become too large to be manually verified
  - Electric utilities do not have IT resources to manage incidents
- Lack of situational awareness solutions to understand the impact of potential threats
  - Metrics can help

Approach

- The NetAPT tool performs a comprehensive security policy analysis
  - Determine flows that are permitted
  - Identify threat and impact of stepping-stone attacks that use permitted flows and compromised hosts to circumscribe firewall defenses

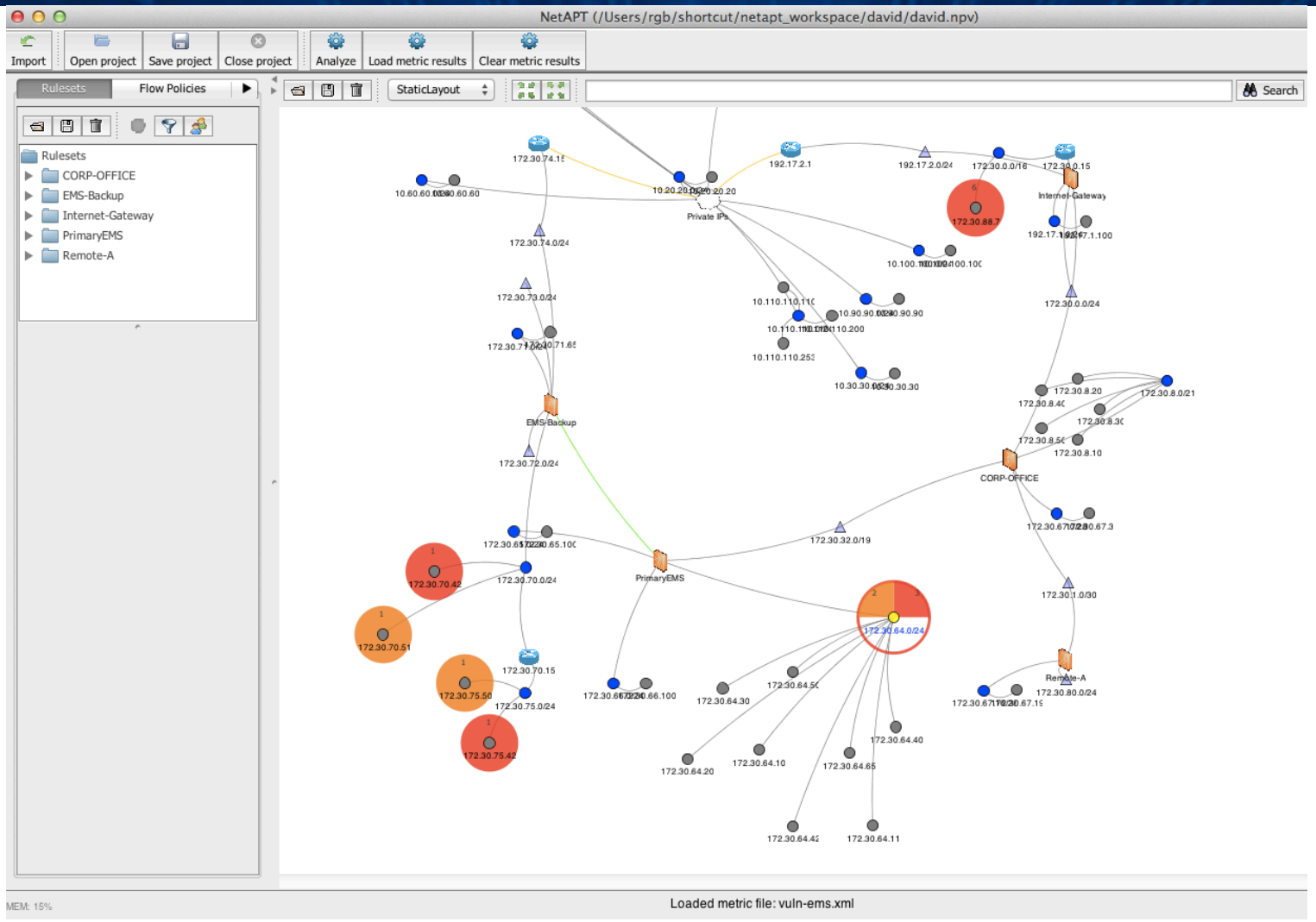
- Highly-usable GUI with network mapping and exploration capabilities
- Defense-in-depth metrics and representation on GUI



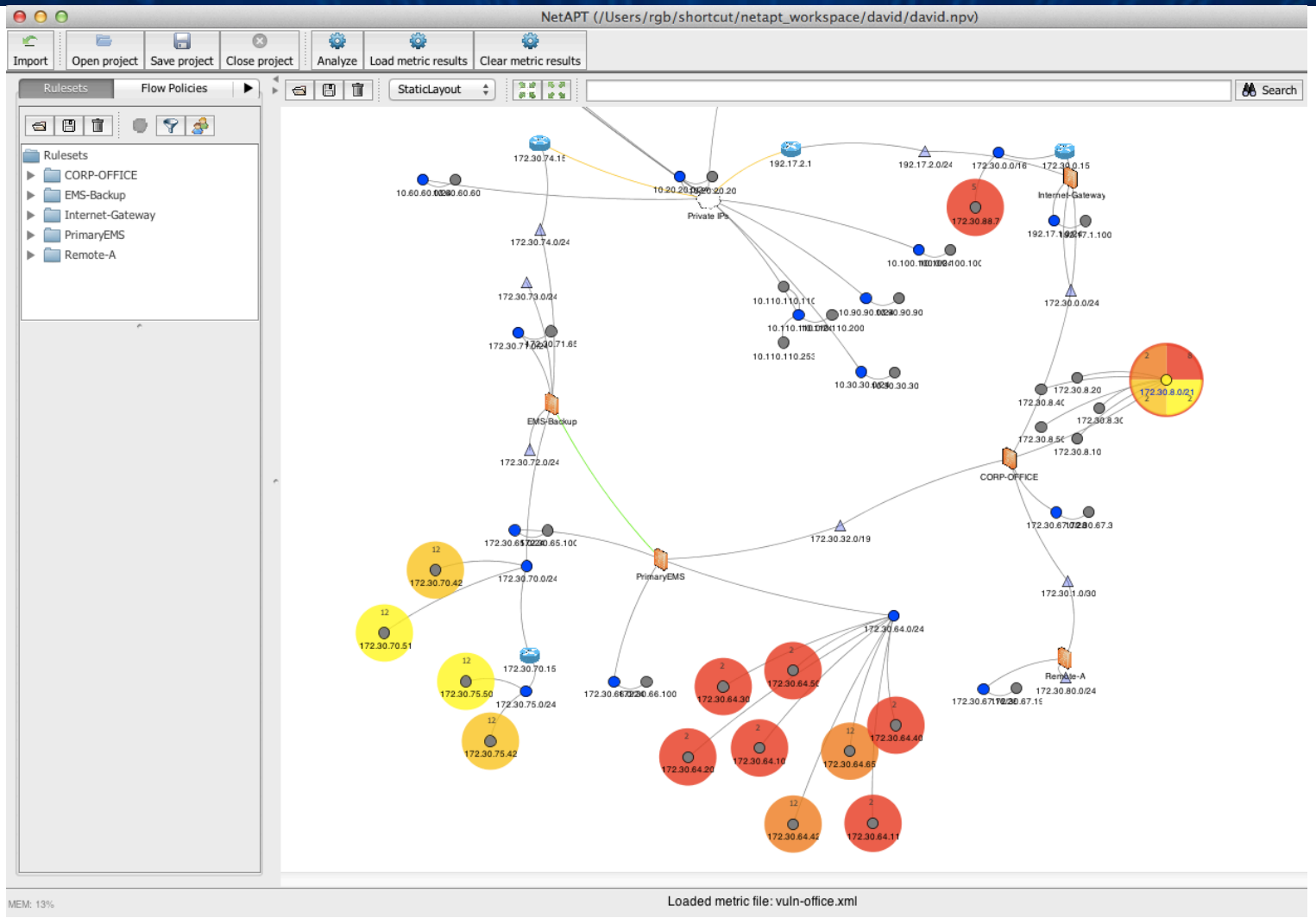
Approach (cont.)

- Access paths describe compliance
- For any host or network compute ‘vulnerability’ to another host or network in terms of
  - ‘*depth*’ : Minimum number of stepping stones (compromised hosts) required for access
  - ‘*width*’ : measure of number of attacking hosts, or unique stepping stone attack vectors
- Metrics give insight into configuration strength or vulnerability
  - Long depth, low width reflects tight configuration
  - Short depth means few compromises needed
  - High width means many different combinations of compromised hosts give access

Approach: EMS Configuration is Tight



Approach: Corporate Configuration is not so Tight



Benefits

- Significantly reduces resources needed to comply with CIP regulations
  - Cut average firewall rule analysis time
- Improves accuracy of security analysis
  - Supports changes that reduce attack surface and mitigates human errors
- Provides metrics to assess potentials of stepping-stone attacks, and optimize network changes
  - Describe the network's defensive strength (reachability metrics)
  - Facilitate audit process (IP and service usage metrics)

Current Status

- Accomplishments / Milestones
  - Refactored tool, development & integration of metrics
  - Focused documentation and user guides
  - Placement in NERC-CIP audits
  - Users training at NERC-CIP audit workshop
  - 50+ evaluation licenses
- Deliverables
  - Refactored code, and documentation.

Schedules

  - Project extended to 31 December.

Next Steps

- Metrics sensitive to host/service vulnerabilities and ability to serve as stepping stone
- Integration and testing of 2 additional firewalls beyond Cisco, Checkpoint, and Sonicwall
  - Juniper and Fortinet
  - Support additional NERC-CIP audit
- Tech Transfer
  - Network Perception fully launched
    - http://www.network-perception.com
  - Business model
    - Consulting + tool placement
    - Licensing of core technologies
  - Accepted to participate in NSF I-Core program

Contact Information

David M. Nicol (dmnicol@illinois.edu) (217) 244-1925
Robin Berthier (rgb@illinois.edu) (217) 265-6382