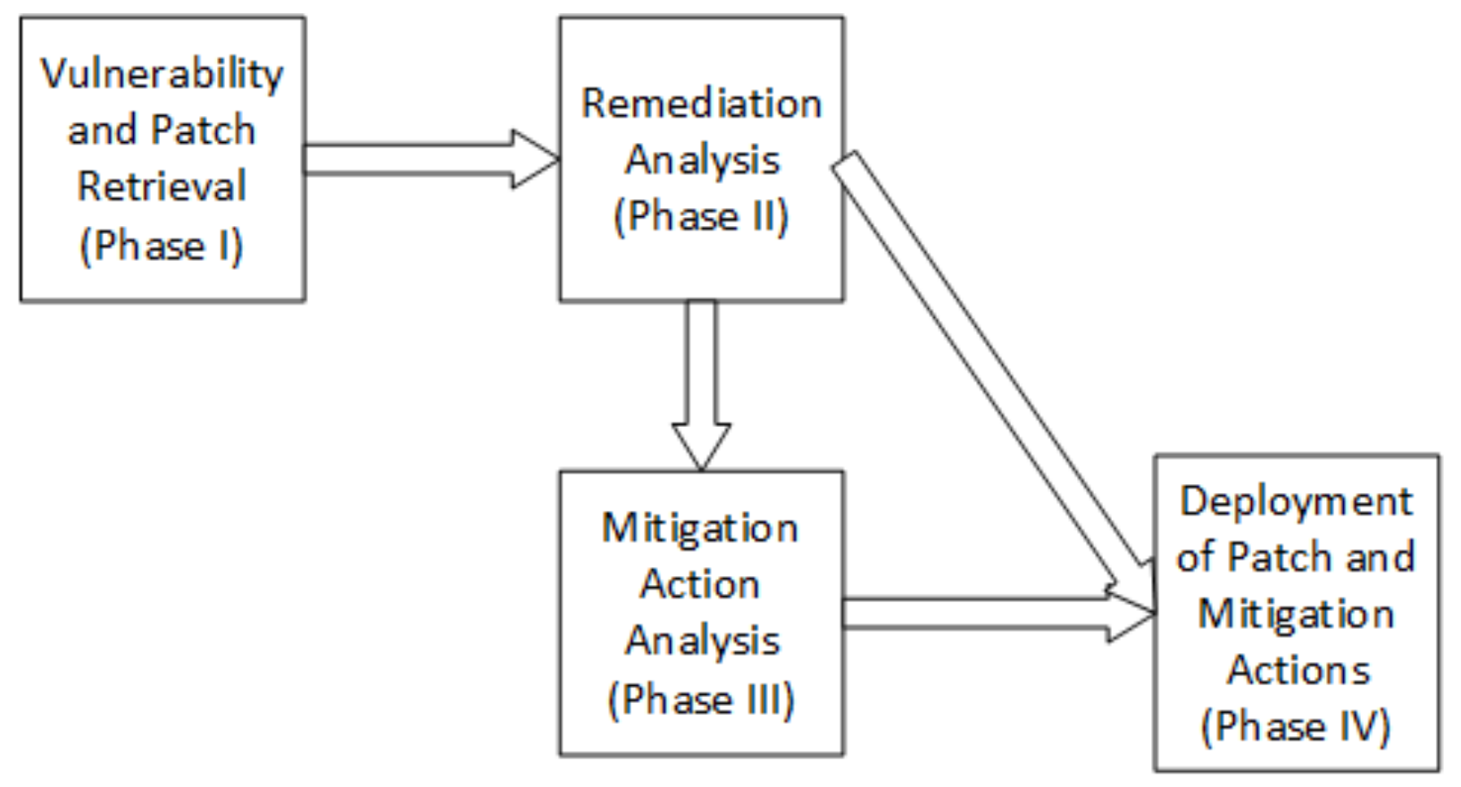
CAREER: Towards Automated Security Vulnerability and Patch Management for Power Grid Operations

NSF Award Number: 1751255

PI: Qinghua Li
Students: Fengli Zhang, Kylie McClanahan, David Darling
University of Arkansas

Introduction

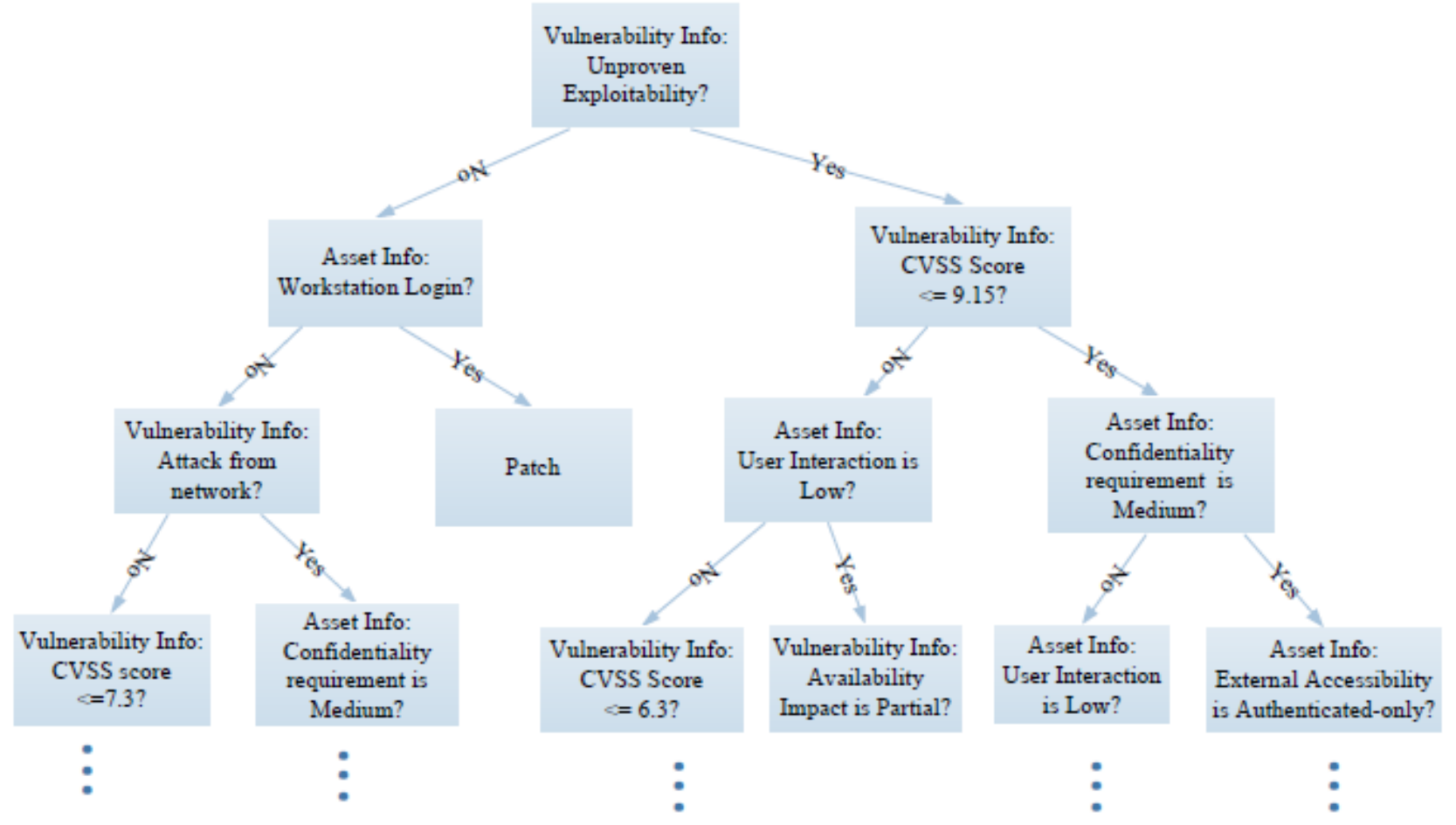
- Vulnerability and patch management (VPM) is one core component of security in energy companies


Vulnerability and Patch Retrieval (Phase I)
Remediation Analysis (Phase II)
Mitigation Action Analysis (Phase III)
Deployment of Patch and Mitigation Actions (Phase IV)

- Challenges
  - Many vulnerabilities with assets emerge each month
  - The National Electric Regulatory Commission (NERC) Critical Infrastructure Protection (CIP) compliance regulation CIP-007-6 R2 requires flawless vulnerability remediation
  - Energy companies need to remediate each and every vulnerability through patching or mitigation plans
  - Remediating vulnerabilities is currently a heavily manual process, with vulnerabilities exposed for months
  - No research or tools available for automating VPM decision making
- Goal: Automate VPM decision making to get better security at lower cost

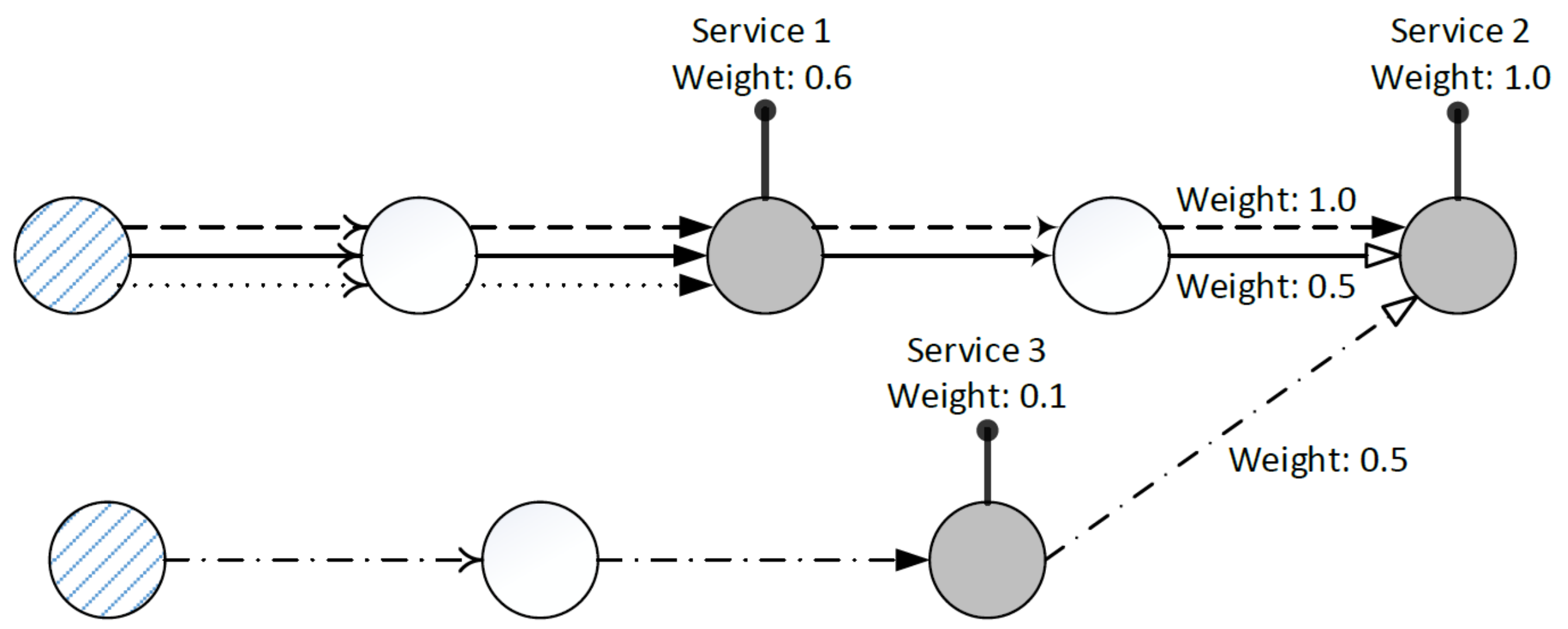
Research Approaches and Outcomes

- Learning-Based Automated Remediation Action Analysis
  - Problem: predict how to remediate a new vulnerability, e.g., Patch-Now, Mitigate-Now-Patch-Later, and Patch-Later.
  - Approach: Decision tree based prediction and reason code generation optimized with data analytics and domain knowledge
  - Evaluation: two one-year VPM operation datasets from an electric utility partner
  - Results: prediction accuracy 99.8%, false negative 0.2%


Vulnerability Info: Unproven Exploitability?
No
Yes
Asset Info: Workstation Login?
Vulnerability Info: CVSS Score <= 9.15?
No
Yes
No
Yes
Vulnerability Info: Attack from network?
Patch
Asset Info: User Interaction is Low?
Asset Info: Confidentiality requirement is Medium?
No
Yes
No
Yes
No
Yes
Vulnerability Info: CVSS score <=7.3?
Asset Info: Confidentiality requirement is Medium?
Vulnerability Info: CVSS Score <= 6.3?
Vulnerability Info: Availability Impact is Partial?
Asset Info: User Interaction is Low?
Asset Info: External Accessibility is Authenticated-only?

Research Approaches and Outcomes (Cont'd)

- Automated Mitigation Action Selection
  - Problem: choose the best mitigation actions for a set of vulnerabilities to minimize the impact to system functions
  - Approach: data flow driven modeling and formulation of Minimal Impact Mitigation Action Selection (MIMAS) Problem.



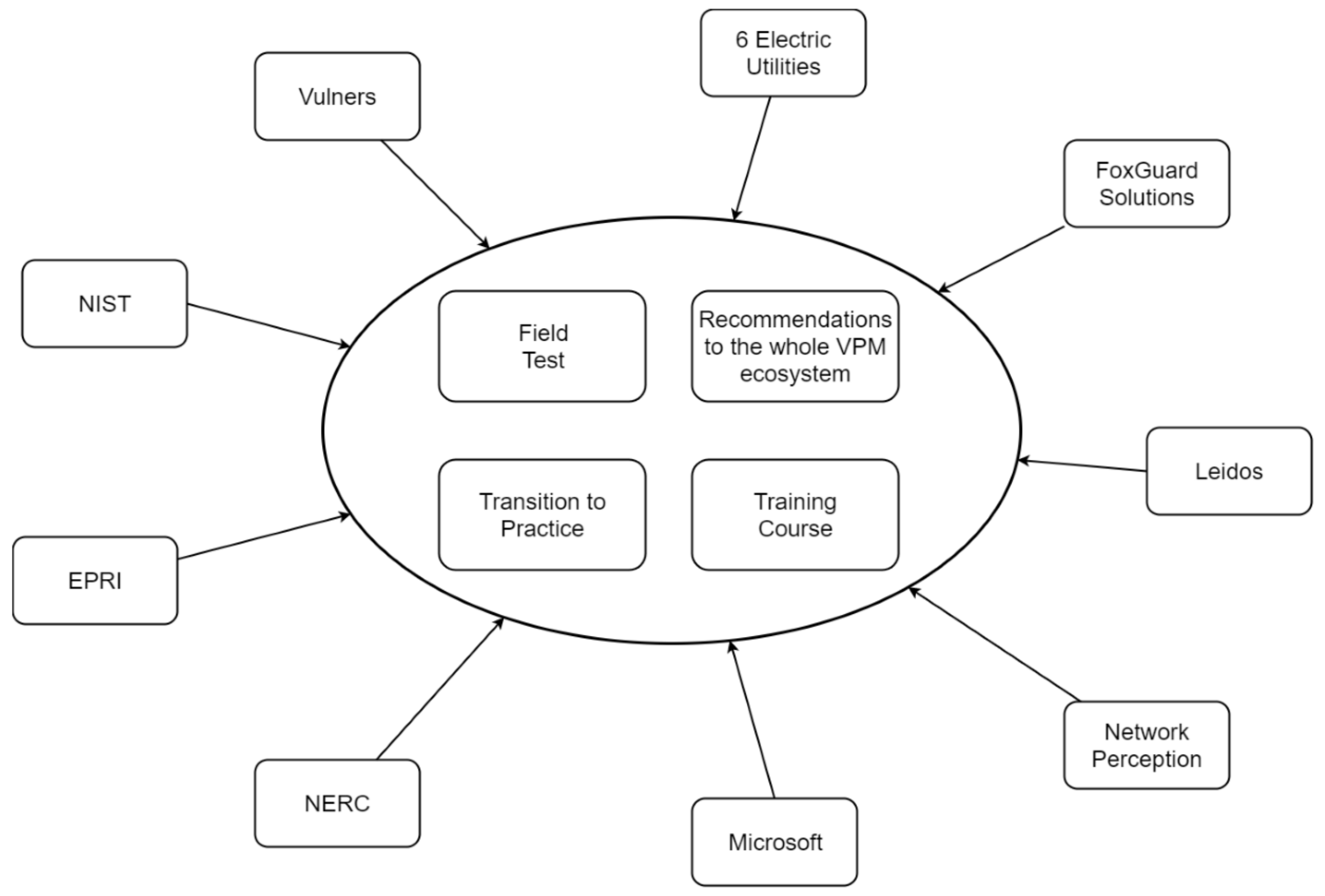
- Risk-Aware Patching Scheduling
  - Problem: find the optimal schedule for applying patches and mitigation actions to reduce security risks and cost
  - Approach: formulate a Minimal Risk Patch Scheduling Problem and develop solutions
  - Initial results of a heuristic solution: 40% risk reduction
- Data study findings
  - Localities of vulnerabilities in the feature space
  - Inconsistency in manual decisions for medium-risk vulnerabilities

Education Activities

- Course development on VPM for graduate students and senior undergraduate students
  - Topics of interest from the industry perspective collected in the NERC CIPC Meeting in September 2019
  - Course being designed and planned to be offered in Fall 2020
- Short training course for security operators at electric utilities
  - Topics of interest from the industry perspective collected in the NERC CIPC Meeting in September 2019
  - Course being developed and planned to be first offered in Summer 2020

Partners and Connections Established

- Three electric utility companies (anonymized upon their request) as field test sites
- Three other electric utility companies in conversation as potential field test sites
- Third-party services: FoxGuard Solutions
- Vendors: Network Perception, Microsoft, Leidos (Industrial Defender)
- Regulation organization: NERC
- Technology transfer partners: Network Perception, EPRI
- Public VPM data partners: NIST, Vulners



Impacts and Disseminations

- Much shorter delays and much less time needed for electric utility companies to make VPM decisions and develop mitigation plans: better security at lower cost
- Better trained workforce for VPM through courses for future employees and short training courses for current employees
- Invited talk at the Southwest Power Pool Security Working Group Meeting in February 2019
- Invited talk at the NERC Critical Infrastructure Protection Committee Meeting in September 2019
- Hosted a training workshop on automated VPM at the NERC Critical Infrastructure Protection Committee Meeting in September 2019
- Paper submitted to IEEE INFOCOM 2020
- Another paper in preparation for IEEE CNS 2020
- Two female students supported and trained