

Towards Automated Security Vulnerability and Patch Management for Power Grid Operations



UNIVERSITY OF
ARKANSAS

Challenge:

- Large number of software vulnerabilities that electric utilities must deal with every month
- Vulnerability analysis and remediation decision-making is currently a heavily manual process, causing long delays and high security risks

Solution:

- AI-based automation technologies for vulnerability and patch management
- Dynamic vulnerability risk analysis
- Optimal patch scheduling
- Asset-vulnerability mapping
- Blockchain-based non-attributable vulnerability intelligence sharing



Scientific Impact:

- Innovative solutions for automated vulnerability analytics and remediation decision-making to reduce security risks
- Security operation automation solves not only a security problem but also a human problem by saving manual efforts

Broader Impact and Broader Participation:

- Transform the current vulnerability and patch management practice in the electric sector from manual operations to automated operations
- Technology licensed to a company for commercialization
- 4 publications, 1 patent application, 1 tutorial, 2 invited talks
- 2 PhD graduated
- 3 female students, 1 African American student, and 2 high-school students involved

Award Number: 1751255
Recipient: University of Arkansas
PI: Qinghua Li
Email: qinghual@uark.edu